

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное автономное образовательное учреждение высшего образования
«Севастопольский государственный университет»**

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к лабораторным работам по дисциплине
“ОПЕРАЦИОННЫЕ СИСТЕМЫ”, часть 2,
для студентов ОФО и ЗФО направлений подготовки:
09.03.01 «Информатика и вычислительная техника»
09.03.02 «Информационные системы и технологии»
27.03.04 «Управление в технических системах»**

Севастополь
2020

УДК 004.451

Методические указания к выполнению лабораторных работ по дисциплине «Операционные системы», часть 1, для студентов ОФО и ЗФО направлений подготовки: 09.03.01 «Информатика и вычислительная техника», 09.03.02 «Информационные системы и технологии» / Сост. М.А. Лебедева, Е.М. Шалимова. – Севастополь: Изд-во СевГУ, 2020. – 62с.

Целью методических указаний является оказание помощи студентам в выполнении лабораторных работ по дисциплине «Операционные системы».

Приведены теоретические сведения, необходимые для выполнения лабораторных работ, варианты заданий, рекомендации по выполнению, требования к отчетам.

Методические указания рассмотрены и утверждены на заседании кафедры «Информационные технологии и компьютерные системы», протокол № 1 от 31.08.2020г.

Рецензент: доцент кафедры «Информационные технологии и компьютерные системы», к.т.н. Е.В. Козлова.

СОДЕРЖАНИЕ

- 1. ЛАБОРАТОРНАЯ РАБОТА №1. ИЗУЧЕНИЕ НАСТРОЕК ОС WINDOWS**
- 2. ЛАБОРАТОРНАЯ РАБОТА №2. ИНТЕРПРЕТАТОР КОМАНДНОЙ СТРОКИ ОС WINDOWS**
- 3. ЛАБОРАТОРНАЯ РАБОТА №3. УПРАВЛЕНИЕ ФАЙЛАМИ В ОС WINDOWS**
- 4.ЛАБОРАТОРНАЯ РАБОТА № 4. ЗАЩИТА УЧЁТНЫХ ЗАПИСЕЙ И ДАННЫХ В ОС WINDOWS**
- 5. ЛАБОРАТОРНАЯ РАБОТА №5. УПРАВЛЕНИЕ ПАМЯТЬЮ И ВВОДОМ/ВЫВОДОМ В ОС WINDOWS**
- 6.ЛАБОРАТОРНАЯ РАБОТА №6. МОНИТОРИНГ ПРОИЗВОДИТЕЛЬНОСТИ ОС WINDOWS**
- 7.ЛАБОРАТОРНАЯ РАБОТА №7.ВЫЯВЛЕНИЕ ПРИСУТСТВИЯ НА КОМПЬЮТЕРЕ ВРЕДНОСНЫХ ПРОГРАММ**
- 8. ЛАБОРАТОРНАЯ РАБОТА № 8. АУДИТ**
- 9. ЛАБОРАТОРНАЯ РАБОТА №9. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА В ОС WINDOWS**
- 10. ЛАБОРАТОРНАЯ РАБОТА №10. БРАНДМАУЭР WINDOWS**

ЛАБОРАТОРНАЯ РАБОТА №1. ИЗУЧЕНИЕ НАСТРОЕК ОС WINDOWS.

Цель работы: получение навыков в использовании настроек операционной системы.

1.1 Основные теоретические положения

1.1.1 Понятие автозапуска

Автозапуск – это функция операционной системы (ОС), которая заключается в том, что ОС сразу же после подключения устройства приступает к загрузке и считыванию информации. При этом появляется окно (рисунок 1.1), отображающее процесс сканирования устройства и определения типов файлов на носителе.

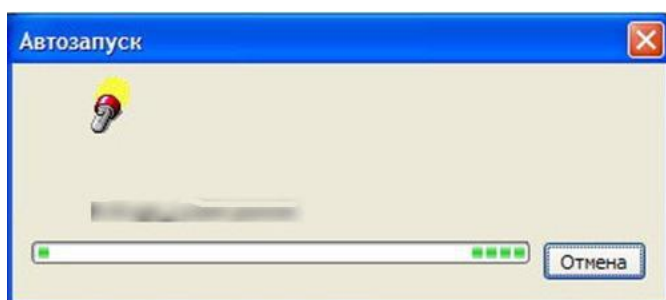


Рисунок 1.1.- Процесс сканирования устройства

Затем открывается другое окно (рисунок 2), в котором у пользователя спрашивают, какое действие следует выполнить с открываемым устройством. Например, при помещении в DVD-привод диска с музыкой система автоматически определит тип диска, запустит программу воспроизведения аудиофайлов и приступит к проигрыванию музыки.



Рисунок 1. 2.- Окно выбора действия

С одной стороны, функция очень удобная и полезная: автоматически выполняет некоторые функции. Но с другой стороны, этот механизм таит в себе угрозу. Так, вирус, проникнув на носитель информации и прописавшись в файле "autorun.inf", обеспечит себе "беспрепятственный" пропуск на компьютер при подключении устройства к системе. Поэтому рекомендуется отключить функцию автозапуска флешки и других носителей в системе. Следует отметить, что функция автозапуска ОС семейства Windows включена по умолчанию.

1.1.2 Отключение автозапуска флеш-накопителя в Windows 7

1. Нажмите кнопку *Пуск* и в поиске введите *автозапуск*. Система найдет все варианты, в которых встречается это слово. Выберите пункт *Автозапуск*, как показано на рисунке 3.

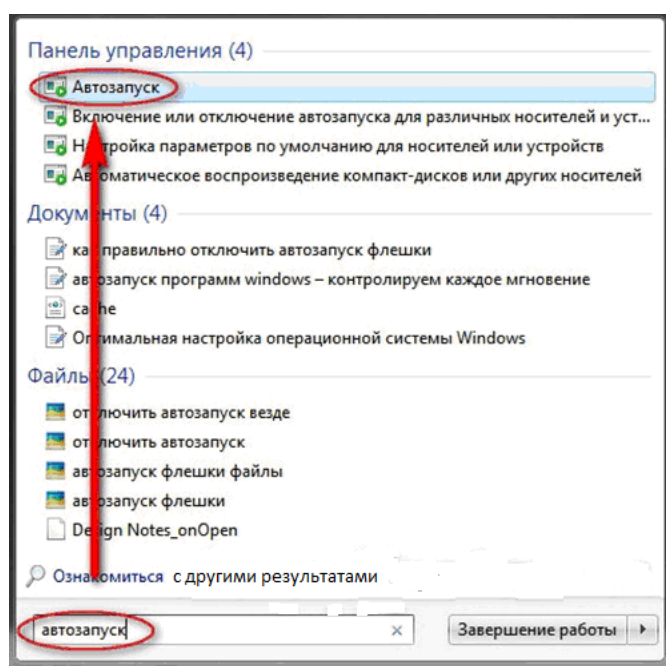


Рисунок 1.3.- Окно выбора *Автозапуска*

2. В открывшемся окне снимите галочку *Использовать автозапуск для всех носителей и устройств* и кликните по кнопке *Сохранить*. Можете также в этом же окне самостоятельно настроить автозапуск необходимых устройств.

1.1.3. Получение информации о компьютере

Подробную информацию о компьютере и установленной ОС можно узнать разными способами, в том числе с помощью специальных программ.

Однако в ОС Windows есть один способ, о котором не все знают. С его помощью можно получить много полезной информации, в том числе и время бесперебойной работы компьютера (как долго компьютер работает с момента включения). Сделайте следующее:

Пуск → *Все программы* → *Стандартные* → *Командная строка*.

Далее в командной строке наберите *systeminfo* и ознакомьтесь с полученной информацией.

1.1.4. Восстановление прежних окон папок при входе в систему

Если у Вас открыты важные окна и появилась необходимость выключить или перезагрузить компьютер, в есть возможность сделать так, что при следующем включении компьютера окна будут на том же месте, где и были до перезагрузки. Эта возможность действует только на окна (открытые папки), но не на запущенные программы.

Для запуска такой возможности её активировать.

В Windows 7 – Пуск → Панель управления → Все элементы управления → Параметры папок, затем поставьте галочку в пункте Восстанавливать прежние окна папок при входе в систему и нажмите кнопку ОК.

1.1.5. Полезные советы по настройке Windows

При работе часто возникают ситуации, когда происходит сбой в системе или какая-нибудь программа «зависает» и приходится ее отключать. В таких ситуациях обычно появляется окно с предложением об отправке отчета в службу Microsoft.

Для отключения появления таких окон совершаем правый клик по ярлыку *Мой компьютер – Свойства → Панель управления → Все элементы управления → Устранение неполадок* устанавливаем соответствующие флажки.

.

2. Задание на выполнения лабораторную работу

1. Изучить материал, представленный в данных методических указаниях.
2. Отключить автозапуск флеш-накопителя.
3. Получить информацию о компьютере.
4. Ответить на контрольные вопросы.
5. Оформить отчет о проделанной работе.

3. Контрольные вопросы

1. Для чего необходим автозапуск дисков?
2. Какие проблемы связаны с автозапуском?
3. Как отключить автозапуск?
4. Каким образом безопаснее открывать usb-флешки и иные внешние носители?
5. Каким образом можно получить подробную информацию о своем компьютере?
7. Для чего нужен отчет об ошибках? Какие могут быть отрицательные последствия в случае его отключения?
8. Что нужно сделать, чтобы происходило восстановление прежних окон папок при входе в систему?

2. ЛАБОРАТОРНАЯ РАБОТА №2. ИНТЕРПРЕТАТОР КОМАНДНОЙ СТРОКИ ОС WINDOWS

Цель работы: изучение возможностей интерпретатора командной строки ОС Windows, приобретение практических навыков работы в командном режиме.

2.1. Основные теоретические положения

2.1.1. Запуск оболочки командной строки

Во всех версиях ОС Windows поддерживается интерактивная оболочка командной строки (command shell) и определенный набор утилит (количество и состав этих утилит зависит от версии ОС). Начиная с версии Windows NT, оболочка командной строки представляется интерпретатором Cmd.exe.

Запуск командного интерпретатора (открытия нового сеанса командной строки) можно выполнить разными способами, например:

через меню «Пуск»: «Пуск» - «Все приложения»- «Стандартные»-«Командная строка»;
комбинацией клавиш WINDOWS+X (в WINDOWS 10);

в окне ПОИСК набрать cmd;

в окне «Выполнить» (Windows+R) набрать cmd.

Единственный из способов, который не позволяет запустить командную строку от имени администратора, – это использование команды «Выполнить». В результате откроется окно, представленное на рисунке 2.1.

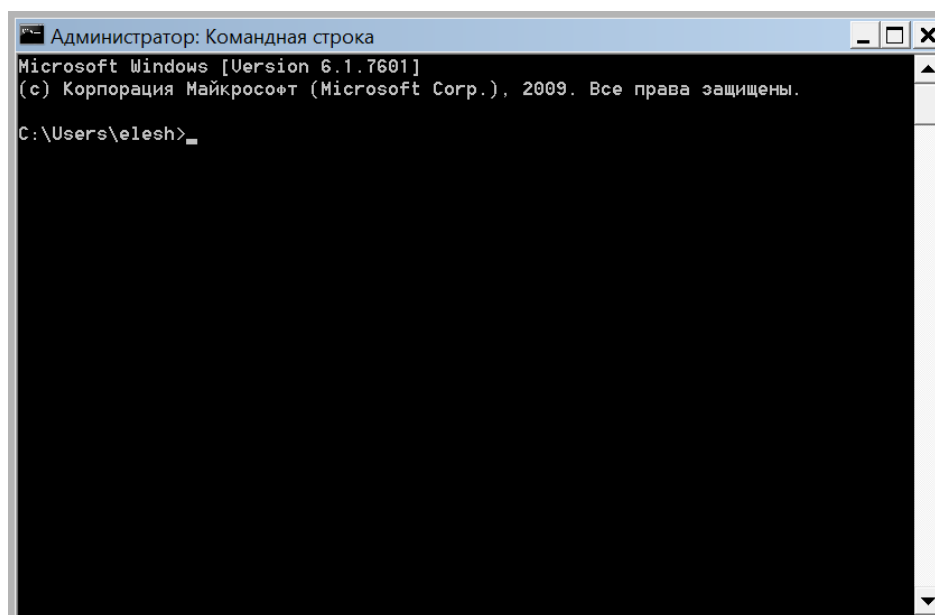


Рисунок 2.1 - Командное окно интерпретатора Cmd.exe в Windows 7

2.1.2. Команды

Все команды делятся на две группы: внутренние и внешние. Команды, которые распознаются и выполняются непосредственно самим командным интерпретатором, команды называются **внутренними** (например, COPY или DIR). Другие команды ОС представляют собой отдельные программы, расположенные по умолчанию в том же каталоге, что и Cmd.exe, которые Windows загружает и выполняет аналогично другим программам. Такие команды называются внешними (например, MORE или XCOPY).

Для того, чтобы выполнить команду, после приглашения командной строки (например, `C:\>`) следует ввести имя этой команды (регистр не важен), параметры и ключи (если они необходимы) и нажать клавишу `<Enter>`. Например: `C:\>COPY C:\myfile.txt A:\ /V`
Здесь `COPY` — имя команды здесь, `C:\myfile.txt` и `A:\` — параметры, а `/V` является ключом. Отметим, что в некоторых командах ключи могут начинаться не с символа `/`, а с символа `-` (минус), например, `-V`.

Многие команды Windows имеют большое количество дополнительных параметров и ключей. Большинство команд снабжено встроенной справкой, для доступа к которой следует ввести команду с ключом `/?`.

Для некоторых команд текст справки может быть довольно большим и не уместиться на одном экране. В этом случае информацию можно выводить последовательно по одному экрану с помощью команды `MORE` и символа конвейеризации `|`, например:

`XCOPY /? | MORE`

В этом случае после заполнения очередного экрана вывод помощи будет прерываться до нажатия любой клавиши. Кроме того, используя символы перенаправления вывода `>` и `>>`, можно текст, выводимый на экран, направить в текстовый файл для дальнейшего просмотра. Например, для вывода текста справки по команде `XCOPY` в текстовый файл `xcopy.txt`, используется следующая команда:

`XCOPY /? > XCOPY.TXT`

В командах вместо имени файла можно указывать обозначения устройств компьютера. В ОС Windows поддерживаются следующие **имена устройств**: `PRN` (принтер), `CON` (терминал: при вводе — это клавиатура, при выводе — монитор), `NUL` (пустое устройство, все операции ввода/вывода для него игнорируются).

2.1.3 Перенаправление ввода/вывода и конвейеризация команд

С помощью переназначения устройств ввода/вывода одна программа может направить свой вывод на вход другой или перехватить вывод другой программы, используя его в качестве своих входных данных. Таким образом, имеется возможность передавать информацию от процесса к процессу при минимальных программных издержках. Практически это означает, что для программ, которые используют стандартные входные и выходные устройства, ОС позволяет:

выводить сообщения программ не на экран (стандартный выходной поток), а в файл или на принтер (перенаправление вывода);

читать входные данные не с клавиатуры (стандартный входной поток), а из заранее подготовленного файла (перенаправление ввода);

передавать сообщения, выводимые одной программой, в качестве входных данных для другой программы (конвейеризация или композиция команд).

Из командной строки эти возможности реализуются следующим образом. Для того, чтобы перенаправить текстовые сообщения, выводимые какой-либо командой, в текстовый файл, нужно использовать конструкцию

команда `>` имя_файла

Если при этом заданный для вывода файл уже существовал, то он перезаписывается, если не существовал — создается. Можно также не создавать файл заново, а *дописывать* информацию, выводимую командой, в конец существующего файла. Для этого команда перенаправления вывода должна быть задана в виде:

команда `>>` имя_файла

С помощью символа `<` можно прочитать входные данные для заданной команды не с клавиатуры, а из заранее подготовленного файла:

команда `<` имя_файла

Рассмотрим примеры перенаправления ввода/вывода.

1) Вывод встроенной справки для команды COPY в файл copy.txt:

```
COPY /? > copy.txt
```

2) Добавление текста справки для команды XCOPY в файл copy.txt:

```
XCOPY /? >> copy.txt
```

3) Вывод текущей даты в файл date.txt (DATE /T — это команда для просмотра и изменения системной даты, T - ключ для получения только даты без запроса нового значения):

```
DATE /T > date.txt
```

Если при выполнении определенной команды возникает ошибка, то сообщение об этом выводится на экран. В случае необходимости сообщения об ошибках (стандартный поток ошибок) можно перенаправить в текстовый файл с помощью конструкции

```
команда 2> имя_файла
```

В этом случае стандартный вывод будет производиться на экран.

Также имеется возможность информационные сообщения и сообщения об ошибках выводить в один и тот же файл. Делается это следующим образом:

```
команда > имя_файла 2>&1
```

Например, в приведенной ниже команде стандартный выходной поток и стандартный поток ошибок перенаправляются в файл copy.txt:

```
XCOPY A:\1.txt C: > copy.txt 2>&1
```

С помощью конструкции команда1 | команда2 можно использовать сообщения, выводимые первой командой, в качестве входных данных для второй команды (конвейер команд).

Используя механизмы перенаправления ввода/вывода и конвейеризации, можно из командной строки посылать информацию на различные устройства и автоматизировать ответы на запросы, выдаваемые командами или программами, использующими стандартный ввод. Для решения таких задач служит команда

ECHO [сообщение], которая выводит сообщение на экран. Пример использования этой команды.

Удаление всех файлов в текущем каталоге без предупреждения (автоматический положительный ответ на запрос об удалении):

```
ECHO y | DEL *.*
```

1.1.4. Команды MORE и SORT

Одной из наиболее часто используемых команд, для работы с которой применяется перенаправление ввода/вывода и конвейеризация, является MORE. Эта команда считывает стандартный ввод из конвейера или перенаправленного файла и выводит информацию частями, размер каждой из которых не больше размера экрана. Используется MORE обычно для просмотра длинных файлов. Возможны три варианта синтаксиса этой команды:

```
MORE [диск:][путь]имя_файла
```

```
MORE < [диск:][путь]имя_файла
```

```
имя_команды | MORE
```

Параметр [диск:] [путь] имя_файла определяет расположение и имя файла с просматриваемыми на экране данными. Параметр имя_команды задает команду, вывод которой отображается на экране (например, DIR или команда TYPE, используемая для вывода содержимого текстового файла на экран). Приведем два примера.

Для поэкранного просмотра текстового файла news.txt возможны следующие варианты команд:

```
MORE news.txt
```

```
MORE < news.txt
```

```
TYPE news.txt | MORE
```

Другой распространенной командой, использующей перенаправление ввода/вывода и конвейеризацию, является SORT. Эта команда работает как фильтр: она считывает символы в

заданном столбце, упорядочивает их в возрастающем или убывающем порядке и выводит отсортированную информацию в файл, на экран или другое устройство. Возможны два варианта синтаксиса этой команды:

`SORT [/R] [/+n] [[диск1:][путь1]файл1] [> [диск2:][путь2]файл2]`

или

`[команда] SORT [/R] [/+n] [> [диск2:][путь2]файл2]`

В первом случае параметр `[диск1:] [путь1] файл1` определяет имя файла, который нужно отсортировать. Во втором случае будут отсортированы выходные данные указанной команды. Если параметры `файл1` или команда не заданы, то `SORT` будет считывать данные с устройства стандартного ввода.

Параметр `[диск2:] [путь2] файл2` задает файл, в который будет направляется сортированный вывод; если этот параметр не задан, то вывод будет направлен на устройство стандартного вывода.

По умолчанию сортировка выполняется в порядке возрастания. Ключ `/R` позволяет изменить порядок сортировки на обратный (от `Z` к `A` и затем от `9` до `0`). Например, для постраничного просмотра отсортированного в обратном порядке файла `price.txt`, нужно задать следующую команду:

`SORT /R < price.txt |MORE`

Ключ `/+n` задает сортировку в файле по символам `n`-го столбца. Например, `/+10` означает, что сортировка должна осуществляться, начиная с 10-й позиции в каждой строке. По умолчанию файл сортируется по первому столбцу.

2.1.5 Условное выполнение и группировка команд

В командной строке Windows можно использовать специальные символы, которые позволяют вводить несколько команд одновременно и управлять работой команд в зависимости от результатов их выполнения. С помощью таких символов условной обработки можно содержание небольшого пакетного файла записать в одной строке и выполнить полученную составную команду.

Используя символ амперсанда `&`, можно разделить несколько утилит в одной командной строке, при этом они будут выполняться друг за другом. Например, если набрать команду `DIR & PAUSE & COPY /?` и нажать клавишу `<Enter>`, то вначале на экран будет выведено содержимое текущего каталога, а после нажатия любой клавиши — встроенная справка команды `COPY`.

Условная обработка команд в Windows осуществляется с помощью символов `&&` и `||` следующим образом. Двойной амперсанд `&&` запускает команду, стоящую за ним в командной строке, только в том случае, если команда, стоящая перед амперсандами была выполнена успешно. Например, если в корневом каталоге диска `C:` есть файл `plan.txt`, то выполнение строки `TYPE C:\plan.txt && DIR` приведет к выводу на экран этого файла и содержимого текущего каталога. Если же файл `C:\plan.txt` не существует, то команда `DIR` выполняться не будет.

Два символа `||` осуществляют в командной строке обратное действие, т.е. запускают команду, стоящую за этими символами, только в том случае, если команда, идущая перед ними, не была успешно выполнена. Таким образом, если в предыдущем примере файл `C:\plan.txt` будет отсутствовать, то в результате выполнения строки `TYPE C:\plan.txt || DIR` на экран выведется содержимое текущего каталога.

Отметим, что условная обработка действует только на ближайшую команду, то есть в строке

`TYPE C:\plan.txt && DIR & COPY /?`

команда `COPY /?` запустится в любом случае, независимо от результата выполнения команды `TYPE C:\plan.txt`.

Несколько утилит можно сгруппировать в командной строке с помощью *круглых скобок*. **Рассмотрим две строки:**

```
TYPE C:\plan.txt && DIR & COPY /?
```

```
TYPE C:\plan.txt && (DIR & COPY /?)
```

В первой из них символ условной обработки && действует только на команду DIR, во второй — одновременно на две команды: DIR и COPY.

2.1.6. Команды для работы с файловой системой

Рассмотрим некоторые наиболее часто используемые команды для работы с файловой системой. Отметим сначала несколько особенностей определения путей к файлам в Windows.

2.1.6.1 Пути к объектам файловой системы

Файловая система логически имеет древовидную структуру и имена файлов задаются в формате [диск:] [путь\] имя_файла, то есть обязательным параметром является только имя файла. При этом, если путь начинается с символа "\", то маршрут вычисляется от корневого каталога, иначе — от текущего каталога. Например, имя C:123.txt задает файл 123.txt в текущем каталоге на диске C:, имя C:\123.txt — файл 123.txt в корневом каталоге на диске C:, имя ABC\123.txt — файл 123.txt в подкаталоге ABC текущего каталога.

Существуют особые обозначения для текущего каталога и родительского каталогов. Текущий каталог обозначается символом . (точка), его родительский каталог — символами .. (две точки). Например, если текущим каталогом является C:\WINDOWS, то путь к файлу autoexec.bat в корневом каталоге диска C: может быть записан в виде ..\autoexec.bat.

В именах файлов (но не дисков или каталогов) можно применять так называемые **групповые символы** или шаблоны: ? (вопросительный знак) и * (звездочка). Символ * в имени файла означает произвольное количество любых допустимых символов, символ ? — один произвольный символ или его отсутствие. Скажем, под шаблон text??1.txt подходят, например, имена text121.txt и text11.txt, под шаблон text*.txt — имена text.txt, textab12.txt, а под шаблон text.* — все файлы с именем text и произвольным расширением.

Для того, чтобы использовать длинные имена файлов при работе с командной строкой, их нужно заключать в двойные кавычки. Например, чтобы запустить файл с именем 'Мое приложение.exe' из каталога 'Мои документы', нужно в командной строке набрать "C:\Мои документы\Мое приложение.exe" и нажать клавишу <Enter>.

2.1.6.2 Команда CD

Текущий каталог можно изменить с помощью команды CD [диск:][путь\]. Путь к требуемому каталогу указывается с учетом приведенных выше замечаний. Например, команда CD \ выполняет переход в корневой каталог текущего диска. Если запустить CD без параметров, то на экран будут выведены имена текущего диска и каталога.

2.1.6.3 Команда COPY

Одной из наиболее часто повторяющихся задач при работе на компьютере является копирование и перемещение файлов из одного места в другое. Для копирования одного или нескольких файлов используется команда COPY.

Синтаксис этой команды:

```
COPY [/A/B] источник [/A/B] [+ источник [/A/B] [+ ...]]
```

```
[результат [/A/B]] [/V]/[Y/-Y]
```

Параметры, ключи и их описание для команды COPY представлены в таблице 6.1

Таблица 2.1-Параметры и ключи команды COPY

Параметр	Описание
источник	Имя копируемого файла или файлов
/A	Файл является текстовым файлом ASCII, то есть конец файла обозначается символом с кодом ASCII 26 (<Ctrl>+<Z>)
/B	Файл является двоичным. Этот ключ указывает на то, что интерпретатор команд должен при копировании считывать из источника число байт, заданное размером в каталоге копируемого файла
результат	Каталог для размещения результата копирования и/или имя создаваемого файла
/V	Проверка правильности копирования путем сравнения файлов после копирования
/Y	Отключение режима запроса подтверждения на замену файлов
/-Y	Включение режима запроса подтверждения на замену файлов

Примеры использования команды COPY.

Копирование файла abc.txt из текущего каталога в каталог D:\PROGRAM под тем же именем:

`COPY abc.txt D:\PROGRAM`

Копирование файла abc.txt из текущего каталога в каталог D:\PROGRAM под новым именем def.txt:

`COPY abc.txt D:\PROGRAM\def.txt`

Копирование всех файлов с расширением txt с диска A: в каталог 'Мои документы' на диске C:

`COPY A:*.txt "C:\Мои документы"`

Если не задать в команде целевой файл, то команда COPY создаст копию файла-источника с тем же именем, датой и временем создания, что и исходный файл, и поместит новую копию в текущий каталог на текущем диске. Например, для того, чтобы скопировать все файлы из корневого каталога диска A: в текущий каталог, достаточно выполнить такую команду:

`COPY A:*.*`

Пример 1. Создание нового текстового файла и запись в него информации без использования текстового редактора.

Для решения задачи необходимо ввести команду `COPY CON my.txt`, которая копирует вводимые с клавиатуры символы в файл my.txt (если этот файл существовал, то он перезапишется, иначе — создастся). Для завершения ввода необходимо ввести символ конца файла нажатием клавиш <Ctrl>+<Z>.

Команда COPY может также объединять (склеивать) несколько файлов в один. Для этого необходимо указать единственный результирующий файл и несколько исходных. Это достигается путем использования групповых знаков (? и *) или формата файл1 + файл2 + файл3. Например, для объединения файлов 1.txt и 2.txt в файл 3.txt можно задать следующую команду:

`COPY 1.txt+2.txt 3.txt`

Объединение всех файлов с расширением dat из текущего каталога в один файл all.dat может быть произведено так:

`COPY /B *.dat all.dat`

Ключ /B здесь используется для предотвращения усечения соединяемых файлов, так как при комбинировании файлов команда COPY по умолчанию считает файлы текстовыми.

Если имя целевого файла совпадает с именем одного из копируемых файлов (кроме первого), то исходное содержимое целевого файла теряется. Если имя целевого файла опущено, то в его качестве используется первый файл из списка.

Например, команда `COPY 1.txt+2.txt` добавит к содержимому файла 1.txt содержимое файла 2.txt. Командой `COPY` можно воспользоваться и для присвоения какому-либо файлу **текущей даты и времени** без модификации его содержимого. Для этого нужно ввести команду

`COPY /B 1.txt +,,`

Здесь запятые указывают на пропуск параметра приемника, что и приводит к требуемому результату.

Команда `COPY` имеет ряд особенностей: с ее помощью нельзя копировать скрытые и системные файлы, файлы нулевой длины, файлы из подкаталогов. Кроме того, если при копировании группы файлов `COPY` встретит файл, который в данный момент нельзя скопировать (например, он занят другим приложением), то процесс копирования прервется, и остальные файлы не будут скопированы.

2.1.6.4 Команда `XCOPY`

Указанные при описании команды `COPY` проблемы можно решить с помощью команды `XCOPY`, которая предоставляет намного больше возможностей при копировании. Однако, `XCOPY` может работать только с файлами и каталогами, но не с **устройствами**.

Синтаксис команды: `XCOPY` источник [результат] [ключи]

Команда `XCOPY` имеет множество ключей, далее приведены лишь некоторых из них. Ключ `/D[:[дата]]` позволяет копировать только файлы, измененные не ранее указанной даты. Если параметр дата не указан, то копирование будет производиться только если источник новее результата. Например, команда `XCOPY "C:\Мои документы*.*" "D:\BACKUP\Мои документы" /D` скопирует в каталог 'D:\BACKUP\Мои документы' только те файлы из каталога 'C:\Мои документы', которые были изменены со времени последнего подобного копирования или которых вообще не было в 'D:\BACKUP\Мои документы'.

Ключ `/S` позволяет копировать все непустые подкаталоги в каталоге-источнике. С помощью же ключа `/E` можно копировать вообще все подкаталоги, включая и пустые.

Если указан ключ `/C`, то копирование будет продолжаться даже в случае возникновения ошибок. Это бывает очень полезным при операциях копирования, производимых над группами файлов, например, при резервном копировании данных.

Ключ `/I` важен для случая, когда копируются несколько файлов, а файл назначения отсутствует. При задании этого ключа команда `XCOPY` считает, что файл назначения должен быть каталогом. Например, если задать ключ `/I` в команде копирования всех файлов с расширением `txt` из текущего каталога в несуществующий еще подкаталог `TEXT`, `XCOPY *.txt TEXT /I` то подкаталог `TEXT` будет создан без дополнительных запросов.

Ключи `/Q`, `/F` и `/L` отвечают за режим отображения при копировании. При задании ключа `/Q` имена файлов при копировании не отображаются, ключа `/F` — отображаются полные пути источника и результата. Ключ `/L` обозначает, что отображаются только файлы, которые должны быть скопированы (при этом само копирование не производится).

С помощью ключа `/H` можно копировать скрытые и системные файлы, а с помощью ключа `/R` — заменять файлы с атрибутом "Только для чтения". Например, для копирования всех файлов из корневого каталога диска C: (включая системные и скрытые) в каталог `SYS` на диске D:, нужно ввести следующую команду:

`XCOPY C:*.* D:\SYS /H`

Ключ `/T` позволяет применять `XCOPY` для копирования только структуры каталогов источника, без дублирования находящихся в этих каталогах файлов, причем пустые каталоги и подкаталоги не включаются. Для того, чтобы все же включить пустые каталоги и подкаталоги, нужно использовать комбинацию ключей `/T /E`.

Используя XCOPY можно при копировании обновлять только уже существующие файлы (новые файлы при этом не записываются). Для этого применяется ключ /U. Например, если в каталоге C:\2 находились файлы a.txt и b.txt, а в каталоге C:\1 — файлы a.txt, b.txt, c.txt и d.txt, то после выполнения команды:

```
XCOPY C:\1 C:\2 /U
```

в каталоге C:\2 по-прежнему останутся лишь два файла a.txt и b.txt, содержимое которых будет заменено содержимым соответствующих файлов из каталога C:\1. Если с помощью XCOPY копировался файл с атрибутом "Только для чтения", то по умолчанию у файла-копии этот атрибут снимется. Для того, чтобы копировать не только данные, но и полностью атрибуты файла, необходимо использовать ключ /K.

Ключи /Y и /-Y определяют, нужно ли запрашивать подтверждение перед заменой файлов при копировании. /Y означает, что такой запрос нужен, /-Y — не нужен.

2.1.6.5. Команда DIR

Команда: DIR [диск:][путь][имя_файла] [ключи] используется для вывода информации о содержимом дисков и каталогов. Параметр [диск:][путь] задает диск и каталог, содержимое которого нужно вывести на экран. Параметр [имя_файла] задает файл или группу файлов, которые нужно включить в список.

Например, команда DIR C:*.bat выведет на экран все файлы с расширением bat в корневом каталоге диска C:. Если задать эту команду без параметров, то выводится метка диска и его серийный номер, имена (в коротком и длинном вариантах) файлов и подкаталогов, находящихся в текущем каталоге, а также дата и время их последней модификации. После этого выводится число файлов в каталоге, общий объем (в байтах), занимаемый файлами, и объем свободного пространства на диске.

Например:

```

Том в устройстве C имеет метку PHYS1_PART2
Серийный номер тома: 366D-6107
Содержимое папки C:\aditor
.      <ПАПКА>    25.01.15 17:15 .
..     <ПАПКА>    25.01.15 17:15 ..
HILITE DAT      1 082 18.09.16      18:55 hilite.dat
TEMPLT01 DAT    48 07.08.16      1:00 templt01.dat
TTABLE DAT      357 07.08.16      1:00 ttable.dat
ADITOR EXE     461 312 01.12.15     23:13 aditor.exe
README TXT      3 974 25.01.15     17:26 readme.txt
ADITOR HLP      24 594 08.10.16     23:12 aditor.hlp
ТЕКСТО~1 TXT      0 11.03.15     9:02 Текстовый файл.txt
    11 файлов      533 647 байт
     2 папок      143 261 696 байт свободно

```

С помощью ключей команды DIR можно задать различные режимы расположения, фильтрации и сортировки. Например, при использовании ключа /W перечень файлов выводится в широком формате с максимально возможным числом имен файлов или каталогов на каждой строке.

С помощью ключа /A[:]атрибуты можно вывести имена только тех каталогов и файлов, которые имеют заданные атрибуты (R — "Только чтение", A — "Архивный", S — "Системный", H — "Скрытый", префикс "-" имеет значение НЕ). Если ключ /A используется более чем с одним значением атрибута, будут выведены имена только тех файлов, у которых все атрибуты совпадают с заданными. Например, для вывода имен всех файлов в корневом

каталоге диска C:, которые одновременно являются скрытыми и системными, можно задать команду

```
DIR C:\ /A:HS
```

а для вывода всех файлов, кроме скрытых — команду

```
DIR C:\ /A:-H
```

Отметим здесь, что атрибуту каталога соответствует буква D, и для того, чтобы, например, вывести список всех каталогов диска C:, нужно задать команду

```
DIR C: /A:D
```

Ключ /O[:]сортировка] задает порядок сортировки содержимого каталога при выводе его командой DIR. Если этот ключ опущен, DIR печатает имена файлов и каталогов в том порядке, в котором они содержатся в каталоге. Если ключ /O задан, а параметр сортировка не указан, то DIR выводит имена в алфавитном порядке. В параметре сортировка можно использовать следующие значения: N — по имени (алфавитная), S — по размеру (начиная с меньших), E — по расширению (алфавитная), D — по дате (начиная с более старых), A — по дате загрузки (начиная с более старых), G — начать список с каталогов. Префикс "-" означает обратный порядок. Если задается более одного значения порядка сортировки, файлы сортируются по первому критерию, затем по второму и т.д.

Ключ /S означает вывод списка файлов из заданного каталога и его подкаталогов. Ключ /B перечисляет только названия каталогов и имена файлов (в длинном формате) по одному на строку, включая расширение. При этом выводится только основная информация. Например:

```
templt02.dat
UNINST1.000
hilite.dat
templt01.dat
UNINST0.000
ttable.dat
aditor.exe
readme.txt 23
aditor.hlp
Текстовый файл.txt
```

2.1.6.6 Команды MKDIR и RMDIR

Для создания нового каталога и удаления уже существующего пустого каталога используются команды MKDIR [диск:]путь и RMDIR [диск:]путь [ключи] соответственно (или их короткие аналоги MD и RD). Например:

```
MKDIR "C:\Примеры"
```

```
RMDIR "C:\Примеры"
```

Команда MKDIR не может быть выполнена, если каталог или файл с заданным именем уже существует. Команда RMDIR не будет выполнена, если удаляемый каталог не пустой.

2.1.6.7 Команда DEL

Удалить один или несколько файлов можно с помощью команды

```
DEL [диск:][путь]имя_файла [ключи]
```

Для удаления сразу нескольких файлов используются групповые знаки ? и *. Ключ /S позволяет удалить указанные файлы из всех подкаталогов, ключ /F — принудительно удалить файлы, доступные только для чтения, ключ /A[:]атрибуты] — отбирать файлы для удаления по атрибутам (аналогично ключу /A[:]атрибуты] в команде DIR).

2.1.6.8 Команда REN

Переименовать файлы и каталоги можно с помощью команды RENAME (REN).
Синтаксис этой команды имеет следующий вид:

REN [диск:][путь][каталог1|файл1] [каталог2|файл2]

Здесь параметр каталог1|файл1 определяет название каталога/файла, которое нужно изменить, а каталог2|файл2 задает новое название каталога/файла. В любом параметре команды REN можно использовать групповые символы ? и *. При этом представленные шаблонами символы в параметре файл2 будут идентичны соответствующим символам в параметре файл1. Например, чтобы изменить у всех файлов с расширением txt в текущей директории расширение на doc, нужно ввести такую команду:

REN *.txt *.doc

Если файл с именем файл2 уже существует, то команда REN прекратит выполнение, и произойдет вывод сообщения, что файл уже существует или занят. Кроме того, в команде REN нельзя указать другой диск или каталог для создания результирующих каталога и файла. Для этой цели нужно использовать команду MOVE, предназначенную для переименования и перемещения файлов и каталогов.

2.1.6.9 Команда MOVE

Синтаксис команды для перемещения одного или более файлов имеет вид:

MOVE [/Y|/Y] [диск:][путь]имя_файла1[,...] результирующий_файл

Синтаксис команды для переименования папки имеет вид:

MOVE [/Y|/Y] [диск:][путь]каталог1 каталог2

Здесь параметр результирующий_файл задает новое размещение файла и может включать имя диска, двоеточие, имя каталога, либо их сочетание. Если перемещается только один файл, допускается указать его новое имя. Это позволяет сразу переместить и переименовать файл. Например, MOVE "C:\Мои документы\список.txt" D:\list.txt.

Если указан ключ /-Y, то при создании каталогов и замене файлов будет выдаваться запрос на подтверждение. Ключ /Y отменяет выдачу такого запроса.

2.2. Задание на лабораторную работу

1. Изучить теоретический материал.
2. Запустить интерпретатор командной строки
3. Увеличить размер окна интерпретатора и задать цвет фона и цвет шрифта (Для этого следует использовать пункт Свойства управляющего меню окна, рекомендуется синий фон и белый шрифт). Выполнить все примеры из п 2.1
4. Создать текстовый файл, содержащий справочные сведения по командам DIR, COPY и XCOPY.
5. Вывести содержимое указанного в таблице 2.2 каталога по указанному формату на экран и в файл.

Замечание 1. При создании текстового файла интерпретатор командной строки использует кодировку **кириллица (DOS)**. Поэтому рекомендуется переназначить вывод в файл с расширением **.txt**, а для просмотра содержимого файла использовать Internet Explorer, указав вид кодировки **кириллица (DOS)**. Пример вывода содержимого текстового файла приведен на рис. 3.

Замечание 2. Интерпретатор хранит историю введенных команд в буфере (размером 50 строк). Для просмотра содержимого буфера используйте клавиши клавиатуры СТРЕЛКА

ВВЕРХ и СТРЕЛКА ВНИЗ. Полученную команду можно отредактировать и выполнить снова.

Таблица 2.2.-Варианты индивидуальных заданий

Варианты заданий для бригад Номера бригад	Имя каталога	Что выводить	Сортировать по	Атрибуты фай-лов и каталогов
1	Студент	Только файлы	По размеру	Системный
2	Студент	Файлы и подкаталоги	По дате	Скрытый
3	Студент	Только подкаталоги	По имени	Только чтение
4	Студент	Только файлы bmp	По размеру	Только чтение
5	Студент	Только файлы jpg	По имени	Любые
6	Студент	Только подкаталоги	По дате	Любые
7	Студент	Файлы и подкаталоги	По размеру	Любые
8	Студент	Только файлы pdf	По имени	Только чтение

3. ЛАБОРАТОРНАЯ РАБОТА №3. УПРАВЛЕНИЕ ФАЙЛАМИ В ОС WINDOWS

Цель работы: изучение возможностей интерпретатора командной строки ОС Windows, приобретение практических навыков работы в командном режиме.

3.1. Часть 1. Командный язык ОС

Диалог с ОС осуществляется в форме команд. Команда состоит из имени команды и параметров, разделенных пробелами. Имя команды MS-DOS и параметры могут набираться как прописными, так и строчными латинскими буквами. Ввод каждой команды заканчивается нажатием клавиши [ENTER].

Когда MS-DOS готова к диалогу с пользователем выдается приглашение:

A:\>

C:\>

Основные параметры любой команды можно узнать с помощью встроенной справки:

<имя команды> /?

Cls – очистка содержимого экрана. По этой команде с экрана будет удалена вся информация, и останется одно приглашение операционной системы.

Ver – выводит на экран название и версию ОС.

Vol – выводит на экран метку и серийный номер тома для диска. Под томом подразумевается логический диск. Если жёсткий диск не разбит на логические диски, то подразумевается сам диск.

Date – вывод на экран текущей системной даты и приглашение для ввода новой даты. Дата вводится в том формате, который предлагает операционная система. Например, формат (дд-мм-гг) означает, что надо ввести арабскими цифрами день-месяц-год (например, 11-01-07). *Дата вводится без скобок!*

Time – вывод на экран текущего системного времени и приглашение для ввода нового времени в том формате, который предлагает операционная система. Практически достаточно ввести только часы и минуты через двоеточие (например, 12:45).

Некоторые команды имеют ключи, расширяющие возможности команды. Ключи записываются после имени команды и последующего за ним прямого слэша (символ /). Так, например, для всех команд существует ключ “?” (знак вопроса без кавычек). По данному ключу на экран выводится назначение команды, формат её записи и дополнительные ключи данной команды.

3.1.1. Работа с файлами и папками

Создание текстовых файлов: **copy con** (дискковод:) (\ путь\) имя_файла

После ввода команды построчно вводится текст, в конце каждой строки нажимается клавиша *Enter*, а после ввода последней строки – клавиши *F6* и затем *Enter*. Команда выведет сообщение: « 1 file(s) copied» (один файл скопирован) и на диске появится файл с указанным в команде именем.

Удаление файлов: **del** (дискковод:) (\ путь\) имя_файла

Перед удалением файла выводится имя файла и запрос «Delete (Y/N)?». При нажатии клавиши *Y* файл будет удалён, при нажатии *N* удаление отменяется.

Переименование файлов:

ren (дискковод:)(\ путь\) имя_файла_1 имя_файла_2

В результате выполнения команды имя файла_1 заменяется именем файла_2. Эта команда не обрабатывает файлы с атрибутом «скрытый».

Копирование файлов:

copy (дискковод:)(\путь\) **имя_файла_1** (дискковод:)(\путь\) **имя_файла_2**

В результате выполнения команды файл 1 копируется на место файла 2. Если файл с таким же именем, как у копии, уже существует, то он замещается без каких-либо предупреждений. Файлы с атрибутом «скрытый» не копируются. В этой команде вместо имён файлов можно использовать обозначения устройств *DOS* (клавиатуры, монитора, принтера). Если эта команда используется для объединения содержимого нескольких файлов, то вместо параметра «имя файла 1» перечисляются через знак «+» имена объединяемых файлов, а затем имя файла, в которое копируется содержимое объединяемых файлов.

Редактирование файла **edit** (дискковод:)(\путь\) **имя_файла**

Вывод файла на экран: **type** (дискковод:)(\путь\) **имя_файла**

Команда смены текущего дисковод: имя дисковода и двоеточие (**d:**)

Изменение текущего каталога: **cd** (дискковод:)(\путь\) **имя_каталога**

Если задан дисковод, то текущий каталог изменяется на этом дисководе, иначе - на текущем дисководе. Если в команде отсутствуют параметры, то в результате выполнения сообщаются текущие диск и каталог. Для перехода в каталог на другом диске нужно ввести команду перехода на другой диск и затем данную команду для изменения текущего каталога. Выход из каталога на уровень выше **cd..**

Просмотр каталога: **dir** (дискковод:)(\путь\) (**имя_файла**) (**параметры**)

Если имя файла не задано, то выводится всё оглавление каталога. Управление выводом сведений о каталоге осуществляется с помощью многочисленных параметров команды (например, **/P** – по-экранный вывод оглавления с паузами при заполнении экрана).

Параметры:

filename - имя файла или файлов;

/O:order - сортировка каталога: (**D** - сортировка по дате, **E** - сортировка по расширению; **N** - сортировка по имени; **S** - сортировка по размеру);

/B - вывести имена файлов и подкаталогов;

/P - поэкранный вывод;

/S - просмотр подкаталогов;

/W - вывод в широком формате.

Комментарий: ключ **/S** дает возможность искать файлы в пределах всего диска. Пример **DIR *.BAK /S /B** - вывод указанных файлов в пределах всего диска.

Создание каталога: **md** (дискковод:)(\путь\) **имя_каталога**

Удаление пустого каталога: **rd** (дискковод:)(\путь\) **имя_каталога**

Удаление каталога со всем содержимым:

rd /S (дискковод:)(\путь\) **имя_каталога**

Если параметр **/Q** не указан, то выдаётся запрос на подтверждение удаления каталога, иначе - удаление выполняется без запросов.

Переименование каталога: **ren** **имя_каталога** **новое_имя_каталога**

У старого имени можно указать диск и путь и тем самым переименовывать не только подкаталоги текущего каталога, но и других каталогов.

Структура папок: **tree** (дискковод:)(\путь\)- графическое отображение структуры папок заданного диска или заданной папки.

При подаче некоторых команд (**dir**, **copy**, **del**) в командной строке допускается использовать символы «?» и «*» (их можно использовать в имени и типе файла). При этом символ «?» будет рассматриваться как один из символов, допустимых в данной команде, а символ «*» заменяет собой произвольное число любых допустимых в данной команде символов. Например, командой «**del c:\dos\k1?.***» удалятся все файлы с любым расширением (в том числе и без него) в каталоге *DOS* на диске C:, имена которых состоят из 3-х символов (причем первые два – **k1**, а третий - произвольный из допустимых).

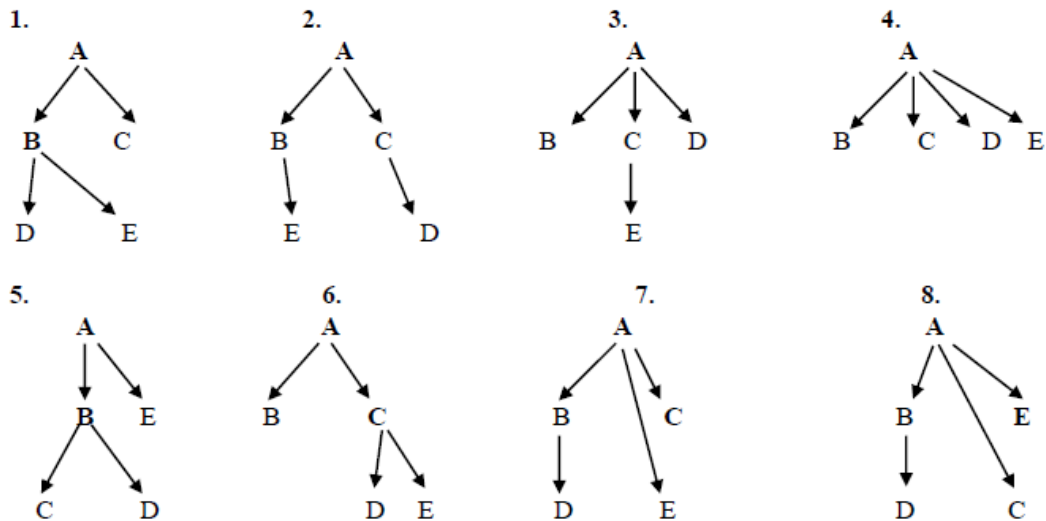
Вызов справки: *help*

Выводит справочную информацию о доступных внешних командах

3.2. Задание на лабораторную работу(часть 1)

1. Запустить командный интерпретатор.
1. Очистить экран (CLS).
- 2.1 Вывести на экран название и версию ОС.
- 2.2 Вывести на экран метки и серийные номера томов (логических дисков).
- 2.3 Вести настоящую дату и настоящее время и вывести их на экран, используя специальный ключ команды (определить его в результате запроса).
2. Через командную строку зайти в каталог Temp диска C.
3. В каталоге Temp создать дерево каталогов в соответствии с вариантом (рисунок 3.1). Отобразить графическую структуру на экране.
4. В каталоге A создать подкаталоги A1 и A2 , в каталоге B- подкаталог B2.
5. В каталоге B создать файл Name.txt, содержащий информацию о студентах (ФИО). Здесь же создать файл Date.txt, содержащий информацию о датах рождения студентов.
6. В каталоге C создать файл Name.txt, содержащий информацию о названии Вуза и специальность, на которой студент обучается. Здесь же создать файл Mark.txt с оценками на вступительных экзаменах и общей суммой баллов.
7. В каталоге E создать файл hobby.txt с информацией об увлечениях студентов.
8. Скопировать файл hobby.txt в каталог A2 и переименовать его в файл Lab_№варианта.txt.
9. Сделать копию файла Lab_№варианта.txt (например, copy_Lab_№варианта.txt) в этом же каталоге.
10. Вывести на экран информацию, хранящуюся в одном из файлов каталога C.
11. Отсортировать все файлы, хранящиеся в каталоге C, по имени.
12. Объединить все файлы, хранящиеся в каталоге C, в файл all.txt и вывести его содержимое на экран.
13. Отредактировать файл all.txt, добавив в него год вашего рождения, и вывести его содержимое на экран.
14. Скопировать файл all.txt в директорию D.
15. Удалить все директории, в названии которых есть буква A или цифра 2.
16. Удалить все оставшиеся файлы и папки.

Варианты иерархии каталогов



3.3. Часть 2. Теоретические сведения

Файл — это упорядоченная совокупность данных, хранящаяся на диске и занимающая поименованную область внешней памяти. Имя файла состоит из имени и расширения файла. Популярные форматы расширений в Windows:

- .txt, .doc – текстовые документы, в том числе документы приложения Word;
- .rar, .zip – архивные файлы;
- .exe, .com – программы и утилиты;
- .jpg, .bmp, .gif, .tiff – цифровые фотографии, изображения;
- .htm, .php – Web-страницы;
- .hlp – справочные файлы;
- .avi, .mpg, .wmv, .mkv – видеофайлы;
- .xls – электронные таблицы приложения Excel.

При установке или работе программ создаются временные файлы Windows с расширением .tmp. После завершения установки или работы такие временные файлы удаляются автоматически, но это происходит не всегда. Большое количество временных файлов может замедлять работу компьютера, поэтому их рекомендуется удалять вручную.

Для организации эффективной работы с данными, хранящимися в памяти, предназначена файловая система. Файловая система – это набор спецификаций и соответствующее им программное обеспечение, которое отвечает за создание, удаление, организацию, чтение, запись, модификацию и перемещение файлов информации, а также за управление доступом к файлам и за управление ресурсами, которые используются файлами. Файловая система определяет способ организации данных на диске и принципы хранения данных на физическом носителе. Файловая система должна обеспечивать:

- 1) безопасное и надежное хранение данных (т. е. защищенное от несанкционированного использования и различного рода сбоев и ошибок);
- 2) программный интерфейс доступа к файлам;
- 3) организацию файлов в виде иерархии каталогов.

С точки зрения операционной системы, жесткий диск – это набор кластеров. **Кластер** – область диска определенного размера для хранения данных. Том или логический диск – область внешней памяти, с которой операционная система работает как с единым целым.

В ОС Windows 7 доступны следующие файловые системы: NTFS, FAT32 и редко используемая система FAT (FAT16).

В NTFS (файловая система новой технологии, основная файловая система ОС Windows) размер кластера равен 4Кб, размер тома не более 2ТБ. Структурой NTFS предусмотрено хранение для каждого файла и каждой папки специального блока безопасности, который содержит следующую информацию:

- идентификатор (имя) пользователя, создавшего файл;
- список контроля доступа, в котором перечислены разрешения доступа к файлу или папке для пользователей и групп;
- системный список контроля доступа, в котором перечислено, какие действия (например, чтение, запись и т.п.) для каких пользователей и групп необходимо фиксировать в журнале аудита.

NTFS, поддерживает защиту файлов и каталогов; сжатие файлов; поддержка многопоточных файлов; отслеживание связей; шифрование.

FAT (таблица размещения файлов) - линейная табличная структура со сведениями о файлах – именами файлов, их атрибутами и другими данными, определяющими местоположение файлов или их фрагментов в среде FAT, размер кластера 32Кб. Элемент FAT определяет фактическую область диска, в котором хранится начало физического файла. В файловой системе FAT логическое дисковое пространство любого логического диска состоит из двух областей:

- системная область – создается при форматировании диска и обновляется при манипулировании файловой структурой;
- область данных – содержит файлы и каталоги, подчиненные корневому каталогу, доступна через пользовательский интерфейс.

3.4. Задание на лабораторную работу(часть 2)


3.4.1. Определение типа файловой системы.

Открыть папку «Компьютер», выбрать диск С:, кликнуть его правой кнопкой мышки и выбрать в контекстном меню пункт «Свойства». В открывшемся окне на вкладке «Общие» сверху будет указан тип диска и используемая файловая система. Например, для Windows 7 будет указан тип файловой системы NTFS.

Определить тип файловой системы диска С:. Вставить флэш-накопитель и определить тип диска и используемую файловую систему для съемного диска

3.4.2. Отображение расширений файлов

Если дважды щелкнуть мышью на имени файла со значком, будет запущена программа *Word*, в которой, в свою очередь, откроется выбранный файл. Задача *Windows* состоит в том, чтобы обработать файл согласно его расширению. При этом имя файла может быть любым. Расширения файлов не отображаются по умолчанию в *Windows 7*. Чтобы это сделать, необходимо выполнить следующие действия.

1. Открыть раздел «Параметры папок». Для этого нажать кнопку *Пуск* , выбрать последовательно компоненты *Панель управления*, и *Параметры папок*.

2. Перейти на вкладку *Вид* и в разделе *Дополнительные параметры* выполнить одно из следующих действий.

- Для отображения расширения имен файлов, снять флажок *Скрывать расширения для зарегистрированных типов файлов* и нажать кнопку ОК.
- Для сокрытия расширения имен файлов, установить флажок *Скрывать расширения для зарегистрированных типов файлов* и нажать кнопку ОК.

Выполнить действия по отображению расширений файлов.

3.4.3. Отображение скрытых папок и файлов

Наряду с обычными файлами в *Windows* есть системные файлы. Эти файлы содержат программы и данные, отвечающие за работу операционной системы. Поэтому изменять,

переименовывать, удалять их ни в коем случае нельзя. Располагаются системные файлы в папке *Windows*, в которую проводится установка операционной системы, а также в некоторых других папках. Основные системные файлы по умолчанию скрыты для просмотра. Чтобы их увидеть, в окне *Параметры папок*, на вкладке *Вид* в разделе *Дополнительные параметры* нужно установить флажок *Показывать скрытые папки, файлы и диски*. Системные файлы защищены от перезаписи.

ВНИМАНИЕ! Удаление или изменение системных файлов может привести к тому, что ОС перестанет запускаться или будет работать с ошибками.

Отобразить скрытые файлы и папки

3.4.4. Свойства файлов и папок

Чтобы просмотреть свойства определенного файла, необходимо щелкнуть правой кнопкой мыши на значке файла и в появившемся контекстном меню выбрать команду **Свойства**. При этом на экране появится окно с несколькими вкладками, каждая из которых позволит указать для файла различные параметры. Количество вкладок и их содержимое зависит непосредственно от параметров самого файла. Окно **Свойства** открывается на вкладке **Общие** (Рисунок 3.1).

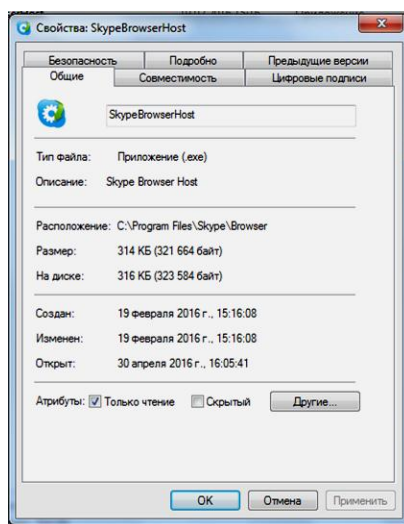


Рисунок 3.1. - Окно свойств файла, вкладка «Общие»

Вверху этой вкладки указывается имя файла, которое при желании можно изменить. В поле **Приложение** указывается программа, которая используется для открытия файла с данным расширением.

Если файл сам является программой, то для него этот раздел отсутствует. Далее на вкладке **Общие** последовательно указываются местоположение и размер файла, его размещение на диске, дата создания и последней модификации, а также дата последнего открытия.

Вкладка **Подробно** (Рисунок 3.2) окна **Свойства** содержит общие сведения о файле. То, какие сведения отображаются, зависит от типа файлов. Например, если это текстовый файл, то на вкладке **Подробно** будут отображена информация о количестве страниц, слов, знаков, имени автора и прочие сведения.

Внизу вкладки **Общие** с помощью флажков можно указать свойства (или, другими словами, атрибуты) файлов. Свойство **Только чтение** позволяет сделать файл доступным только для чтения, т.е. содержимое такого файла можно будет лишь просматривать или печатать. Удалить или изменить подобный файл нельзя. Если установить флажок **Скрытый**, то файл станет невидимым для обычного просмотра. Флажок **Архивный** будет присутствовать только в том случае, если используется файловая система FAT32. Если используется файловая система NTFS, то вместо флажка **Архивный** будет расположена

кнопка *Другие* (атрибуты сжатия и шифрования). Щелкнув на этой кнопке, можно в новом окне изменить различные параметры, связанные с файловой системой NTFS.

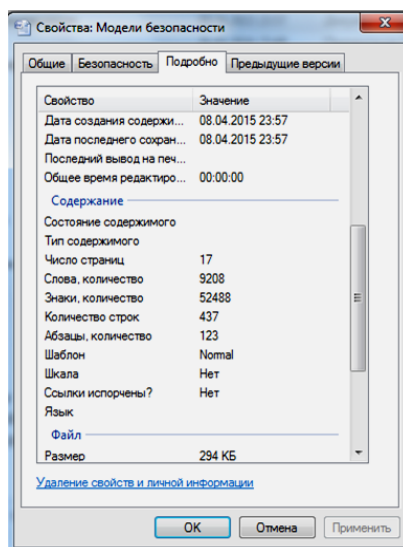


Рисунок 3.2.- Окно свойств файла, вкладка «Подробно»

Окно свойств папки вызывается из контекстного меню после щелчка правой кнопкой мыши по значку папки и содержит вкладки *Общие*, *Доступ*, *Безопасность*, *Настройка*.

Просмотреть и выписать свойства текстового файла Word, рабочей книги Excel, свойства папки, расположенные на разных вкладках окна «Свойства».

3.4.5. Удаление временных файлов

Если система установлена на диск "C:", то адрес нахождения первой папки с временными файлами Windows - C:\Windows\Temp\ . Вторая папка Temp в Windows 7 находится по адресу: C:\Users\Имя пользователя\AppData\Local\AppData и имеет свойство скрытой папки. Увидеть её можно только включив отображение скрытых файлов и папок.

Самым простым способом избавиться от временных файлов является программа «Очистка диска», которая встроена в Windows. Чтобы запустить её, нужно нажать левой кнопкой мыши на диск C: в разделе «Компьютер», выбрать пункт «Свойства» и во вкладке «Общие» кликнуть по кнопке «Очистка диска». Поставить галочку «Временные файлы», затем нажать «ОК».

Удалить временные файлы из папок Temp можно вручную. Для того, чтобы найти вторую папку Temp, нужно отобразить скрытые файлы и папки. Находим в меню «Панель управления» и выбираем «Параметры папок». Во вкладке «Вид» в окне «Дополнительные параметры» выбираем «Показывать скрытые файлы, папки и диски» и жмем «ОК». Вторая папка находится по адресу C:\Users\Имя пользователя\AppData\Local\Temp.

Также можно зайти в «Пуск» — «Выполнить» и ввести %TEMP%, после чего нажать *Enter*. Выделить файлы в этой папке (Ctrl+A) и удалить. Причем может случиться так, что появится сообщение, что некоторые файлы нельзя удалить. Это нормально, потому что некоторые из них могут использоваться системой в данный момент. Нажать «ОК».

Удалить временные файлы с помощью программы *Очистка диска* и вручную.

4.ЛАБОРАТОРНАЯ РАБОТА № 4. ЗАЩИТА УЧЁТНЫХ ЗАПИСЕЙ И ДАННЫХ В ОС WINDOWS

Цель работы: ознакомление с инструментами ограничения возможных действий пользователей и групп путем назначения им прав и разрешений.

4.1 Теоретические сведения

Локальная политика безопасности регламентирует правила безопасности на локальном компьютере. С ее помощью можно распределить административные роли, конкретизировать привилегии пользователей, назначить правила аудита.

По умолчанию поддерживаются следующие области безопасности:

- политика безопасности – задание различных атрибутов безопасности на локальном и доменном уровнях; так же охватывает некоторые установки на машинном уровне;
- управление группами с ограничениями – позволяет управлять членством в группах, которые, по мнению администратора, "чувствительны" с точки зрения безопасности системы;
- управление правами и привилегиями – позволяет редактировать список пользователей и их специфических прав и привилегий.

Все инструменты по настройке операционной системы и ее элементов объединены в одну группу, которую называют *Панелью управления*.

Консоль *Управление компьютером* на Панели управления помогает решать следующие задачи.

- Управление пользователями и группами пользователей.
- Управление совместно используемыми устройствами и дисками.
- Проверка системных журналов событий, содержащих информацию о входе пользователей в систему и ошибках в работе приложений.
- Наблюдение за удаленными пользователями, подключенными к системе.
- Мониторинг работы системных служб, запуск и остановка их работы, а также назначение для них времени автоматического запуска.
- Проверка распределения ресурсов системы, выявление конфликтов устройств и проверка установленного оборудования.
- Настройка запоминающих устройств.
- Просмотр конфигурации аппаратного обеспечения и установка новых драйверов.
- Управление серверными приложениями и службами.

Учетная запись пользователя — перечень сведений, определяющих персональные настройки компьютера, права доступа к файлам и директориям в файловой системе, права пользователя на изменение работы компьютера (глобальные настройки Windows, установка и удаление программ и тому подобное). Для идентификации пользователя в системе используется имя его учетной записи (логин) и пароль.

Учетные записи пользователей в Windows бывают трех типов: администратор, стандартная, гость. Учетная запись администратора предоставляет полный доступ к управлению компьютером. Стандартная учетная запись - пользователь может запускать и работать в большинстве программ, а также изменять настройки операционной системы, которые не влияют на настройки других пользователей или безопасность компьютера. Учетная запись гость, предназначена для предоставления временного доступа к компьютеру постороннего человека и обладает наименьшими правами.

Существует понятие группа пользователей. Для удобства администрирования компьютера учетные записи с одинаковыми правами помещают в одну группу и права задаются для всей группы, а не для каждого пользователя отдельно. В windows по умолчанию есть группа администраторов и группа стандартные пользователи.

Администратор может создавать новые группы, задавать их права и перемещать пользователей между группами. Один пользователь может входить сразу в несколько групп.

С помощью локальных (групповых) политик возможно управлять использованием внешних запоминающих устройств.

Контроль использования информации, перемещаемой за периметр локальной сети компании, — одна из главных задач службы информационной безопасности. С каждым годом эта работа все усложняется. Резко возросло число всевозможных USB-накопителей и их объем (диски в 4 Гбайт уже давно не редкость); переносные MP3-плееры с жестким диском, фотоаппараты, мобильные телефоны — все они имеют большой объем памяти. Для использования режима контроля над применением внешних носителей в Windows 7 администратор должен задействовать групповые (локальные) политики. При помощи групповых политик он может указать конкретные устройства, использование которых на данном компьютере разрешено.

Каждое устройство, использующее USB-порт, обладает так называемым уникальным цифровым идентификатором. То есть для создания списка разрешенных устройств нужно перечислить идентификаторы (ID) этих устройств.

4.2 Задание на лабораторную работу

1. Создать на диске **С:** новую папку с именем «NoAccess» (Нет доступа).
2. Выполнить команду *Пуск > Панель управления > Администрирование > Управление компьютером*. Откроется окно «Управление компьютером» (рисунке 3.1).

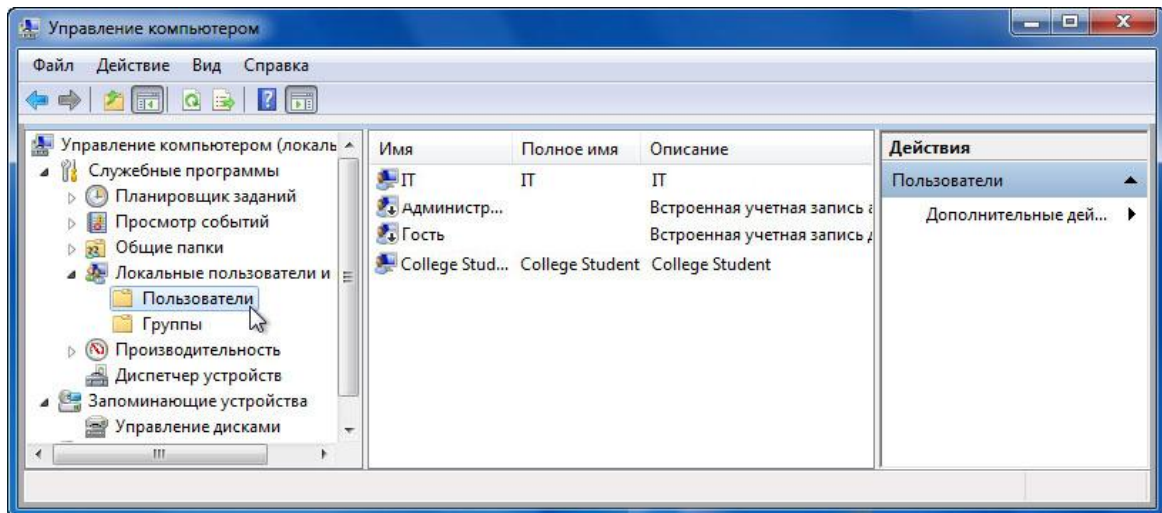


Рисунок 4.1. Окно «управление компьютером»

Раскрыть список *Локальные пользователи и группы > выбрать пункт Пользователи*. Щёлкнуть правой кнопкой мыши *Гость > Свойства > разместить флажок рядом с пунктом Отключить учетную запись > ОК*. Посмотреть на значок учётной записи гостя, вернуть ее в исходное состояние.

3. Щёлкнуть правой кнопкой мыши открытую область на средней панели окна «Управление компьютером». Из контекстного меню выбрать пункт меню *Новый пользователь*. Откроется окно «Новый пользователь» (рис.2.2).

Ввести следующие данные учётной записи:

Имя пользователя: Nov_Polz.

Полное имя: Nov_Polz.

Описание: Student.

Пароль и подтверждение пароля: Tc!15Kwz.

Снять флажок *Требовать смены пароля при следующем входе в систему*.

Установить флажок *Запретить смену пароля пользователем*.

Последовательно нажать кнопки *Создать* > *Заккрыть*.

Рисунок 4.2. - Окно «Новый пользователь»

4. В левой части окна «Управление компьютером» развернуть стрелку рядом с пунктом *Локальные пользователи и группы* и выбрать пункт *Группы*. Щёлкнуть правой кнопкой мыши открытую область на средней панели и выбрать пункт *Создать группу*. Откроется окно «Новая группа».

Рисунок 4.3. - Окно «Выбор: Пользователи»

Ввести следующую информацию:

Имя группы: Temp Account (Временная учётная запись)

Описание: Temporary Users (Временные пользователи)

Нажать кнопку *Добавить*. Откроется окно «Выбор: Пользователи» (рис.3.3).

В поле *Введите имена выбираемых объектов* ввести Nov_Polz, нажать кнопку ОК. Откроется окно «Новая группа». В этом окне последовательно нажать кнопки *Создать* (ОК) > *Заккрыть*. Дважды щёлкнуть группу *Пользователи*. Нажать кнопку *Отмена*, чтобы закрыть окно. Закрыть все открытые окна.

5. Перейти к папке No Access (Нет доступа) и щёлкнуть её правой кнопкой мыши, затем из контекстного меню выбрать *Свойства* > вкладка *Безопасность* > *Изменить* > *Добавить*. Откроется окно «Выбор: "Пользователи" или "Группы"» (рис.2.4). Ввести Temp Account (Временная учётная запись). Users (Пользователи) > ОК.

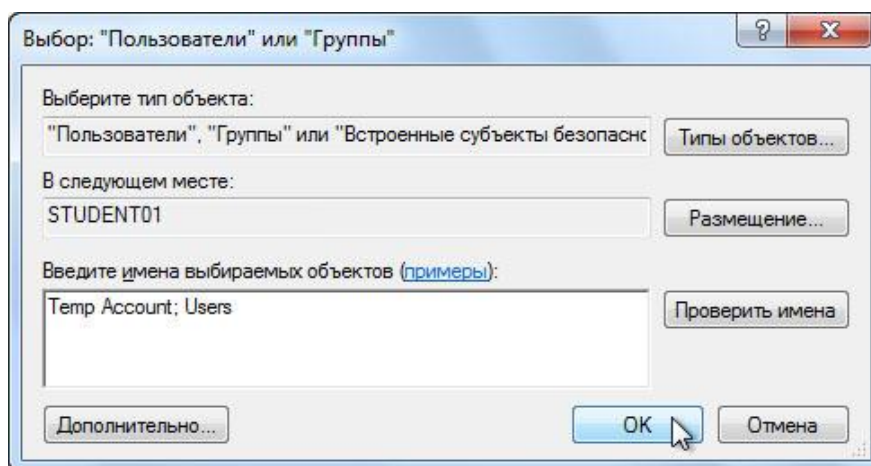


Рисунок 4.4. - Окно «Выбор: "Пользователи" или "Группы"»

Откроется окно разрешений для "No Access" (Нет доступа). Выбрать группу *Temp Account* (Временная учётная запись) (рис.3.5)

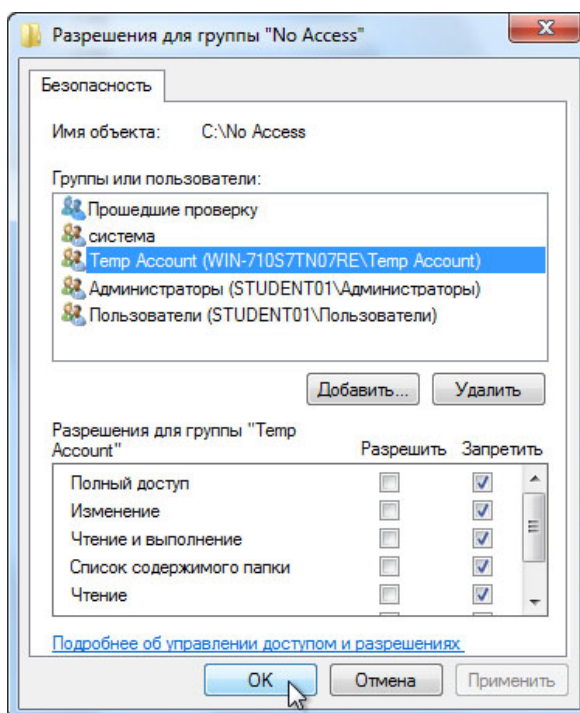


Рисунок 4.5. - Окно разрешений

Выбрать *Запретить* для полного управления. Нажать кнопку ОК. Откроется окно «Безопасность Windows». Нажать кнопку *Да*, затем кнопку ОК, чтобы закрыть окно «Свойства папки "No Access"». Закрыть все открытые окна.

6. Завершить сеанс на компьютере и начать новый сеанс как Nov_Polz. Выбрать *Пуск > Компьютер > Локальный диск (C:) >* дважды щёлкнуть папку «NoAccess» (Нет доступа). Посмотреть, Возможен ли доступ к папке из учётной записи? Закрыть все открытые окна.

7. Для получения ID флэш-накопителя нужно подсоединить его к USB-порту, в окне «Компьютер» щелкнуть правой кнопкой мыши по значку съемного диска, в контекстном меню выбрать пункт «Свойства», вкладка «Оборудование». Нажать кнопку «Свойства» и перейти на вкладку «Сведения» (рис.3.6).

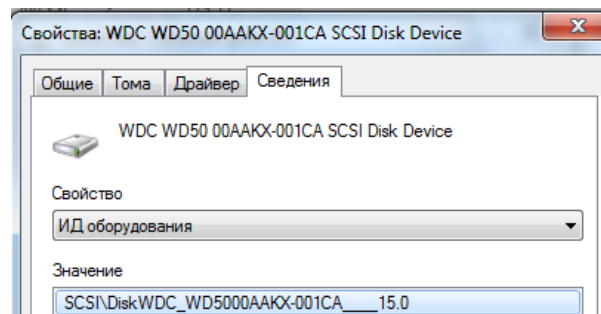


Рисунок 4.6. - Идентификатор устройства

В раскрывающемся списке «Свойство» выбрать «ИД оборудования» и запомнить значение параметра в текстовом редакторе.

После получения уникального ID устройства перейти к настройке групповых политик. Для настройки групповых политик в режиме командной строки запустить команду `gpedit.msc`. В появившемся окне групповых политик выбрать *Конфигурация компьютера—Административные шаблоны—Система— Установка устройств – Ограничения на установку устройств* (рис.3.7)

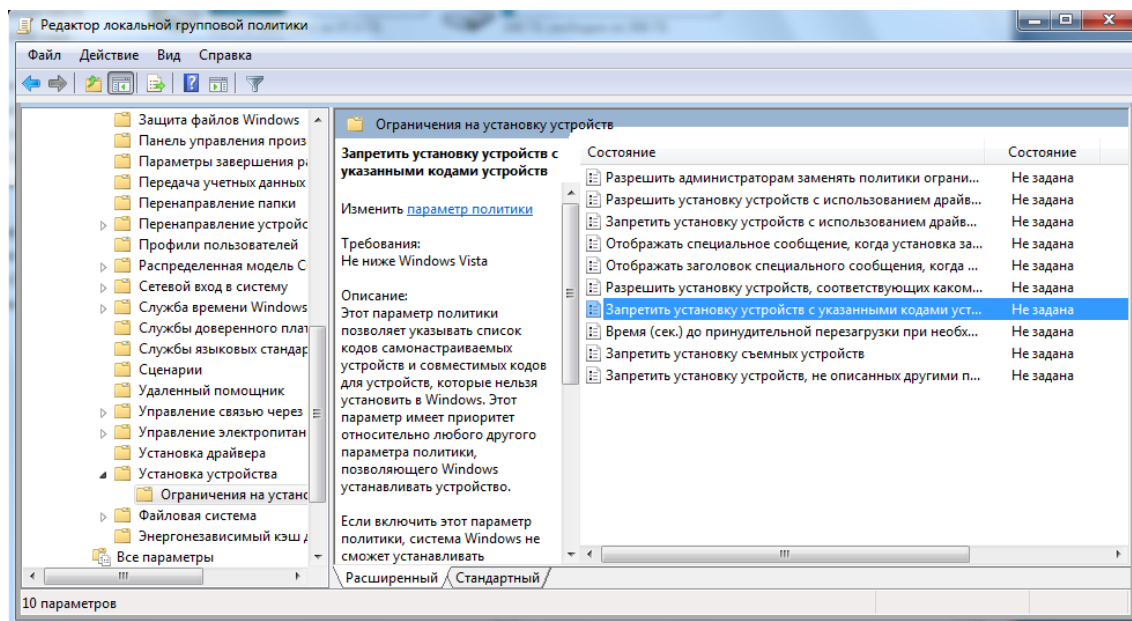


Рисунок 4.7-Редактор групповой локальной политики

В левой части окна редактора групповой локальной политики выбрать пункт *Запретить установку устройств с указанными кодами*, двойным щелчком открыть окно, установить переключатель *Включить*, нажать кнопку *Показать*, в появившемся поле ввести ИД оборудования, нажать ОК, затем кнопку *Применить*.

8. Щёлкнуть правой кнопкой мыши *Рабочий стол > Персонализация > Экранная заставка*. Откроется окно «Параметры экранной заставки». Выбрать экранную заставку из раскрывающегося списка и установить флажок *Начинать с экрана входа в систему*. Значение параметра «Интервал» должно быть установлено равным 1 минуте. Нажать кнопку ОК и подождать одну минуту.

9. Перейти опять к окну «Параметры экранной заставки». Установить экранную заставку на (Нет) и снять флажок *Начинать с экрана входа в систему* и нажмите кнопку «ОК». Завершить сеанс на компьютере.

Начать сеанс на компьютере с правами администратора. Выбрать *Пуск > Компьютер > Локальный диск (C:)*. Правой кнопкой мыши щёлкнуть папку No Access (Нет доступа) и последовательно нажать кнопки *Удалить > Да*. Последовательно выбрать *Пуск > Панель*

управления > Администрирование > Управление компьютером, развернуть стрелку рядом с пунктом *Локальные пользователи и группы*. Выбрать *Пользователи*, после чего щёлкнуть правой кнопкой мыши Nov_Polz, нажать кнопку *Удалить* > Да. Щёлкнуть правой кнопкой мыши учётную запись Гость, щёлкнуть *Свойства*, снять флажок *Отключить учетную запись* и нажать кнопку «ОК». Выбрать *Группы*, после чего щёлкнуть правой кнопкой мыши Temp Account (Временная учётная запись) и нажать кнопку *Удалить* > Да.

4.3 Содержание отчета

Цель работы; постановка задачи; описание выполнения заданий п.3.2, результаты выполнения заданий, выводы по работе.

4.4 Контрольные вопросы

- 1) Что такое учетная запись пользователя?
- 2) Виды учетных записей в Windows.
- 3) Какие задачи помогает решать консоль «Управление компьютером»?
- 4) Что такое политика безопасности?
- 5) Как создать учетную запись нового пользователя?
- 6) Как запретить использование флэш-накопителя?

5. ЛАБОРАТОРНАЯ РАБОТА №5. УПРАВЛЕНИЕ ПАМЯТЬЮ И ВВОДОМ/ВЫВОДОМ В ОС WINDOWS

Цель работы: Практическое знакомство с управлением вводом/выводом в ОС Windows и кэширования операций ввода/вывода.

5.1. Краткие теоретические сведения

Необходимость обеспечить программам возможность осуществлять обмен данными с внешними устройствами и при этом не включать в каждую двоичную программу соответствующий двоичный код, осуществляющий собственно управление устройствами ввода/вывода, привела разработчиков к созданию системного программного обеспечения и, в частности, самих операционных систем.

Программирование задач управления вводом/выводом является наиболее сложным и трудоемким, требующим очень высокой квалификации. Поэтому код, позволяющий осуществлять операции ввода/вывода, стали оформлять в виде системных библиотечных процедур; потом его стали включать не в системы программирования, а в операционную систему с тем, чтобы в каждую отдельно взятую программу его не вставлять, а только позволить обращаться к такому коду. Системы программирования стали генерировать обращения к этому системному коду ввода/вывода и осуществлять только подготовку к собственно операциям ввода/вывода, то есть автоматизировать преобразование данных к соответствующему формату, понятному устройствам, избавляя прикладных программистов от этой сложной и трудоемкой работы. Другими словами, системы программирования вставляют в машинный код необходимые библиотечные подпрограммы ввода/вывода и обращения к тем системным программным модулям, которые, собственно, и управляют операциями обмена между оперативной памятью и внешними устройствами.

Таким образом, управление вводом/выводом — это одна из основных функций любой ОС. Одним из средств правления вводом/выводом, а также инструментом управления памятью является диспетчер задач Windows, он отображает приложения, процессы и службы, которые в текущий момент запущены на компьютере. С его помощью можно контролировать производительность компьютера или завершать работу приложений, которые не отвечают.

При наличии подключения к сети можно также просматривать состояние сети и параметры ее работы. Если к компьютеру подключились несколько пользователей, можно увидеть их имена, какие задачи они выполняют, а также отправить им сообщение.

Также управлять процессами можно и «вручную» при помощи командной строки.

Команды Windows для работы с процессами:

- at — запуск программ в заданное время
- Schtasks — настраивает выполнение команд по расписанию
- Start — запускает определенную программу или команду в отдельном окне.
- Taskkill — завершает процесс
- Tasklist — выводит информацию о работающих процессах

Для получения более подробной информации, можно использовать центр справки и поддержки или команду help (например: help at)

- command.com — запуск командной оболочки MS-DOS
- cmd.exe — запуск командной оболочки Windows

5.2 Задание на лабораторную работу

Часть 1. Работа с Диспетчером задач Windows 7.

1. Запустите Windows 7

2. Запуск диспетчера задач можно осуществить двумя способами:

1) Нажатием сочетания клавиш Ctrl+Alt+Del. При использовании данной команды не стоит пренебрегать последовательностью клавиш. Появится меню, в котором курсором следует выбрать пункт «Диспетчер задач».

2) Переведите курсор на область с показаниями системной даты и времени и нажмите правый клик, будет выведено меню, в котором следует выбрать «Диспетчер задач».

3. Будет выведено окно как на рис. 5.1.

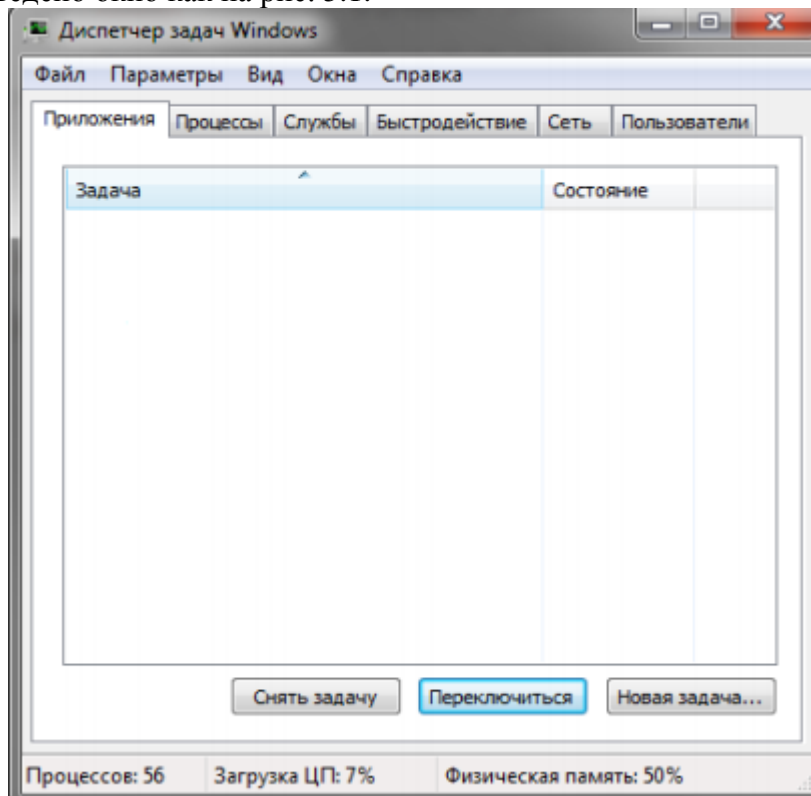


Рис. 5.1.- Диспетчер задач Windows 7.

В диспетчере задач есть 6 вкладок:

1. Приложения
2. Процессы
3. Службы
4. Быстродействие
5. Сеть
6. Пользователи

- Вкладка «Приложения» отображает список запущенных задач (программ) выполняющиеся в настоящий момент не в фоновом режиме, а также отображает их состояние. Также в данном окне можно снять задачу переключиться между задачами и запустить новую задачу при помощи соответствующих кнопок.

- Вкладка «Процессы» отображает список запущенных процессов, имя пользователя запустившего процесс, загрузку центрального процессора в процентном соотношении, а также объем памяти используемого для выполнения процесса. Также присутствует возможность отображать процессы всех пользователей, либо принудительного завершения процесса. Процесс — выполнение пассивных инструкций компьютерной программы на процессоре ЭВМ.

- Вкладка «Службы» показывает, какие службы запущены на компьютере. Службы — приложения, автоматически запускаемые системой при запуске ОС Windows и выполняющиеся вне зависимости от статуса пользователя.

- Вкладка «Быстродействие» отображает в графическом режиме загрузку процессора, а также хронологию использования физической памяти компьютера. Очень эффективным инструментом наблюдения является «Монитор ресурсов». С его помощью можно наглядно наблюдать за каждой из сторон «жизни» компьютера. Подробное изучение инструмента произвести самостоятельно, интуитивно.
- Вкладка «Сеть» отображает подключенные сетевые адаптеры, а также сетевую активность.
- Вкладка «Пользователи» отображает список подключенных пользователей.
- Потренируйтесь в завершении и повторном запуске процессов.
- Разберите мониторинг загрузки и использование памяти.
- Попробуйте запустить новые процессы при помощи диспетчера, для этого можно использовать команды: `cmd`, `msconfig`.

Задание 2. Работа в командной строке Windows.

1. Для запуска командной строки в режиме Windows следует нажать: (Пуск) > «Все программы» > «Стандартные» > «Командная строка»
2. Поработайте выполнением основных команд работы с процессами: запуская, отслеживая и завершая процессы.

Основные команды:

`Schtasks` — выводит выполнение команд по расписанию;

`Start` — запускает определенную программу или команду в отдельном окне. `Taskkill` — завершает процесс;

`Tasklist` — выводит информацию о работающих процессах;

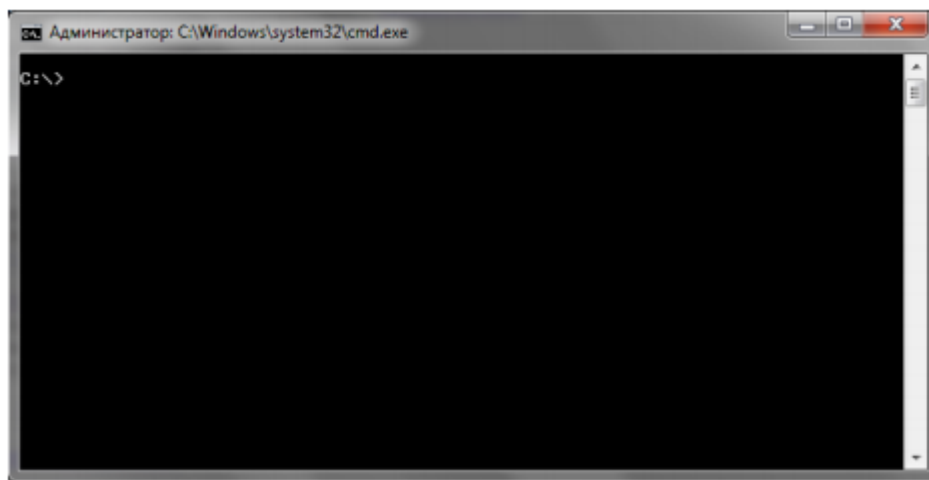


Рисунок 5.2.- Командная строка Windows 7.

3. В появившемся окне (рисунок 5.2) наберите:
`cd\` — переход в корневой каталог;
`cd windows` – переход в каталог Windows.
`dir` — просмотр содержимого каталога.
 В данном каталоге мы можем работать с такими программами как «WordPad» и «Блокнот».
4. Запустите программу «Блокнот»:
`C:\Windows > start notepad.exe`
 Отследите выполнение процесса: `C:\Windows > tasklist`
 Затем завершите выполнение процесса: `C:\Windows > taskkill /IM notepad.exe`
5. Самостоятельно, интуитивно, найдите команду запуска программы WordPad. Необходимый файл запуска найдите в папке Windows.
6. Выполнение задания включить в отчет по выполнению лабораторной работы.

Задание 3.

1. Отследите выполнение процесса explorer.exe при помощи диспетчера задач и командной строки.
2. Продемонстрируйте преподавателю завершение и повторный запуск процесса explorer.exe из:
 - Диспетчера задач;
 - Командной строки.
3. Выполнение задания включить в отчет по выполнению лабораторной работы.

Контрольные вопросы:

1. Дайте понятие процессу в операционной системе.
2. Дайте понятие службе в операционной системе.
3. Причислите основные команды работы с процессами при помощи командной строки.

6.ЛАБОРАТОРНАЯ РАБОТА №6. МОНИТОРИНГ ПРОИЗВОДИТЕЛЬНОСТИ ОС WINDOWS

Цель работы: практическое знакомство с методикой использования системного монитора (монитора производительности) perfmon для поиска узких мест в вычислительной системе.

6.1. Краткие теоретические сведения

1.1 Мониторинг производительности ОС с помощью системного монитора

Цель мониторинга работы ОС – поиск узких мест в системе, обусловленных нехваткой ресурсов – аппаратных или информационных. В качестве исходных данных для анализа узких мест могут использоваться данные, получаемые со счетчиков производительности.

Счетчики производительности. Семейство операционных систем MS Windows получает информацию о производительности от аппаратных и программных компонентов компьютера. Системные компоненты (драйверы режима ядра) в ходе своей работы генерируют данные о производительности. Такие компоненты называются *объектами производительности*. В ОС имеется ряд объектов производительности, обычно соответствующих аппаратным компонентам, таким как память, процессоры, внешние устройства и т. д.

Каждый объект производительности предоставляет счетчики, которые собирают данные производительности (**performance counters**). Счетчик производительности представляет собой механизм, с помощью которого в MS Windows производится сбор сведений о производительности различных системных ресурсов. В MS Windows имеется предопределенный набор счетчиков производительности, с которыми можно взаимодействовать — некоторые из этих счетчиков присутствуют на всех компьютерах с установленной ОС Windows, а некоторые относятся к определенным приложениям и имеются только на некоторых компьютерах. Каждый счетчик относится к определенной области функций системы. В качестве примера можно привести счетчики, следящие за загрузкой процессора, использованием памяти и количеством полученных или переданных по сети байтов. Экземпляр компонента PerformanceCounter можно использовать для непосредственного подключения к существующим счетчикам производительности и для динамического взаимодействия с данными этих счетчиков.

Счетчик производительности следит за поведением объектов производительности компьютера. Эти объекты включают в себя физические компоненты, такие как процессоры, диски, память и системные объекты, такие как процессы, потоки и задания. Системные счетчики, относящиеся к одному и тому же объекту производительности, группируются в категории, отражающие их общую направленность. При создании экземпляра компонента PerformanceCounter сначала указывается категория, с которой будет взаимодействовать компонент, затем внутри этой категории выбирается счетчик, с которым будет осуществляться взаимодействие.

Примером категории счетчиков производительности в Windows является категория «Память». Системные счетчики в этой категории отслеживают такие данные, как количество доступных и кэшируемых байтов. Чтобы узнать в приложении количество кэшируемых

байтов, нужно создать экземпляр компонента PerformanceCounter и связать его с категорией «Память», а затем выбрать в этой категории соответствующий счетчик (в данном случае счетчик кэшируемых байтов).

Некоторые объекты (такие как Память и Сервер) имеют только один экземпляр, другие объекты производительности могут иметь множество экземпляров. Если объект имеет множество экземпляров, то можно добавить счетчики для отслеживания статистики по каждому экземпляру или для всех экземпляров одновременно.

Например, если в системе установлены несколько процессоров, или процессор имеет несколько ядер, то объект Процессор будет иметь множество экземпляров. В случае, если объект поддерживает множество экземпляров, то при объединении экземпляров в группу появятся родительский экземпляр и дочерние экземпляры, которые будут принадлежать данному родительскому экземпляру.

В счетчиках производительности сохраняются данные о различных частях системы. Эти значения не запоминаются как записи, но они сохраняются, пока для заданной категории дескриптор остается открытым в памяти. Процесс извлечения данных из счетчика производительности называется получением выборки данных. При получении выборки происходит извлечение непосредственного или рассчитанного значения счетчика.

В зависимости от определения счетчика это значение может соответствовать текущему использованию ресурса (мгновенное значение) или может быть средним значением двух измерений за период времени между выборками. Например, при извлечении значения счетчика потоков из категории Process для конкретного процесса извлекается число потоков на момент последнего измерения. Полученная величина является мгновенным значением. Тем не менее, при извлечении значения счетчика Pages/Sec категории Memory извлекается значение в секундах, которое вычисляется на основе среднего числа страниц, полученных между двумя последними выборками.

Использование ресурсов может сильно изменяться в зависимости от работы в разное время дня. Поэтому счетчики производительности, отражающие процент использования ресурсов за интервал, являются более информативным средством измерения, чем вычисление среднего на основе мгновенных значений счетчиков. Средние значения могут включать в себя данные, соответствующие запуску службы или другим событиям, что на короткий период приведет к выходу значений далеко за пределы диапазона, и, следовательно, к искажению результатов.

Для работы со счетчиками производительности используется встроенная в ОС Windows программа Performance Monitor (perfmon.exe). Она не представлена в Главном меню, но ее всегда можно запустить посредством команды «Выполнить» (комбинация клавиш Win+R), далее в строке набрать perfmon.exe.

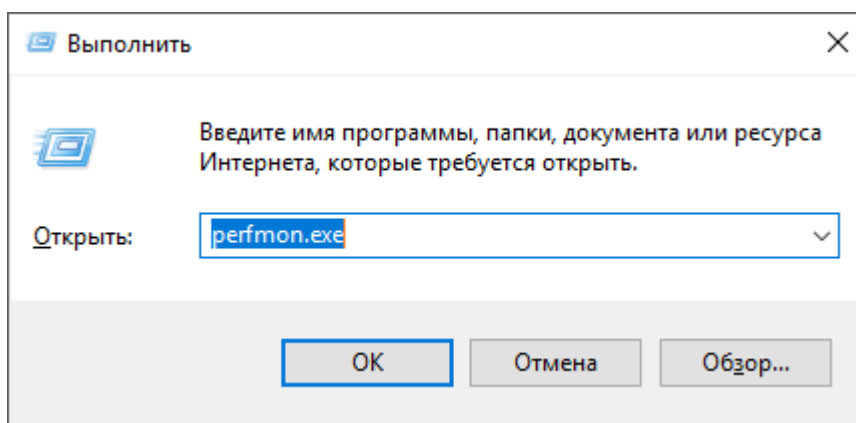


Рисунок 6.1 – Запуск Performance Monitor

Для добавления счетчиков необходимо вызвать правой кнопкой мыши КЗМ на поле графиков (рисунок 6.2), выбрать пункт «Добавить счетчики...», из списка «Имеющиеся счетчики» выбрать необходимые, нажать кнопку «Добавить >>» и «ОК».

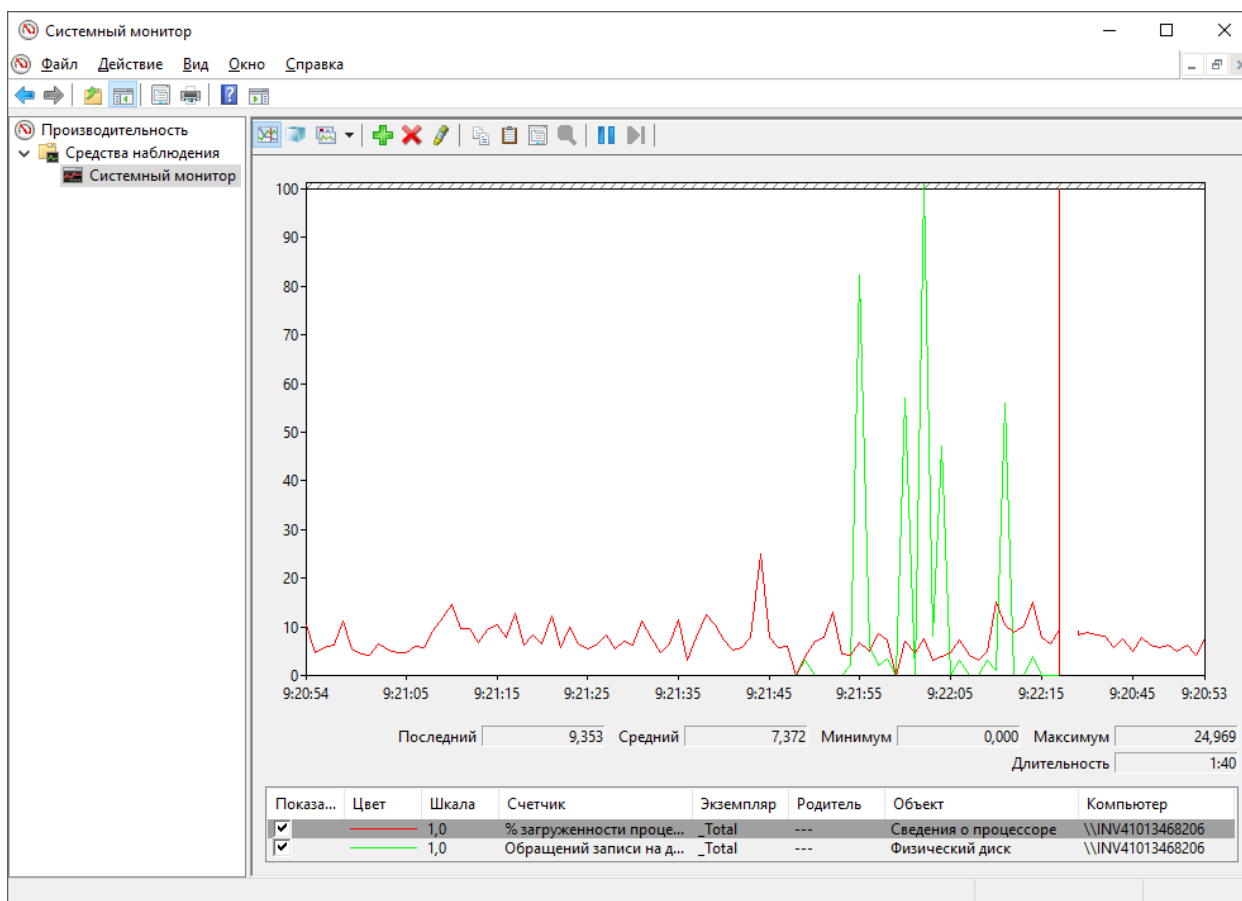


Рисунок 6.2 – Внешний вид программы Performance Monitor в MS Windows 10

В качестве примера рассмотрим последовательность действий при построения графика зависимости размера ошибок страницы/с страниц процесса Блокнот (Notepad) от времени.

1. Запустить Блокнот.
2. Запустить системный монитор perfmon.

3. Используя кнопку «Удалить», очистить окно вывода и перечень выводимых графиков.
4. Правой кнопкой мыши вызвать КЗМ, выбрать Пункт «Добавить счетчики».
5. В окне «Добавление» (рисунок 3) выбрать из списка Объект категорию Процесс, далее из списка процессов выбрать процесс notepad, выбрать счетчик Ошибок страницы/с из списка счетчиков
6. Нажать кнопку «Добавить >>», затем «ОК».

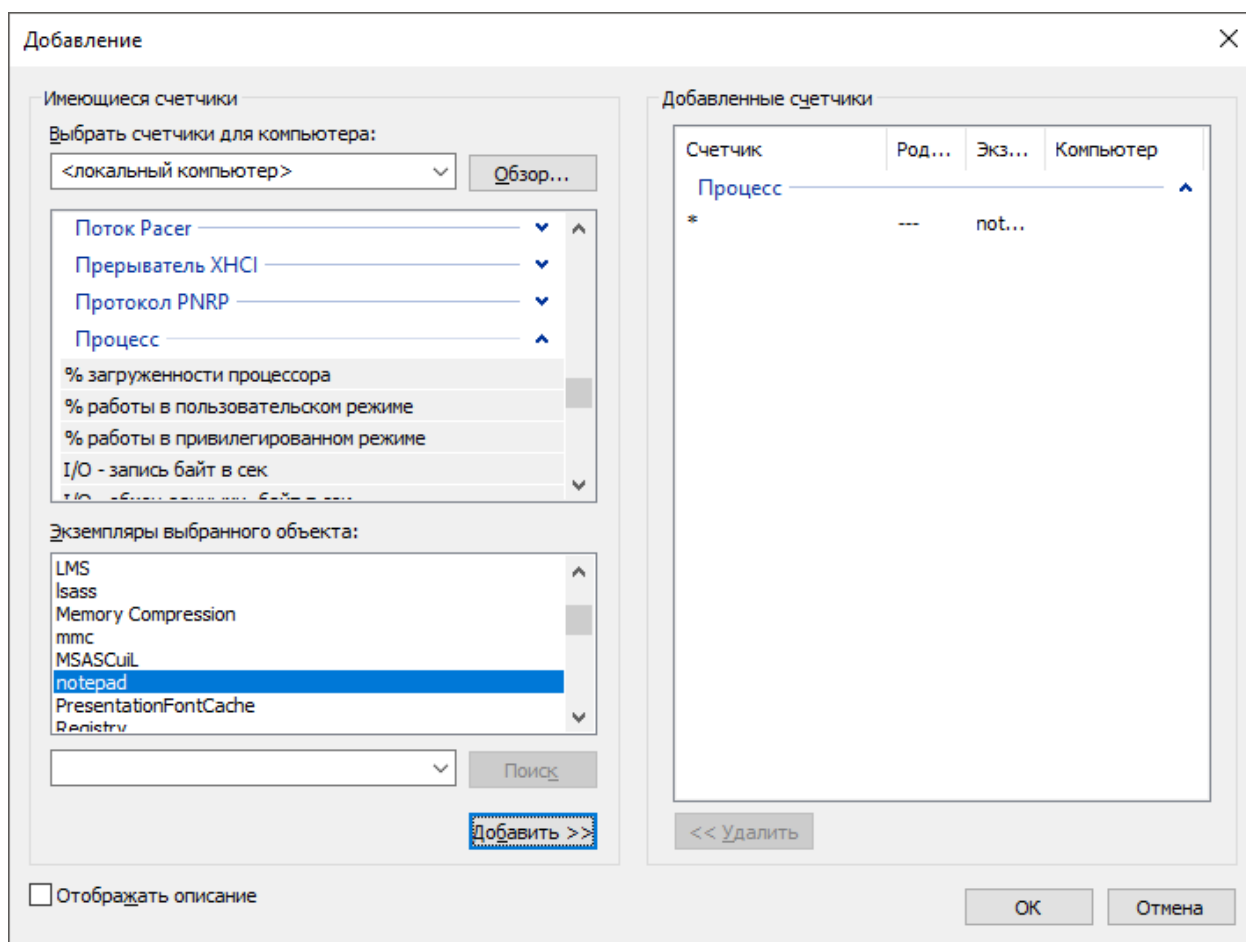


Рисунок 6.3 – Добавление нового счетчика

Управление формой представления графиков производится с помощью окна свойств, которое открывается с помощью кнопки Свойства.

Диапазон значений вертикальной шкалы задается в окне «Свойства: системный монитор» – рисунок 6.4. Для вызова используется КЗМ на графике, пункт «Свойства...».

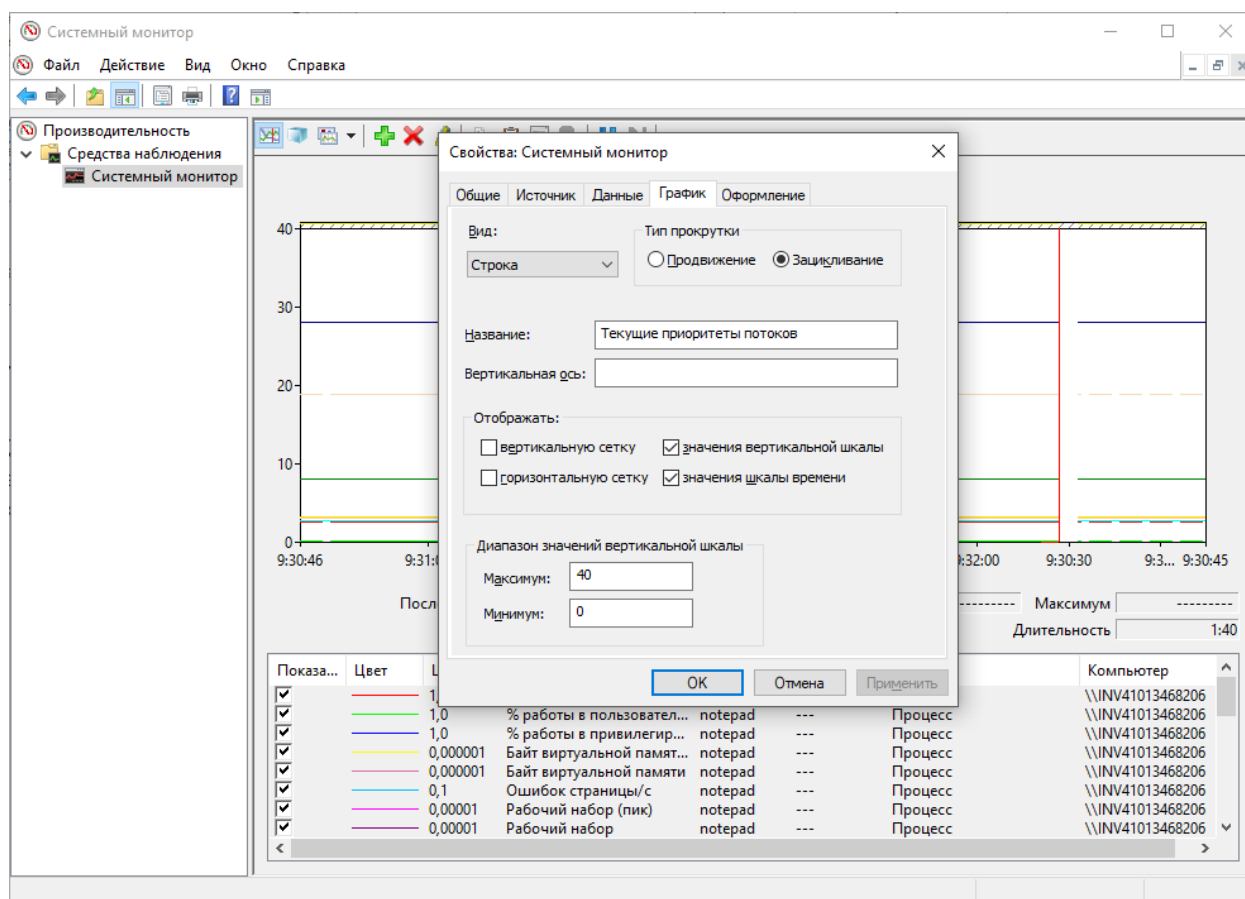


Рисунок 6.4 – Окно «Свойства: системный монитор»

В окне Свойства необходимо задать максимальное и минимальные значения вертикальной шкалы и нажать кнопку Применить.

На рисунке 6.5 показан полученный график изменения Ошибок страницы/с программы notepad в процессе создания текстового файла.

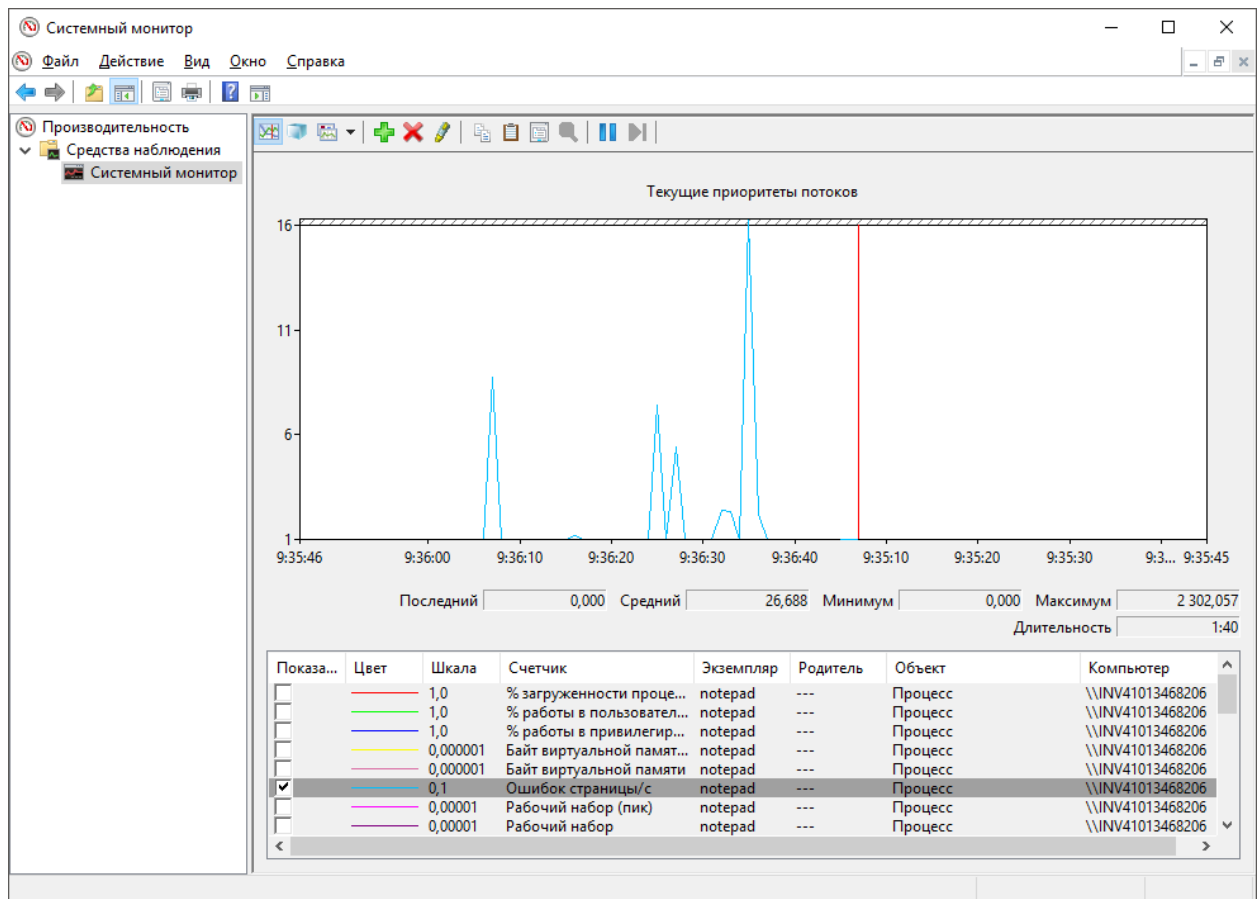


Рисунок 6.5 – График изменения Ошибок страницы/с notepad при создании файла

6.2 Задание на лабораторную работу

1. Построить графики изменения количества потоков приложений Notepad и Microsoft Office Word при создании документа, содержащего текст из одного слова.
2. Для приложения Калькулятор построить 2-3 наиболее динамично изменяющихся графика изменения текущего приоритета потоков при вычислении значения арифметического выражения, перемещении калькулятора по экрану, перемещении курсора мыши по экрану в области окна калькулятора.
3. Для приложения Microsoft Office Word построить график изменения объема используемого файла подкачки при последовательном открытии 3-4 файлов увеличивающегося размера.
4. Выполнить индивидуальные задания (таблица 6.1).

Таблица 6.1.-Варианты задания

вариант	Задание
1	Для программы Проводник построить графики изменения количества потоков в процессе запуска приложения
2	Показать характер изменения во времени общего количества выполняющихся с системе потоков
3	Для каждого ядра процессора выяснить, в каком режиме ядро работает больше времени – пользовательском или системном
4	Для каждого ядра процессора выяснить, сколько процентов времени ядро выполняет обработку прерываний.

7.ЛАБОРАТОРНАЯ РАБОТА №7.ВЫЯВЛЕНИЕ ПРИСУТСТВИЯ НА КОМПЬЮТЕРЕ ВРЕДОНОСНЫХ ПРОГРАММ

Цель работы: получить практические навыки по выявлению вредоносных программ на локальном компьютере под управлением ОС Windows .

7.1.Теоретические сведения

Одним из основных проявлений вредоносных программ является наличие в списке запущенных процессов подозрительных программ. Исследуя этот список и, особенно, сравнивая его с перечнем процессов, которые были запущены на компьютере сразу после установки системы, можно сделать достаточно достоверные выводы об инфицировании. Это часто помогает при обнаружении вредоносных программ, имеющих лишь только скрытые или косвенные проявления. Однако необходимо четко понимать и уметь отличать легальные процессы от подозрительных.

Диспетчер задач Windows – это стандартная утилита, входящая в любую Microsoft Windows – подобную операционную систему. С ее помощью можно в режиме реального времени отслеживать выполняющиеся приложения и запущенные процессы, оценивать загруженность системных ресурсов компьютера и использование сети.

При работе с домашним компьютером рекомендуется сразу после установки операционной системы ознакомиться со списком запускаемых ею процессов. В дальнейшем, при подозрении на заражение, можно будет вывести перечень процессов и сразу исключить из рассмотрения те, что были с самого начала.

Для того, чтобы прикладная программа начала выполняться, ее нужно запустить. Следовательно, и вирус нуждается в том, чтобы его запустили. Для этого можно использовать два сценария: либо сделать так, чтобы пользователь сам его стартовал (используются обманные методы), либо внедриться в конфигурационные файлы и запускать одновременно с другой, полезной программой. Оптимальным с точки зрения вируса вариантом служит запуск одновременно с операционной системой – в этом случае запуск практически гарантирован. Самый простой способ добавить какую-либо программу в автозагрузку – это поместить ее ярлык в раздел Автозагрузка системного меню Пуск / Программы.

Неожиданно возросшая сетевая *активность* может служить ярким свидетельством работы на компьютере подозрительной программы, производящей несанкционированную рассылку писем, или просто загружающую свои дополнительные модули или атакующей соседние компьютеры. Изучить и проанализировать сетевую *активность* можно с помощью встроенных в операционную систему инструментов или же воспользовавшись специальными отдельно устанавливаемыми приложениями.

7.2. Последовательность выполнения работы

7.2.1. Отслеживание подозрительных процессов

1. Перейти к Диспетчеру задач Windows, нажав одновременно клавиши *Ctrl*, *Shift* и *Esc* (рис. 5.1)

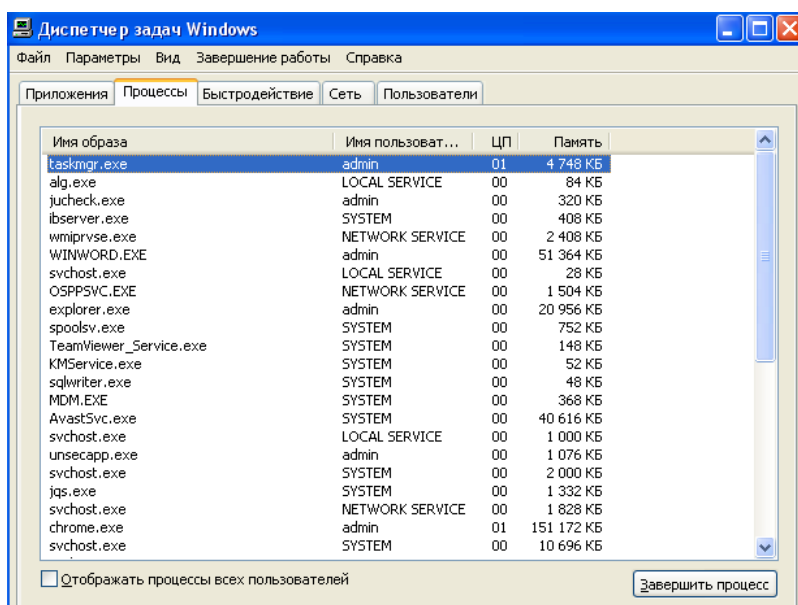


Рисунок 7.1.- Окно Диспетчера задач

Открывшееся окно содержит четыре закладки, отвечающие четырем видам активности, которые отслеживает Диспетчер приложения: приложения, процессы, быстродействие (использование системных ресурсов) и Сеть. Изучить представленный в окне *Процессы* список процессов. Если на компьютере не запущены никакие пользовательские программы, он должен содержать только служебные процессы операционной системы. Для каждого процесса выводятся его параметры: имя образа (может не совпадать с именем запускаемого файла), имя пользователя, от чьего имени был запущен процесс, загрузка этим процессом процессора и объем занимаемой им оперативной памяти. Загрузка процессора представлена в процентах от максимальной. Поэтому для удобства пользователя в списке всегда присутствует пункт "Бездействие системы". С его помощью можно быстро узнать насколько загружен, вернее свободен процессор.

2. Отсортировать все процессы по использованию ресурсов процессора. Для этого нажать на заголовок поля ЦП (ЦП). Поскольку в данный момент не должна быть запущена ни одна пользовательская программа, процессор должен быть свободен. Следовательно, "Бездействие системы" должно оказаться внизу списка с достаточно большим процентом "использования" процессора. (95 %).

Этот метод также можно использовать для того, чтобы в случае заметного снижения производительности определить, какая программа виновна в этом: столбец ЦП покажет загрузку процессора, а *Память* - оперативную память.

В ряде случаев может потребоваться вручную завершить некий процесс. Это можно сделать с помощью кнопки *Завершить процесс*.

3. Не закрывая окна *Диспетчера задач Windows*, открыть программу *Paint*. Не закрывая приложение *Paint*, вернуться к окну *Диспетчера задач Windows* и проследить за изменениями на закладке *Приложения*. Список запущенных приложений должен содержать строку, соответствующую *Paint*. Если программа вызывает ошибку - тогда в ее состоянии будет написано "Не отвечает", нужно воспользоваться кнопкой *Снять задачу* и начать поиски причин. В иных случаях пользоваться этой кнопкой не рекомендуется.

Убедится, что программе *Paint* соответствует процесс mspaint.exe. Для этого найдите его в списке запущенных процессов, не закрывая и не сворачивая окно *Диспетчера задач Windows*, вернитесь в окне *Paint* и закройте его. Проследите, что из списка запущенных процессов пропал mspaint.exe.

4. Перейти к закладке *Быстродействие*. Любые всплески на графиках должны по времени соответствовать неким действиям, например запуску требовательной к ресурсам

программы. Если ничего похожего сознательно не производилось, это может быть причиной для более детального исследования компьютера

5. Закрыть окно Диспетчера задач Windows.

7.2.2 Элементы автозапуска

1. Дважды щелкнуть левой клавишей мыши по названию группы *Автозагрузка* (Пуск – Программы – Автозагрузка). В результате должно открыться соответствующее окно папки автозагрузки. Чтобы программа запускалась автоматически при старте операционной системы необходимо поместить в эту папку ее ярлык.

2. Скопировать из папки *Стандартные* (Пуск / Программы / Стандартные) ярлык *Блокнот* в окно автозагрузки.

3. Перезагрузить компьютер (Пуск / Завершение работы). Убедиться, что по завершению загрузки автоматически запустилась программа *Блокнот*.

4. Для большинства ситуаций, связанных с автозапуском, достаточно использовать системную утилиту *Настройка системы*. В окне *Поиск* набрать msconfig, в окне *Программы* выполнить двойной щелчок по имени утилиты. Откроется окно (рис.5.2).

5. На первой закладке, *Общие*, можно выбрать вариант запуска операционной системы. По умолчанию отмечен *Обычный запуск*. Он обеспечивает максимальную функциональность системы. Остальные два варианта запуска предназначены для диагностики

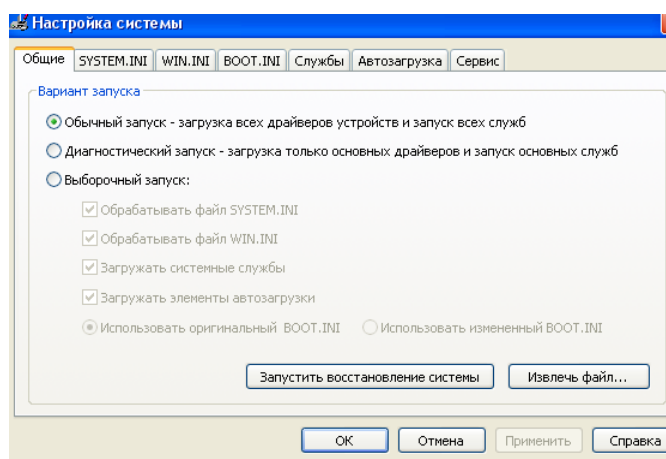


Рисунок 7.2.- Окно «Настройка системы»

Второй режим, *Диагностический запуск*, рекомендуется использовать при подтвердившемся вирусном инциденте - если компьютер уже заражен, сразу установить антивирус в ряде случаев нельзя, например, если вирус сознательно блокирует запуск ряда антивирусных программ. Тогда, если нет возможности удалить или хотя бы временно обезвредить вирус вручную, рекомендуется запустить операционную систему в безопасном режиме, установить антивирус и сразу же проверить весь жесткий диск на наличие вирусов.

6. Перейти на закладку *Службы*, где представлен список всех служб, установленных в системе. Каждая служба представляет собой некое приложение, работающее в фоновом режиме. Например, антивирусный комплекс, обеспечивающий постоянную защиту, также встраивает свою службу, следовательно, она должна присутствовать в этом перечне. Установить флаг: *Не отображать службы Майкрософт*. Если сторонних приложений действительно нет, список должен опустеть.

7. Перейти к закладке *Автозагрузка*, и убедиться, что в списке приложений, автоматически запускаемых при загрузке системы, есть *Блокнот*. Список в окне *Настройки системы* может содержать дополнительные элементы, не отображаемые в разделе *Пуск / Программы / Автозагрузка*. Отключить автоматическую загрузку *Блокнота*, очистив флаг в столбце *Элемент автозагрузки* и нажать *OK*. Перезагрузить компьютер.

8. Перейти к закладке *Автозагрузка* и убедиться, что ее вид не изменился - *Блокнот* все так же присутствует в списке, но отключен. Не закрывая окна *Настройка системы* проверить, что *Блокнот* автоматически не запустился и раздел *Пуск / Программы / Автозагрузка* теперь пуст. На закладке *Общие* окна *Настройка системы* выбрать сценарий *Обычный запуск*. Удалить ярлык *Блокнота* из *Пуск / Программы / Автозагрузка* и выполнить перезагрузку.

7.2.3 Сетевая активность

1. Открыть окно *Диспетчера задач Windows*, нажав одновременно клавиши *Ctrl, Shift* и *Esc*, и перейдите к закладке *Сеть*. Если не иницируется ни одного сетевого соединения, график должен быть пуст (прямая на уровне 0 %). В нижней части окна расположен перечень всех установленных в системе сетевых адаптеров. Обычно он один. В столбце *Использование сети* приводится моментальное значение доли используемого канала, а в *Скорость линии* - пропускная способность. *Состояние* отображает статус (рис 5.3).

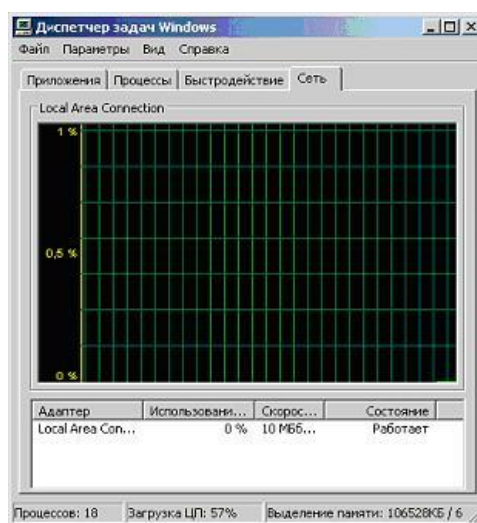


Рисунок 7.3. -Закладка «Сеть» диспетчера задач

2. Инициировать сетевое соединение, например, выход в Интернет. На графике *Диспетчера задач* действия отобразятся в виде пиков сетевой активности, а значение поля *Использование сети* перестанет быть равным нулю. Таким образом, если после закрытия прикладных программ, которые могут инициировать сетевые соединения, сеть все равно продолжает использоваться, нужно искать причину.

3. Диспетчер задач Windows показывает только самую общую информацию. Для получения более подробных данных можно воспользоваться утилитой netstat. Закрыть окно Диспетчера задач Windows и перейти к системному меню *Пуск / Программы / Стандартные / Командная строка*. Набрать *netstat /?* и нажать *Enter* (рисунок 7.4).

```

C:\>netstat /?

Отображение статистики протокола и текущих сетевых подключений TCP/IP.

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p протокол] [-r] [-s] [-v] [интервал]

-a          Отображение всех подключений и ожидающих портов.
-b          Отображение исполняемого файла, участвующего в создании каждого
            подключения, или ожидающего порта. Иногда известные исполняемые
            файлы содержат множественные независимые компоненты. Тогда
            отображается последовательность компонентов, участвующих в
            создании подключения, либо ожидающий порт. В этом случае имя
            исполняемого файла находится снизу в скобках [], сверху -
            компонент, который им вызывается, и так до тех пор, пока не
            достигается TCP/IP. Заметьте, что такой подход может занять
            много времени и требует достаточных разрешений.
-e          Отображение статистики Ethernet. Он может применяться вместе
            с параметром -s.
-n          Отображение адресов и номеров портов в числовом формате.
-o          Отображение кода (ID) процесса каждого подключения.
-p протокол Отображение подключений для протокола, задаваемых этим
            параметром. Допустимые значения: TCP, UDP, TCPv6 или UDPv6.
  
```

Рисунок 7.4.- Эмулятор MS DOS.

4. Набрав `netstat -a` и нажать Enter. Результатом выполнения команды является список активных подключений, в который входят установленные соединения и открытые порты. Открытые TCP-порты обозначаются строкой "LISTENING" в колонке состояние. Часть портов связана с системными службами Windows и отображается не по номеру, а по названию - `ermap`, `microsoft-ds`, `netbios-ssn`. Порты, не относящиеся к стандартным службам, отображаются по номерам.

UDP -порты обозначаются строкой "UDP" в колонке Имя. Они не могут находиться в разных состояниях, поэтому специальная пометка "LISTENING" в их отношении не используется. Как и TCP -порты они могут отображаться по именам или по номерам. Порты, используемые вредоносными программами, чаще всего являются нестандартными и поэтому отображаются согласно их номерам. Впрочем, могут встречаться троянские программы, использующие для маскировки стандартные для других приложений порты, например 80, 21, 443 - порты, используемые на файловых и веб-серверах.

5. Закрыть окно командной строки. Для этого ввести команду `exit`.

7.3 Содержание отчета

Цель работы; постановка задачи; описание выполнения заданий п.5.2, результаты выполнения заданий, выводы по работе.

7.4 Контрольные вопросы

- 1) Каковы признаки вредоносных программ?
- 2) Как снять запущенное на компьютере приложение?
- 3) Как добавить приложение в автозагрузку?
- 4) Что отображается на вкладке «Сеть» Диспетчера задач?

8. ЛАБОРАТОРНАЯ РАБОТА № 8. АУДИТ

Цель работы: Ознакомиться с встроенными средствами протоколирования событий ОС Windows .

8.1. Теоретические сведения

Процедура аудита применительно к ОС заключается в регистрации в специальном журнале, называемом журналом аудита или журналом безопасности, событий, которые могут представлять опасность для ОС. Необходимость включения в защищенную ОС функций аудита обусловлена следующими обстоятельствами:

1) обнаружение попыток вторжения является важнейшей задачей системы защиты, поскольку ее решение позволяет минимизировать ущерб от взлома и собирать информацию о методах вторжения;

2) подсистема защиты ОС может не отличить случайные ошибки пользователей от злонамеренных действий. Администратор, просматривая журнал аудита, сможет установить, что произошло при вводе пользователем неправильного пароля — ошибка легального пользователя или атака злоумышленника. Если пользователь пытался угадать пароль 20—30 раз, то это явная попытка подбора пароля;

3) администраторы ОС должны иметь возможность получать информацию не только о текущем состоянии системы, но и о том, как ОС функционировала в недавнем прошлом. Такую возможность обеспечивает журнал аудита;


4) если администратор ОС обнаружил, что против системы проведена успешная атака, ему важно выяснить, когда была начата атака и каким образом она осуществлялась. Журнал аудита может содержать всю необходимую информацию.

К числу событий, которые могут представлять опасность для ОС, обычно относят следующие:

- вход или выход из системы;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- обращение к удаленной системе;
- смену привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя).

Добавлять записи в журнал аудита может только ОС. Редактировать или удалять отдельные записи в журнале аудита не может ни один субъект доступа, в том числе и сама ОС. Просматривать журнал аудита могут только пользователи, обладающие соответствующей привилегией. Очищать журнал аудита могут только пользователи-аудиторы. После очистки журнала в него автоматически вносится запись о том, что журнал аудита был очищен, с указанием времени очистки журнала и имени пользователя, очистившего журнал. ОС должна поддерживать возможность сохранения журнала аудита перед очисткой в другом файле. Для ограничения доступа к журналу аудита должны применяться специальные средства защиты.

8.2. Последовательность выполнения работы

1. Включение аудита. Открыть раздел «Локальная политика безопасности». Для этого нажать кнопку Пуск , в строке Поиск ввести secpol.msc, после появления команды secpol в окне Программы выполнить двойной щелчок по имени. Откроется окно «Локальная политика безопасности» (рис.6.1)

В левой области дважды щелкнуть строку *Локальные политики* и выбрать пункт *Политика аудита*. Дважды щелкнуть событие, за которым нужно наблюдать, например, Аудит входа в систему. Установить флажки *Успех* или *Отказ* (или оба одновременно), затем нажать ОК.

- Если установить флажок *Успех*, Windows будет фиксировать успешные попытки выполнения события выбранного типа. Например, после включения аудита входа в систему любой вход пользователя в систему будет зарегистрирован как событие успешного входа в систему.

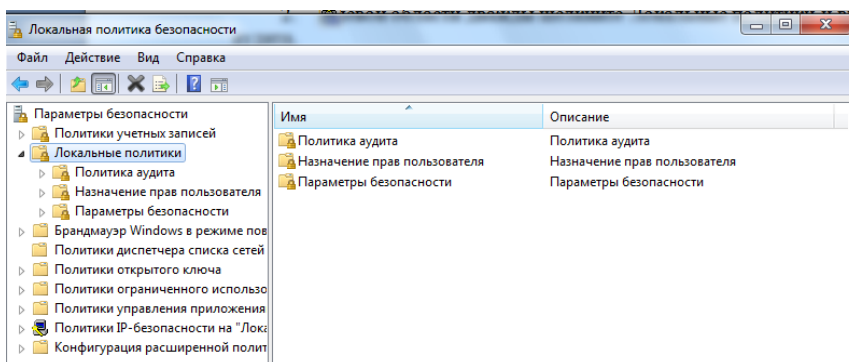


Рисунок 8.1.- Окно «Локальная политика безопасности»

- Если установить флажок *Отказ*, будут зафиксированы все безуспешные попытки входа в систему.

- Если выбрать и *Успех*, и *Отказ*, Windows будет фиксировать все попытки.

Количество фиксируемых событий ограничено, поскольку слишком большой журнал аудита событий может замедлить работу компьютера. Чтобы освободить место, можно удалить события из журнала с помощью окна просмотра событий.

2. Чтобы отслеживать пользователей, открывающих документ, выполняют следующие действия:

1) Щелкнуть правой кнопкой мыши документ, контроль за которым нужно установить, и выбрать из контекстного меню пункт *Свойства*.

2) На вкладке *Безопасность* нажать кнопку *Дополнительно* и перейти на вкладку *Аудит*.

3) Нажать кнопку *Продолжить*. Если отображается запрос на ввод пароля администратора или его подтверждения, указать пароль или предоставить подтверждение.

4) Щелкнуть кнопку *Добавить*. В поле *Введите имена выбираемых объектов* ввести имя пользователя или группы, за которыми нужно установить наблюдение (рис.6.2), и нажать ОК в последующих четырех диалоговых окнах.

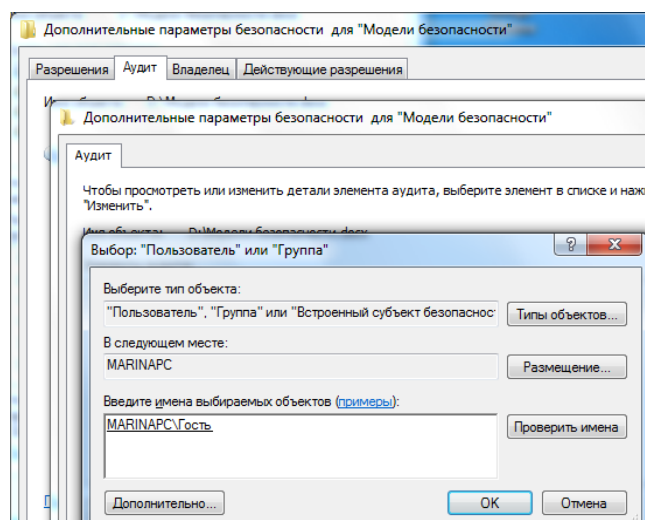


Рисунок 8.2. - Установление наблюдения за пользователями



Если необходимо контролировать всех пользователей, ввести *Everyone*. Если необходимо производить наблюдение за конкретным пользователем, ввести имя компьютера, а затем имя пользователя. Если компьютер входит в домен, следует ввести имя домена и затем имя пользователя: компьютер\имя пользователя или домен\имя компьютера.

5) Установить флажки для всех действий, которые нужно контролировать, а затем щелкнуть ОК. В таблице 6.1 описываются объекты или действия, за которыми можно установить наблюдение.

Таблица 8.1.- Действия над файлами, для которых можно установить аудит

Действие	Описание
Просмотр папок или выполнение файлов	Отслеживание попыток запустить программный файл
Перечисление содержимого папки или чтение данных	Отслеживание попыток просмотра данных в файле
Чтение атрибутов	Отслеживание попыток просмотра атрибутов файла или папки, таких как «Только чтение» или «Скрытый».
Чтение дополнительных атрибутов	Отслеживание попыток просмотра дополнительных атрибутов файла. Дополнительные атрибуты определяются программами, создавшими файл
Создание файлов или запись данных	Отслеживание попыток изменения содержания файла
Создание папок или добавление данных	Отслеживание попыток добавления данных в конец файла.
Запись атрибутов	Отслеживание попыток изменения атрибутов файла
Запись дополнительных атрибутов	Отслеживание попыток изменения дополнительных атрибутов файла
Удаление подпапок и файлов	Отслеживание попыток удаления папок
Удаление	Отслеживание попыток удаления файлов
Чтение разрешений	Отслеживание попыток просмотра разрешений файла
Изменение разрешений	Отслеживание попыток изменения разрешений файла
Смена владельца	Отслеживание события, когда пользователь становится владельцем файла

Флажок Полный доступ позволяет выбрать все доступные для наблюдения действия.

3. Просмотр журнала аудита осуществляется в разделе «Просмотр событий». Для открытия раздела нажать кнопку *Пуск* , выбрать *Панель управления*, *Администрирование*, затем дважды щелкнуть *Просмотр событий* . Если отображается запрос на ввод пароля администратора или его подтверждения, указать пароль или предоставить подтверждение. В левой области дважды щелкнуть *Журналы Windows* и выбрать пункт *Безопасность*. Откроется окно Просмотр событий (рис.6.3).

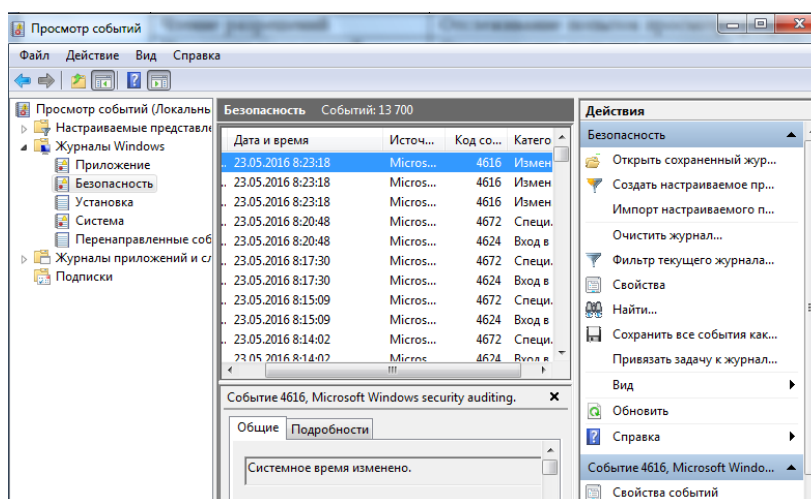


Рисунок 8.3. -Окно «Просмотр событий»

Чтобы просмотреть подробности, необходимо дважды щелкнуть событие. Для очистки журналов нажать *Очистить журнал* на панели действий.

4. Чтобы настроить, просмотреть или изменить настройки аудита файлов и папок, нужно установить указатель мыши на файл или папку, для которой следует выполнить аудит, и нажать правую кнопку. В появившемся контекстном меню выбрать пункт *Свойства*. В окне свойств папки или файла перейти на вкладку *Безопасность*, нажмите кнопку *Дополнительно* и затем перейти на вкладку *Аудит*.

Появится диалоговое окно *Выбор*: Пользователь, Компьютер или Группа, в котором выбирается имя нужного пользователя или группы. Откроется окно диалога *Элемент аудита* для, где можно ввести все необходимые параметры аудита: в списке *Применять* указать, где следует выполнять аудит (это поле ввода доступно только для папок); в группе *Доступ* следует указать, какие события следует отслеживать: окончившиеся успешно(Успех), неудачно (Отказ) или оба типа событий. Флажок *Применять этот аудит к объектам и контейнерам только внутри этого контейнера* определяет, распространяются ли введенные настройки аудита на файлы и папки, находящиеся ниже по дереву каталогов файловой системы (флажок не установлен). В противном случае установить флажок (или выбрать в списке *Применять* опцию *только для этой папки*). Это позволит не выполнять аудит для тех объектов файловой системы, которые не представляют интереса. После завершения настройки аудита для папки или файла закрыть все окна диалога.

8.3 Содержание отчета

Цель работы; постановка задачи; описание выполнения заданий п.8.2, результаты выполнения заданий, выводы по работе.

8.4 Контрольные вопросы

- 5) Что такое аудит?
- 1) Какие действия над файлами контролируются системой?
- 2) Как включить аудит?
- 3) Как отслеживать действия пользователей?

9. ЛАБОРАТОРНАЯ РАБОТА №9. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА В ОС WINDOWS

Цель работы: ознакомление с криптографическими средствами защиты, приобретение практических навыков шифрования файлов и генерации ключей.

9.1 Теоретические сведения

Криптография занимается поиском и исследованием математических методов преобразования информации с целью ее засекречивания. Криптография дает возможность обеспечить защиту информации путем изменения формы ее представления. Обратимое преобразование исходного (открытого) текста с целью его защиты называется шифрованием. Дешифрование - обратный шифрованию процесс, при котором дешифрованный текст преобразуется в исходный. Для шифрования или дешифрования текстов данных используется ключ. В криптографии принято правило Кирхгоффа: «Стойкость шифра должна определяться только секретностью ключа», что подразумевает, что алгоритмы шифрования должны быть открыты. В зависимости от количества ключей, используемых для шифрования и дешифрования, криптографические алгоритмы делятся на симметричные (с одним секретным ключом) и асимметричные (с двумя ключами, открытым и секретным).

Шифрование — это самый надежный способ защиты данных, предоставляемый ОС Windows, который используется для защиты файлов, папок и дисков от несанкционированного доступа.

9.1.1 Шифрование файлов и папок

Встроенная в Windows система шифрования данных EFS шифрует информацию прозрачно для пользователя, то есть с файлами и папками можно работать как обычно, и позволяет сохранять сведения на жестком диске в зашифрованном формате. Если попытаться открыть их в другой среде (ОС, ПК), то доступ к ним будет закрыт.

Работает EFS следующим образом. Когда необходимо зашифровать файл система генерирует случайный ключ называемый FEK — File Encryption Key. Этим ключом с помощью симметричного алгоритма шифрования кодируется файл. В симметричных системах файл шифруется и расшифровывается одним ключом — FEK.

При первой необходимости шифрования информации Windows создает два ключа пользователя: открытый и закрытый. FEK шифруется с помощью асимметричного алгоритма с использованием открытого ключа пользователя. В асимметричных алгоритмах шифрования файл шифруется одним ключом (открытым), а расшифровывается другим (закрытым). Зашифрованный ключ FEK записывается рядом с зашифрованным файлом.

Закрытый ключ шифруется с помощью пароля пользователя. Поэтому защищенность информации напрямую зависит от сложности пароля. Рекомендуется задавать его более чем из 8-ми символов, включая буквы нижнего и верхнего регистров, цифры и специальные символы

Для расшифровки данных необходимо зайти под учетной записью пользователя, который зашифровал файлы. При этом автоматически при вводе правильного пароля расшифровывается закрытый ключ. С помощью последнего расшифровывается FEK — File Encryption Key, которым расшифровывается нужный файл.

9.1.2 Шифрование дисков

Шифрование диска BitLocker является встроенной функцией безопасности в операционной системе Windows 7, которая позволяет защитить данные, хранящиеся на фиксированных и съемных дисках, а также на диске операционной системы. BitLocker позволяет защитить компьютер от "атак с выключением", которые проводятся путем

отключения или обхода установленной операционной системы либо путем физического удаления жесткого диска для взлома данных автономно. Для фиксированных и съемных дисков BitLocker обеспечивает прочтение и запись данных на диск только для пользователей с требуемым паролем, учетными данными смарт-карты или при использовании диска на компьютере с защитой BitLocker и соответствующими ключами.

Защита BitLocker на дисках операционной системы поддерживает двухфакторную проверку подлинности с помощью доверенного платформенного модуля (TPM) с персональным идентификационным номером (ПИН) или загрузочным ключом, а также однофакторную проверку подлинности с помощью ключа, хранящегося на USB-устройстве флэш-памяти, или с помощью доверенного модуля. Использование BitLocker с доверенным платформенным модулем TPM обеспечивает расширенную защиту данных и позволяет сохранить целостность загрузочных компонентов. Для этого варианта компьютер должен иметь совместимый микрочип доверенного платформенного модуля и совместимую версию BIOS. Доверенный платформенный модуль взаимодействует с технологией защиты диска операционной системы BitLocker для обеспечения безопасности при загрузке системы. Это происходит незаметно для пользователей, а процесс входа в систему не изменяется. Однако если изменены сведения загрузки, то BitLocker переведет компьютер в режим восстановления и потребует ввода пароля или ключа восстановления для получения доступа к данным.

Одной из важных функций BitLocker является BitLocker to Go, которая позволяет шифровать съемные накопители, такие как USB флэш-накопители. В этом случае, если съемный носитель украден или утерян, содержащиеся на нем данные не будут скомпрометированы. Шифрование не включено по умолчанию для USB носителей, однако шифрование BitLocker может быть включено либо администратором (в настройках групповой политики), либо конечным пользователем.

9.2 Последовательность выполнения работы

Часть 1. Шифрование файла

1. Выбрать защищаемый файл. С помощью правой кнопки мыши вызвать контекстное меню и выбрать пункт *Свойства*. На вкладке *Общие* в разделе *Атрибуты* нажать кнопку *Другие*. Откроется окно *Дополнительные атрибуты*. В этом окне в разделе *Атрибуты сжатия и шифрования* включить флажок *Шифровать содержимое для защиты данных*, нажать ОК. В окошке свойств документа высвечивается предупреждение при шифровании, где рекомендуется вместе с файлом зашифровать и содержащую его папку. Выбрать рекомендуемый вариант и нажать ОК.

Зашифрованные файлы обычно помечаются зеленым цветом, если это указано в настройках. Для проверки вызвать окно *Панель управления*, нажав на кнопку *Пуск*, открыть раздел «Параметры папок». Перейти на вкладку *Вид* и в разделе *Дополнительные параметры* установить флажок *Отображать сжатые или зашифрованные файлы NTFS другим цветом* (рис.3.1)

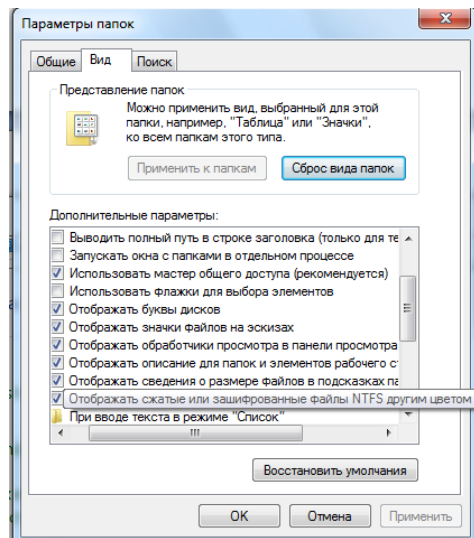


Рисунок 9.1. Окно «Параметры папок», вкладка «Вид»

2. Включение в контекстное меню пунктов для шифрования и дешифрования. Для удобства шифрования и дешифрования файлов можно включить в контекстное меню соответствующие пункты. Выполняется это путем редактирования реестра.

Для вызова утилиты редактирования реестра `regedit` в меню *Пуск* в строке *Поиск* набрать `regedit`. В окне программы выполнить двойной щелчок по `regedit.exe`. Откроется окно редактора. Перейти в раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced** и создать параметр: «**EncryptionContextMenu**»=**dword:00000001**» (рис.3.2)

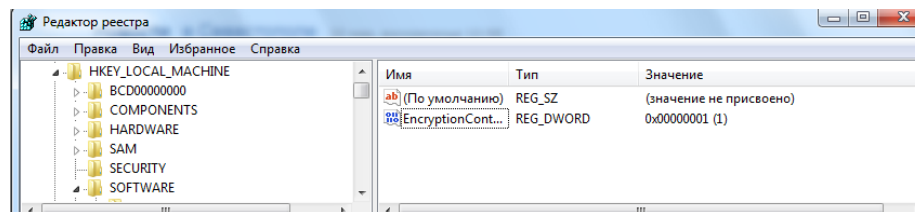


Рисунок 9.2 – Окно «Редактор реестра»

Для того, чтобы создать параметр, кликнуть правой кнопкой мышки на пустом месте в правой части окна «Редактор реестра», из контекстного меню выбрать *Создать > Параметр DWORD (32 бита)*. Появится параметр с именем *Новый параметр* и значением 00000000. Изменить имя *Новый параметр* на *EncryptionContextMenu*, выбрав в контекстного меню строку *Переименовать*. Затем выбрать пункт меню *Изменить двоичные данные*, и заменить первую группу 00 на 01.

Теперь в контекстное меню, вызываемое для любого файла, включены пункты «Зашифровать» и «Расшифровать».

3. Создание сертификатов ключей. При первом шифровании файлов или папок создается два ключа: открытый и закрытый. Открытым происходит шифрация ключа FEK, а закрытым дешифрация. Оба этих ключа (открытый и закрытый) помещаются в сертификат. Соответственно эти сертификаты можно экспортировать для расшифровки данных на другом компьютере.

Делается это следующим образом. В меню *Пуск* в строке *Поиск* набрать `mmc.exe`, в окне *Программы* выполнить двойной щелчок по `mmc` и запустить консоль.

В открывшейся консоли нажать **CTRL+M** или перейти в меню *Файл > Добавить или удалить оснастку* (рис.3.3)

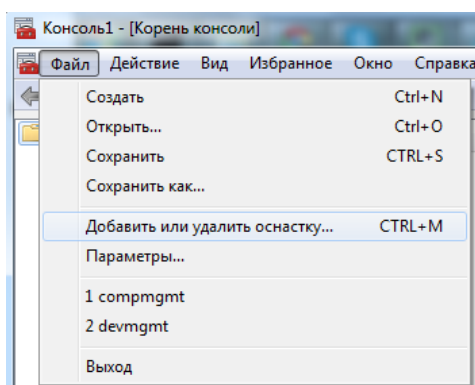


Рисунок 9.3. Добавление оснастки в консоль

В открывшемся окошке в разделе *Доступные оснастки* выбрать *Сертификаты* и нажать кнопку *Добавить* (рис.3.4)

Открывается окно *Добавление и удаление оснастки*, в котором нужно установить переключатель *моей учетной записи пользователя* и нажать *Готово*. Откроется окно *Добавление и удаление оснастки*, в котором нажать *ОК*.

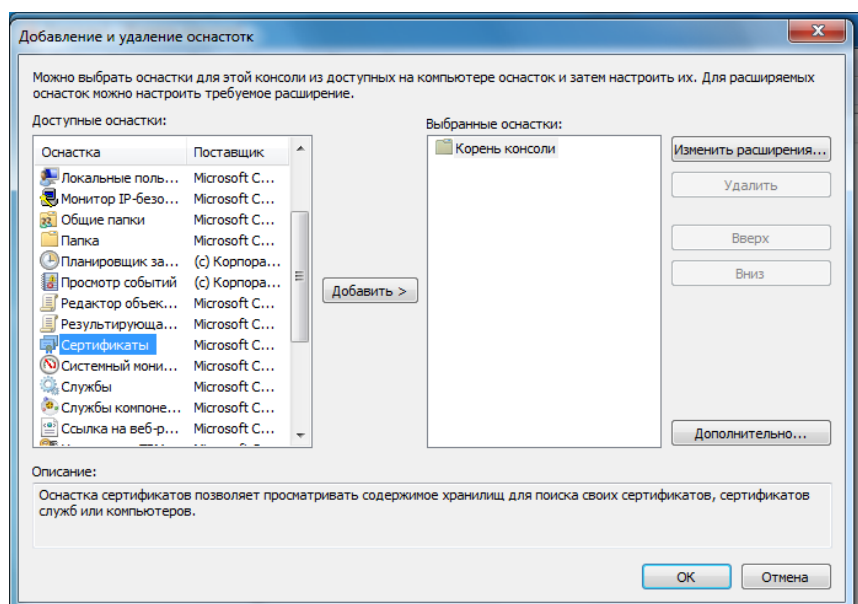


Рисунок 9.4.Добавление сертификатов

Происходит переключение на окно консоли, в левой части которого отображается дерево консоли. В дереве консоли перейти по пути *Сертификаты Личное > Сертификаты*. Выбрать созданный сертификат, в главном меню выполнить *Действия>Все задачи>Экспорт*. Открывается Мастер экспорта сертификатов. Нажать *Далее >* (рис.3.5)

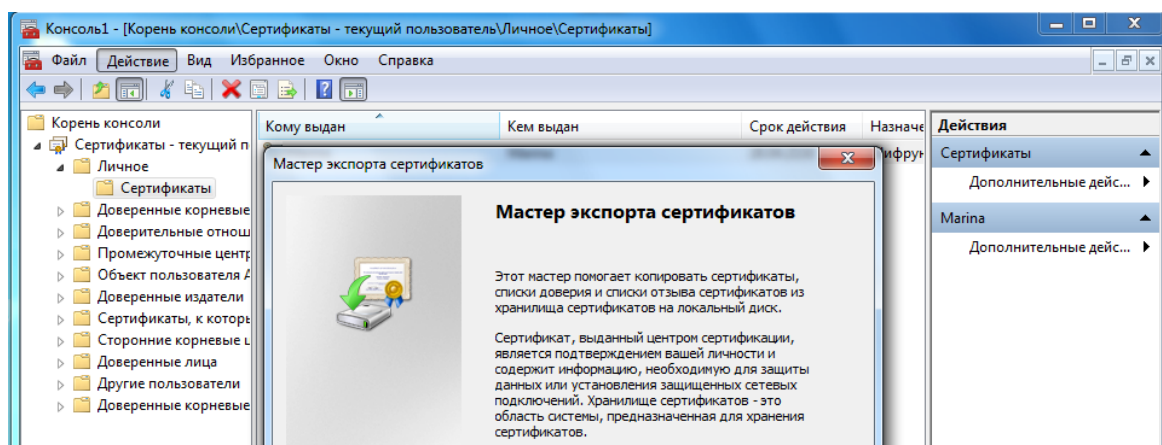


Рисунок 9.5. Запуск Мастера экспорта сертификатов

Можно экспортировать только свои ключи для расшифровки своих файлов. То есть, если другой пользователь установил свой сертификат с ключами для расшифровки своих файлов, его закрытый ключ экспортировать нельзя.

В окне *Экспортирование закрытого ключа* установить переключатель «Да, экспортировать закрытый ключ», нажать *Далее*.

В следующем окне Мастера сертификатов, ничего не меняя нажать *Далее* >. Задать пароль для защиты сертификата и ввести подтверждение пароля.

Далее необходимо указать расположение и имя экспортируемого файла. Нажать *Обзор*, рекомендуется выбрать съемный диск и ввести имя файла с ключами, например, key (рис.3.6)

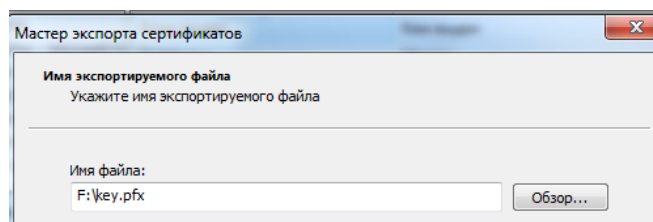


Рисунок 9.6. Сохранение сертификата

В заключительном окошке нажимаем Готово. Экспорт сертификата успешно выполнен в файл .pfx.

Для импорта сертификата на другом ПК достаточно запустить файл .pfx и следовать инструкциям мастера. Без сертификата не получится ни открыть файл, ни скопировать его. Будет возможность только удалить зашифрованный файл.

Установив сертификат, импортировать на тот же компьютер зашифрованные файл и расшифровать его.

Часть 2. Шифрование сменных носителей информации

Щелкнуть правой кнопкой по значку съемного диска в окне «Компьютер», в контекстном меню выбрать строку *Включить BitLocker*.

При выборе опции включения запускается Мастер шифрования диска. На первом шаге мастера Windows просит ввести пароль, который можно использовать для разблокирования диска (рис.9.7). Длина пароля должна быть не менее 8 символов. Имеется также опция использования смарт-карты для разблокировки диска.

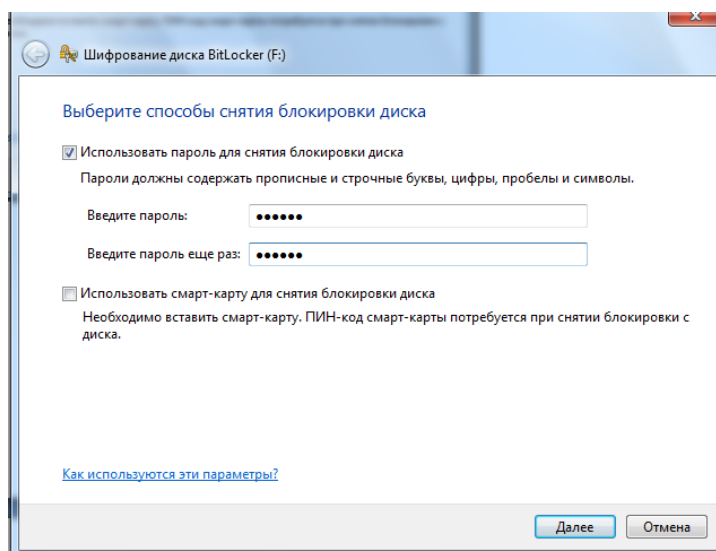


Рисунок 9.7. Способы блокировки диска

После ввода пароля, Windows генерирует ключ восстановления, и просит сохранить его в файл или распечатать. Кнопка *Далее* неактивна до тех пор, пока не будет выполнено, по крайней мере, одно из этих действий. Microsoft рекомендует сохранять или распечатывать ключ восстановления в качестве способа предотвращения потери данных, если пароль будет забыт.

После сохранения или распечатки ключа восстановления можно шифровать диск. Для этого нажать кнопку *Начать шифрование*.

Использование зашифрованного накопителя практически ничем не отличается от использования обычного съемного носителя. Если вставить флэш-накопитель в порт, система потребует ввода пароля. Значок диска теперь имеет значок висячего замка. При подключении зашифрованного накопителя система требует ввести пароль. После ввода пароля значок показывает, что диск разблокирован.

9.3 Содержание отчета

Цель работы; постановка задачи; описание выполнения заданий п.3.2, результаты выполнения заданий, выводы по работе.

9.4 Контрольные вопросы

- 1) Каковы цели шифрования?
- 2) Особенности шифрования файлов и папок в Windows 7.
- 3) Как зашифровать съемный диск?
- 4) Что такое сертификаты ключей?
- 5) Как включить в контекстное меню пункты шифровать и расшифровать?

10. ЛАБОРАТОРНАЯ РАБОТА №10. БРАНДМАУЭР WINDOWS

Цель работы: Ознакомиться со встроенными средствами защиты от сетевых угроз в ОС Windows 7.

10.1 Теоретические сведения

Брандмауэр, фаерволл, межсетевой или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основная задача - защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Система делит общую сеть на две части и определяет условия прохождения пакетов с данными через границу из одной части общей сети в другую.

В зависимости от уровня, на котором происходит контроль доступа, существует разделение на сетевые экраны, работающие на:

- сетевом уровне, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня и статических правил, заданных администратором;

- сеансовом уровне — отслеживающие сеансы между приложениями, не пропускающие пакеты, нарушающие спецификации TCP/IP.

- уровне приложений - фильтрация на основании анализа данных приложения, передаваемых внутри пакета. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации на основании политик и настроек.

Брандмауэр может быть как встроенным в операционную систему (например, брандмауэр Windows), так и устанавливаемым отдельно.

Брандмауэр Windows контролирует входящий и исходящий сетевой трафик подключений. При необходимости брандмауэр динамически открывает порты и позволяет компьютеру принимать запрошенный трафик, например сайт, адрес которого набран в браузере. "Порт" — это сетевой термин, обозначающий точку, через которую сетевой трафик поступает на компьютер. Открываемые порты зависят от типа трафика, который нужно отправить или получить.

Если входящий трафик не запрошен, брандмауэр подключения к интернету блокирует его до того, как он достигнет компьютера. В некоторых случаях, таких как работа в сети, установка онлайн-игр или собственного сервера, можно открыть некоторые порты. Это позволит другим пользователям подключаться к компьютеру, но может также снизить уровень безопасности.

Встроенные брандмауэры, в отличие от брандмауэров сторонних производителей, отличаются скромной функциональностью, но при этом работают без конфликтов с операционной системой. Еще одним существенным преимуществом является их бесплатность.

10.2 Последовательность выполнения работы

1. Для того чтобы открыть брандмауэр Windows выполните следующие действия:
Пуск → Панель управления → Система безопасности → Брандмауэр Windows. На экране появится меню Брандмауэр Windows (рис 4.1).

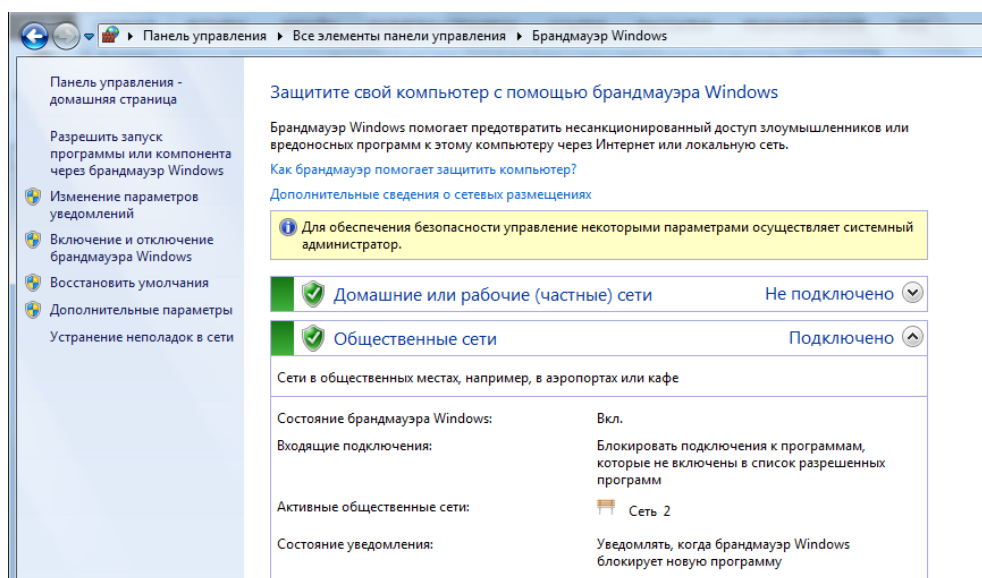


Рисунок 10.1- Окно Брандмауэра Windows

2. Стандартная настройка состояния — включен. Ссылка Включение и выключение Брандмауэра Windows позволяет менять режим работы. Отключить Брандмауэр Windows, а затем вновь включить его.

3. Переход по ссылке *Разрешить запуск программы*, которая находится в левой части окна Брандмауэр приведет к открытию окна «Разрешенные программы». Программы и службы, не блокируемые брандмауэром Windows, будут помечены флажками.

Можно добавлять приложения к этому списку. Это может быть необходимо, если у клиента имеется приложение, требующее связи с внешней сетью, но по какой-то причине брандмауэр Windows не может выполнить настройку автоматически. Для завершения данной процедуры необходимо войти в систему на этом компьютере в качестве администратора.

Перейти по ссылке *Риски разрешения связи для программы*. Откроется окно «Справка и поддержка». Ознакомьтесь с содержанием. Создание слишком большого числа исключений в файле «Программы и службы» может повлечь негативные последствия.

Закрыть окно «Справка и поддержка».

4. Выполнить команду *Пуск > Панель управления > Администрирование > Брандмауэр Windows в режиме повышенной безопасности > Правила для входящих подключений* (либо – *Брандмауэр – Дополнительные параметры*). Развернуть окно, чтобы можно было увидеть полное имя правил для входящих подключений. Найти «Общий доступ к файлам и принтерам (эхо-запрос – входящий трафик ICMPv4)». Щёлкнуть правило правой кнопкой мыши, выбрать *Свойства > вкладка Дополнительно*. Нажать кнопку *Настроить* (рисунок 10.2).

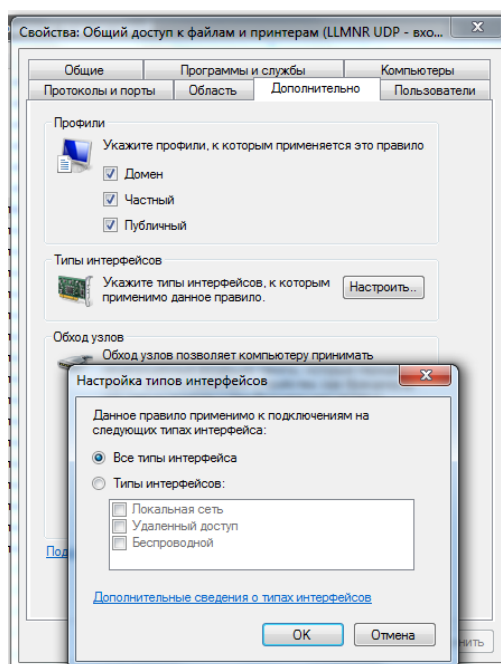


Рисунок 10.2-Настройка типов интерфейса

На вкладке «Дополнительно» отображаются профили, используемые компьютером, а в окне «Настройка типов интерфейсов» отображаются различные подключения, настроенные на компьютере. Нажать кнопку ОК.

Перейти на вкладку *Программы и службы*. Откроется окно «Настройка параметров службы» (рисунок 10.3). Нажать кнопку Параметры.

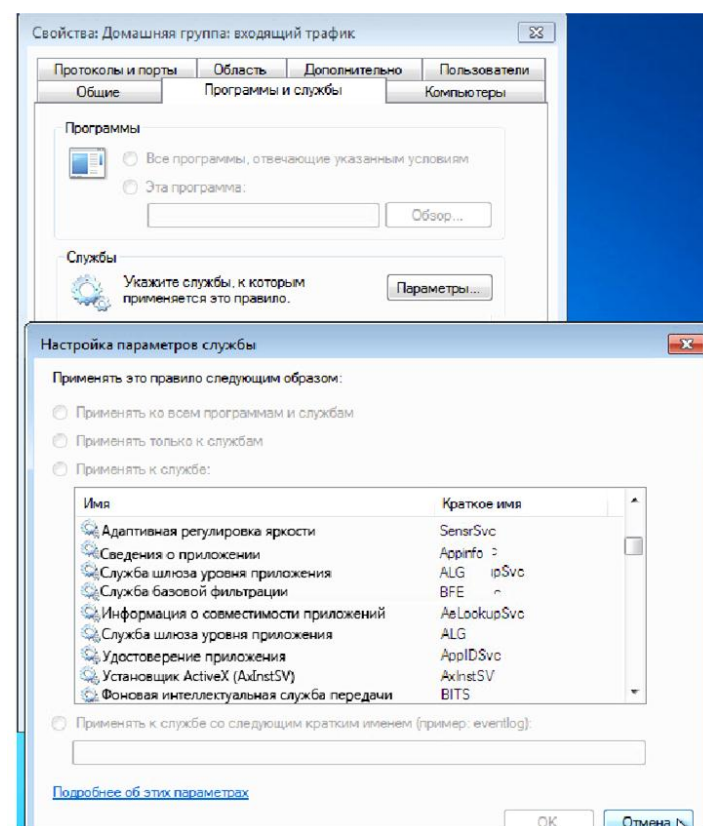


Рисунок 10.3-Настройка параметров служб

В пространстве ниже перечислить краткие имена четырёх доступных служб. Нажать кнопку Отмена.

5. Существует множество приложений, обычно незаметных для пользователя, которым необходимо иметь доступ к компьютеру через брандмауэр Windows. Это команды уровня сети, направляющие трафик в сети и Интернете

Перейти на вкладку *Протоколы и порты*. Для настройки ICMP нажать кнопку *Настроить*. Можно будет увидеть меню, в котором настраиваются исключения ICMP (рис.10.4).

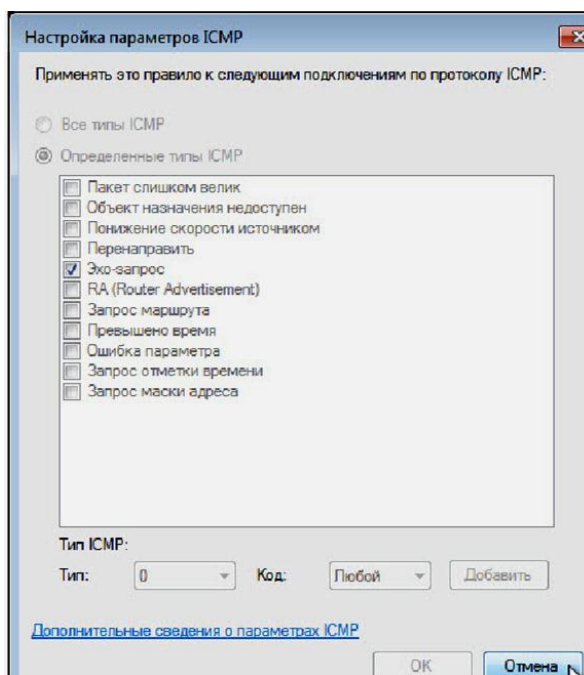


Рисунок 10.4- Настройка параметров ICMP.

В этом примере разрешение входящих эхо-запросов позволяет пользователям сети запрашивать, присутствует ли в ней компьютер. Оно также позволяет видеть, насколько быстро передается информация к компьютеру и от него.

6. Вернуться в окно «Правила для входящих подключений». На вкладке «Действия» с помощью команды «Создать правило» настроить параметры некоторых приложений:

6.1 FTP-клиент: тип: исходящие подключения; протокол: TCP; IP адрес источника: любой, порт источника: любой, IP адрес назначения: любой, порт назначения: 20, 21; действие: разрешить.

6.2 Клиент ICQ: тип: исходящие подключения; протокол: TCP; IP адрес источника: любой, порт источника: любой; IP адрес назначения: 64.12.0.0/16, 205.188.0.0/16; порт назначения: 5190; действие: разрешить.

6.3 Клиент Torrent: тип: исходящие подключения; протокол: TCP; IP адрес источника: любой, порт источника: любой, IP адрес назначения: любой; порт назначения: любой; действие: разрешить.

6.4 Клиент Torrent: тип: входящие подключения; протокол: TCP; IP адрес источника: любой, порт источника: любой, IP адрес назначения: любой; порт назначения: любой; действие: разрешить.

7. Выполнить команду Брандмауэр – Восстановить умолчания.

10.3 Содержание отчета

Цель работы; постановка задачи; описание выполнения заданий п.4.2, результаты выполнения заданий, выводы по работе.

10.4 Контрольные вопросы

- 1) Что такое брандмауэр?
- 2) Цель применения брандмауэра.
- 3) Как включить и выключить брандмауэр?
- 4) Как создать правила фильтрации подключений?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Таненбаум Э. Современные операционные системы. / Э. Таненбаум. –СПб.: Питер, 2011. –1120 с.
2. Stallings W. Operatings Systems. Internals and Design Principles/ W. Stallings.–Sevents Edition. – 2012.– 768 с.
3. Дейтел Х.М. Операционные системы. Том 1. Основы и принципы/ Х.М. Дейтел, П.Дж.Дейтел, Д.Р.Чофнес .–М.: Изд. Бином – 2011. – 1024 с.
4. Информатика: базовый курс: учеб. пособие для студ. вузов/ Ред. С. В. Симонович. - СПб. и др. : Питер, 2008. - 640 с.
5. Лабораторный практикум по информатике и компьютерным технологиям: учеб. пособие для студ. вузов / Харьк. гос. экон. ун-т ; Ред. А. И. Пушкарь. - Харьков : ИНЖЭК, 2004. - 466 с.
6. Мезенцева, Е.М. Операционные системы. Лабораторный практикум / Е.М. Мезенцева, О.С. Коняева, С.В. Малахов.– Самара: ПГУТИ, 2017. – 216 с.
7. Методические указания к выполнению лабораторных работ по дисциплине «Безопасность операционных систем» для магистров ОФО по направлению 38.04.08 «Финансы и кредит», профиль подготовки «Финансовый мониторинг»/ Сост. ст. преподаватель кафедры ИТиКС М.А. Лебедева. – Севастополь: Изд-во СГУ, 2016.– 36с.
8. <https://okeygeek.ru/pyat-sposobov-otkryt-komandnuyu-stroku-v-windows-10/>