

### Лабораторная работа №3

#### Работа с командной строкой. Сетевая активность.

**Цель работы:** Получение практических навыков по работе с Командной строкой и по выявлению вредоносных программ на локальном компьютере под управлением Microsoft Windows XP с помощью командной строки.

#### Теоретическая часть

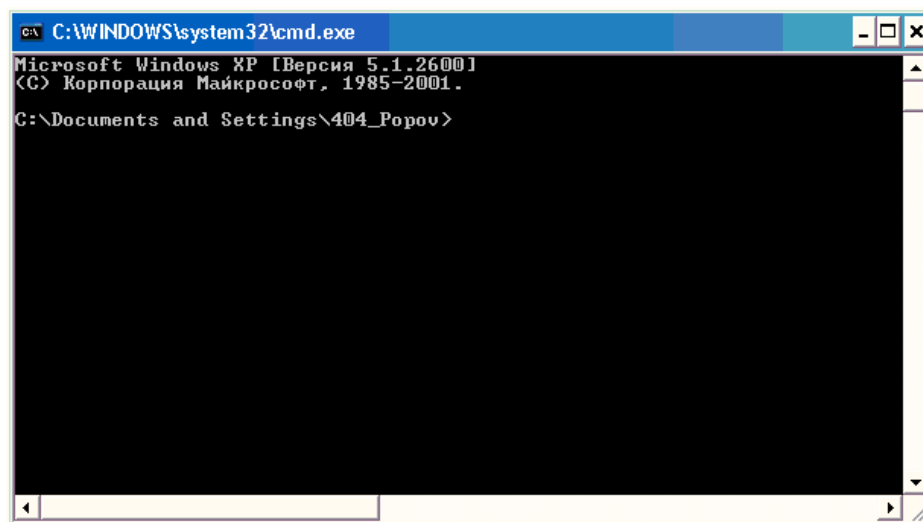
##### Работа с Командной строкой

В операционной системе Windows, как и в других операционных системах, интерактивные (набираемые с клавиатуры и сразу же выполняемые) команды выполняются с помощью так называемого командного интерпретатора, иначе называемого командным процессором или оболочкой командной строки (command shell). Командный интерпретатор или оболочка командной строки — это программа, которая, находясь в оперативной памяти, считывает набираемые вами команды и обрабатывает их. В Windows 9x, как и в MS-DOS, командный интерпретатор по умолчанию был представлен исполняемым файлом `command.com`. Начиная с версии Windows NT, в операционной системе реализован интерпретатор команд `Cmd.exe`, обладающий гораздо более мощными возможностями.

В Windows NT/2000/XP файл `Cmd.exe`, как и другие исполняемые файлы, соответствующие внешним командам операционной системы, находятся в каталоге `%SystemRoot%\SYSTEM32` (значением переменной среды `%SystemRoot%` является системный каталог Windows, обычно `C:\Windows` или `C:\WinNT`).

#### Задание 1. Работа с Командной строкой

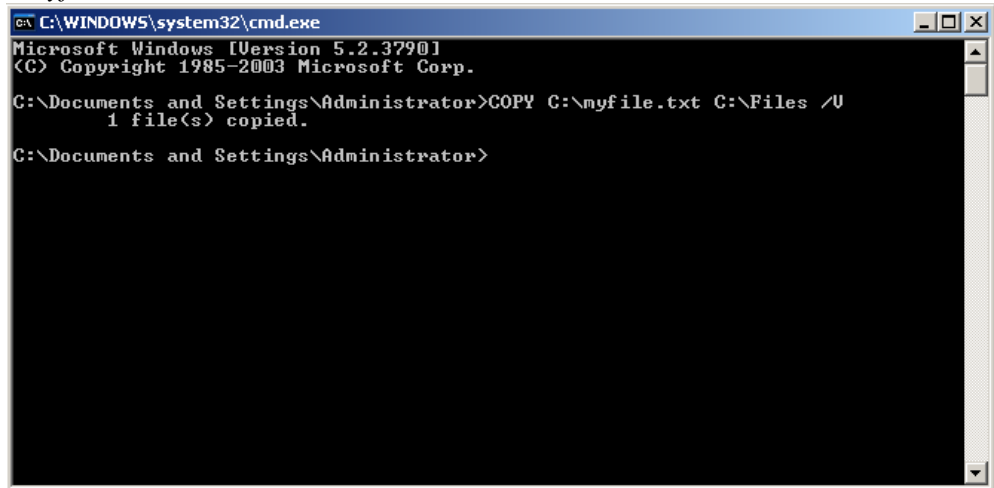
1. Для запуска командного интерпретатора (открытия нового сеанса Командной строки) можно выбрать пункт Пуск / Выполнить, ввести имя файла `Cmd.exe` и нажать кнопку ОК. В результате откроется новое окно, в котором можно запускать команды и видеть результат их работы.



Некоторые команды распознаются и выполняются непосредственно самим командным интерпретатором — такие команды называются внутренними (например, `copy` или `dir`). Другие команды операционной системы 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`).

2. Для того, чтобы выполнить команду, вы после приглашения командной строки (например, `C>`) вводите имя этой команды (регистр не важен), ее параметры и ключи (если они необходимы) и нажимаете клавишу `<Enter>`. Создайте на диске C файл `myfile.txt` и папку `Files`. В Командной строке наберите

*copy C:\myfile.txt C:\Files /V*



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

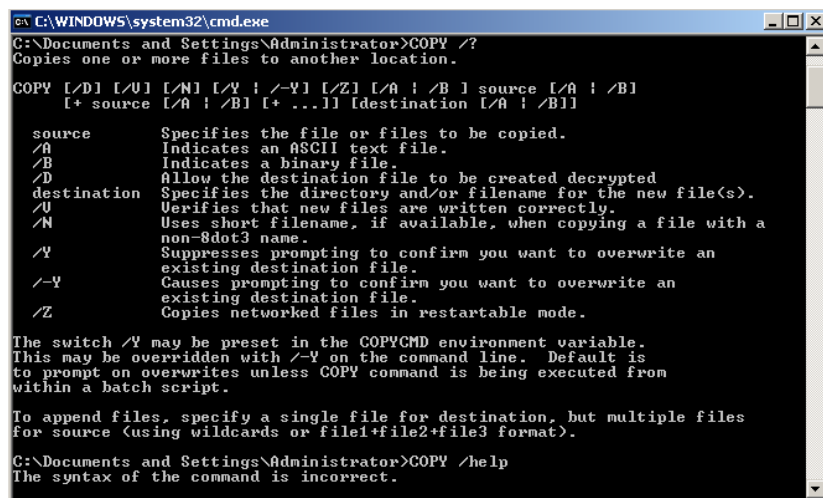
C:\Documents and Settings\Administrator>COPY C:\myfile.txt C:\Files /V
1 file(s) copied.

C:\Documents and Settings\Administrator>
```

Имя команды здесь — *copy*, параметры — *C:\myfile.txt* и *C:\Files*, а ключом является */V*. Отметим, что в некоторых командах ключи могут начинаться не с символа */*, а с символа *-* (минус), например, *-V*.

3. Многие команды Windows имеют большое количество дополнительных параметров и ключей, запомнить которые зачастую бывает трудно. Большинство команд снабжено встроенной справкой, в которой кратко описываются назначение и синтаксис данной команды. Получить доступ к такой справке можно путем ввода команды с ключом */?* или */help*. В командной строке наберите

*copy /?*



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>COPY /?
Copies one or more files to another location.

COPY [/D] [/U] [/N] [/Y | /-Y] [/Z] [/A | /B] source [/A | /B]
[+ source [/A | /B] [+ ...]] [destination [/A | /B]]

source      Specifies the file or files to be copied.
/A          Indicates an ASCII text file.
/B          Indicates a binary file.
/D          Allow the destination file to be created decrypted
destination Specifies the directory and/or filename for the new file(s).
/U          Verifies that new files are written correctly.
/N          Uses short filename, if available, when copying a file with a
non-8dot3 name.
/Y          Suppresses prompting to confirm you want to overwrite an
existing destination file.
/-Y         Causes prompting to confirm you want to overwrite an
existing destination file.
/Z          Copies networked files in restartable mode.

The switch /Y may be preset in the COPYCMD environment variable.
This may be overridden with /-Y on the command line. Default is
to prompt on overwrites unless COPY command is being executed from
within a batch script.

To append files, specify a single file for destination, but multiple files
for source (using wildcards or file1+file2+file3 format).

C:\Documents and Settings\Administrator>COPY /help
The syntax of the command is incorrect.
```

*shutdown /help*

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>shutdown /help
Usage: shutdown [/i] [/s] [/r] [/a] [/p] [/h] [/e] [/f]
[/m \\computer1] [/t xxx] [/d lp:xx:yy] [/c "comment"]

No args      Display help. This is the same as typing /?
/?          Display help. This is the same as not typing any options
/i          Display the graphical user interface (GUI).
            This must be the first option
/l          Log off. This cannot be used with /m or /d option
/s          Shutdown the computer
/r          Shutdown and restart the computer
/a          Abort a system shutdown.
            This can only be used during the time-out period
/p          Turn off the local computer with no time-out or warning.
            This can only be used with /d option
/h          Hibernates the local computer.
            This can only be used with the /f option
/e          Document the reason for an unexpected shutdown of a computer
/m \\computer Specify the target computer
/t xxx      Set time-out period before shutdown to xxx seconds.
            The valid range is 0-600, with a default of 30
/c "comment" Comment on the reason for the restart or shutdown.
            Maximum of 127 characters allowed
/f          Force running applications to close without forewarning users
/d lp:xx:yy Provide the reason for the restart or shutdown
            p indicates that the restart or shutdown is planned
            xx is the major reason number (positive integer less than 256)
            yy is the minor reason number (positive integer less than 65536)

Reasons on this computer:
(E = Expected U = Unexpected P = planned, C = customer defined)
Type Major Minor Title
U 0 0 Other (Unplanned)
E P 0 0 Other (Unplanned)
U 0 5 Other Failure: System Unresponsive
E P 1 1 Hardware: Maintenance (Unplanned)
E P 1 1 Hardware: Maintenance (Planned)
E P 1 2 Hardware: Installation (Unplanned)
E P 1 2 Hardware: Installation (Planned)
E P 2 3 Operating System: Upgrade (Planned)
E P 2 4 Operating System: Reconfiguration (Unplanned)
E P 2 4 Operating System: Reconfiguration (Planned)
E P 2 16 Operating System: Service pack (Planned)
E P 2 17 Operating System: Hot fix (Unplanned)
P 2 17 Operating System: Hot fix (Planned)
P 2 18 Operating System: Security fix (Unplanned)
P 2 18 Operating System: Security fix (Planned)
E P 4 1 Application: Maintenance (Unplanned)
E P 4 1 Application: Maintenance (Planned)
E P 4 2 Application: Installation (Planned)
E P 4 5 Application: Unresponsive
E 4 6 Application: Unstable
```

help

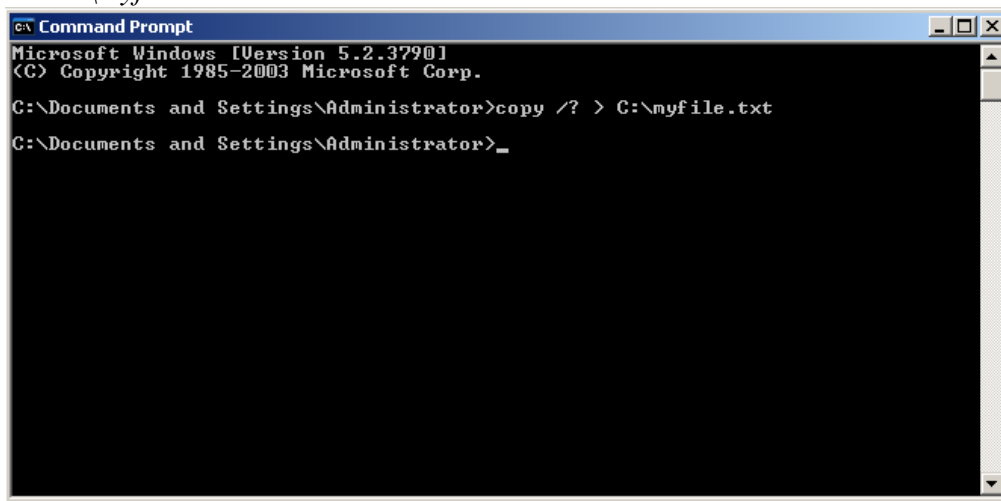
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>help
For more information on a specific command, type HELP command-name
ASSOC      Displays or modifies file extension associations.
ATTRIB     Displays or changes file attributes.
BREAK      Sets or clears extended CTRL+C checking.
BOOTCFG    Sets properties in boot.ini file to control boot loading.
CACLS      Displays or modifies access control lists (ACLs) of files.
CALL       Calls one batch program from another.
CD          Displays the name of or changes the current directory.
CHCP       Displays or sets the active code page number.
CHDIR      Displays the name of or changes the current directory.
CHKDSK     Checks a disk and displays a status report.
CHKNTFS    Displays or modifies the checking of disk at boot time.
CLS        Clears the screen.
CMD        Starts a new instance of the Windows command interpreter.
COLOR      Sets the default console foreground and background colors.
COMP       Compares the contents of two files or sets of files.
COMPACT    Displays or alters the compression of files on NTFS partitions.
CONVERT    Converts FAT volumes to NTFS. You cannot convert the
            current drive.
COPY       Copies one or more files to another location.
DATE       Displays or sets the date.
DEL        Deletes one or more files.
DIR        Displays a list of files and subdirectories in a directory.
DISKCOMP   Compares the contents of two floppy disks.
DISKCOPY   Copies the contents of one floppy disk to another.
DISKPART   Displays or configures Disk Partition properties.
DOSKEY     Edits command lines, recalls Windows commands, and
            creates macros.
DRIVERQUERY Displays current device driver status and properties.
ECHO       Displays messages, or turns command echoing on or off.
ENDLOCAL   Ends localization of environment changes in a batch file.
ERASE      Deletes one or more files.
EVENTVLOG  Displays event log entries for specified criteria.
EXIT       Exits the CMD.EXE program (Command interpreter).
FC         Compares two files or sets of files, and displays the
            differences between them.
FIND       Searches for a text string in a file or files.
FINDSTR    Searches for strings in files.
FOR        Runs a specified command for each file in a set of files.
FORMAT     Formats a disk for use with Windows.
FSUTIL     Displays or configures the file system properties.
FTYPE      Displays or modifies file types used in file extension
            associations.
GOTO       Directs the Windows command interpreter to a labeled line in
            a batch program.
GPRESULT   Displays Group Policy information for machine or user.
GRAFTABL   Enables Windows to display an extended character set in
            graphics mode.
HELP       Provides Help information for Windows commands.
IF         Performs conditional processing in batch programs.
LABEL      Creates, changes, or deletes the volume label of a disk.
MD         Creates a directory.
MKDIR      Creates a directory.
MODE       Configures a system device.
```

Последняя команда выводит список основных команд Командной строки

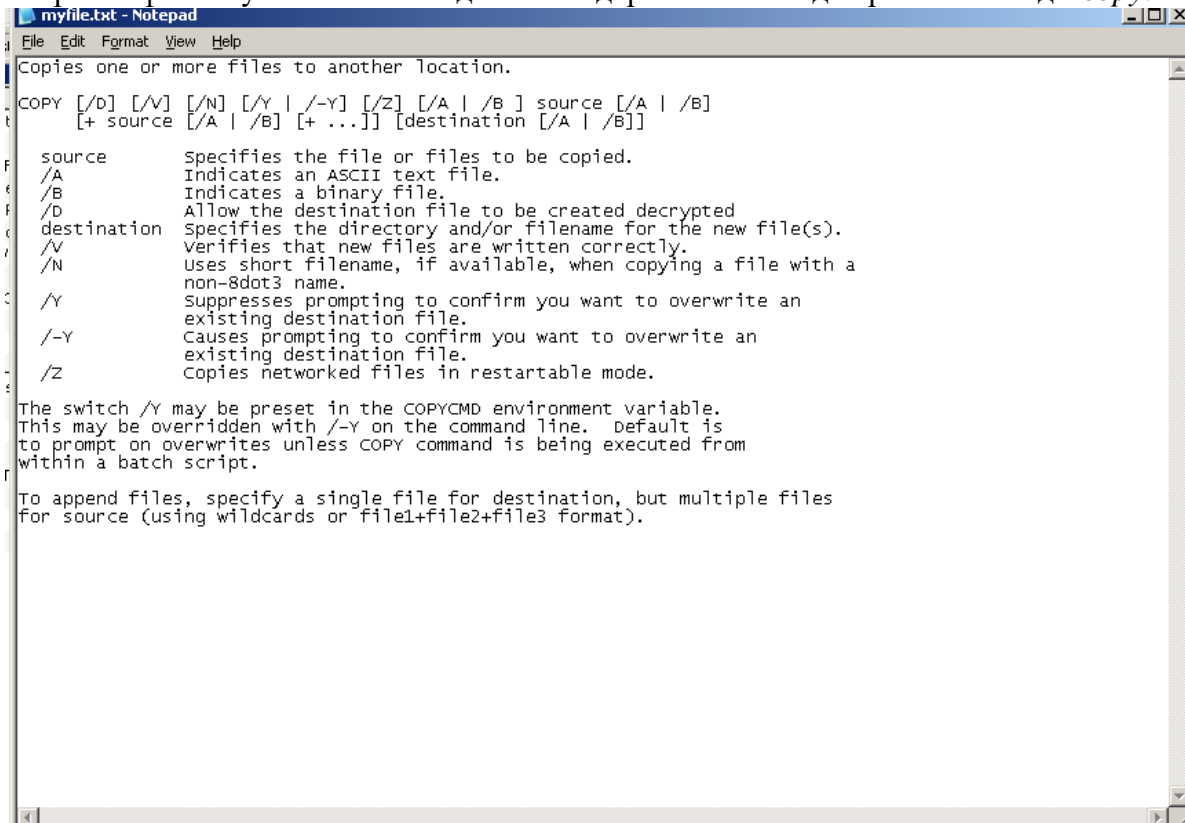
4. С помощью переназначения устройств ввода/вывода одна программа может направить свой вывод на вход другой или перехватить вывод другой программы, используя его в качестве своих входных данных. Таким образом, имеется возможность передавать информацию от процесса к процессу при минимальных программных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

*copy /? > C:\myfile.txt*



Откройте файл *myfile.txt* – в нем должен содержаться вывод справки команды *copy*.



5. С помощью символа < можно прочитать входные данные для заданной команды не с клавиатуры, а из определенного (заранее подготовленного) файла. На диске C создайте файл *date.txt* и напишите в нем 20.10.2009. В Командной строке наберите

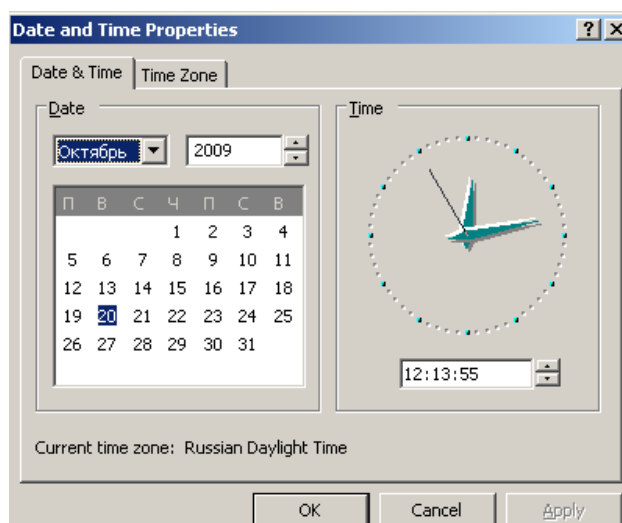
*Date < C:\date.txt*

```
C:\ Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>date < C:\date.txt
The current date is: 21.10.2008
Enter the new date: <dd-mm-yy> 20.10.2009

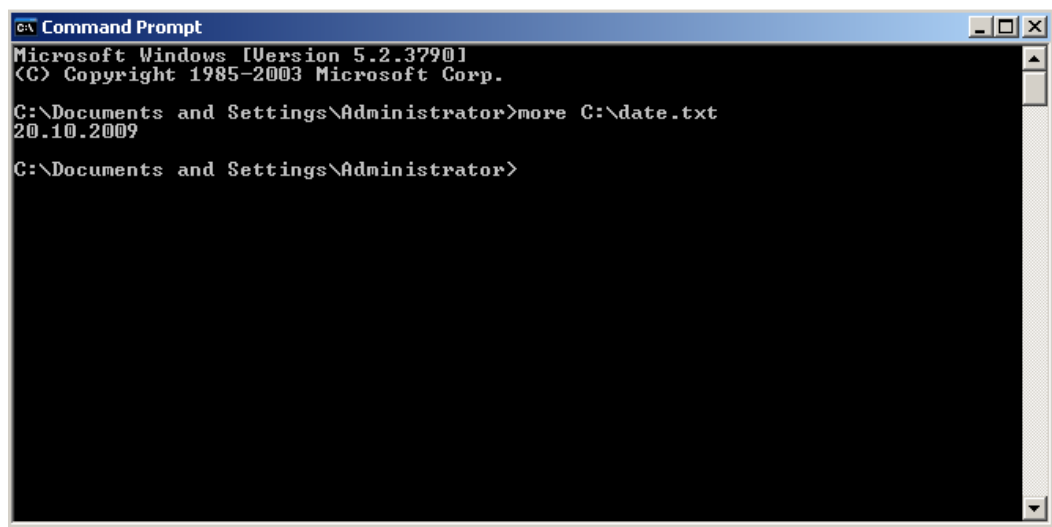
C:\Documents and Settings\Administrator>_
```

Проверьте дату на вашем компьютере, она должна измениться на 20.10.2009



6. Одной из наиболее часто использующихся 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. В Командной строке наберите

*More C:\date.txt*



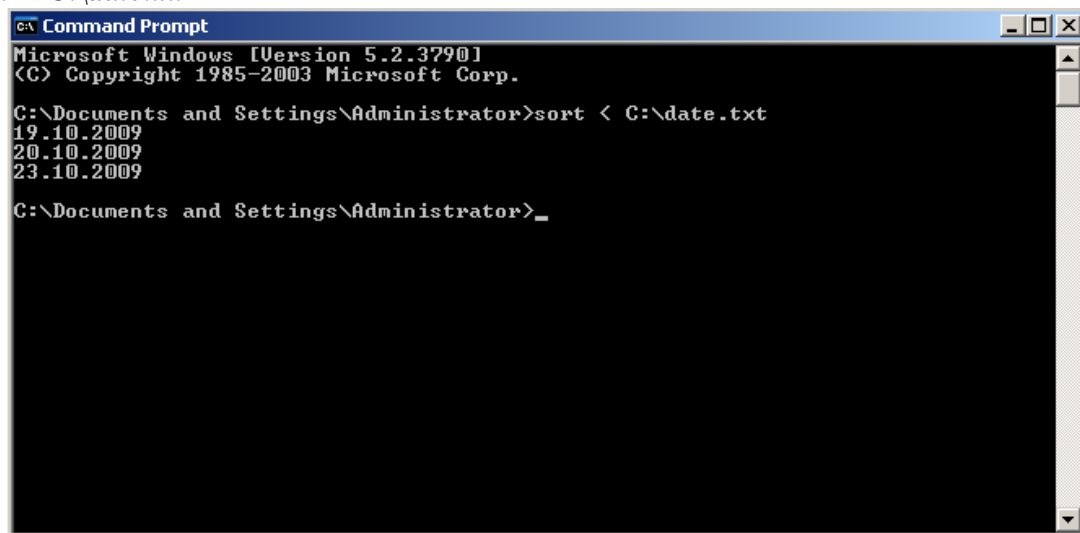
```
GA Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>more C:\date.txt
20.10.2009

C:\Documents and Settings\Administrator>
```

7. 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. В командной строке наберите

*sort < C:\date.txt*

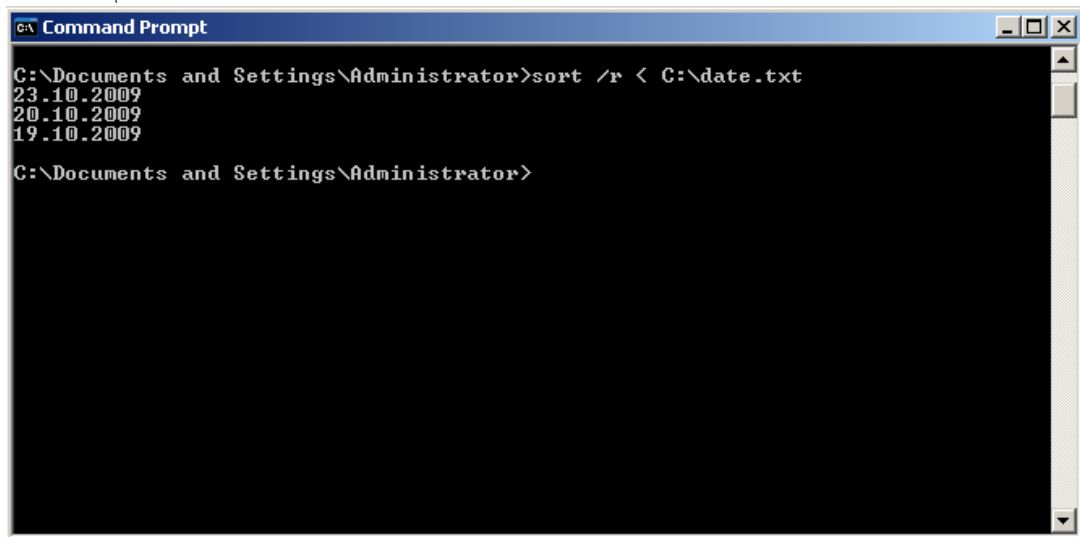


```
GA Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>sort < C:\date.txt
19.10.2009
20.10.2009
23.10.2009

C:\Documents and Settings\Administrator>_
```

*sort /r < C:\date.txt*



```
GA Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>sort /r < C:\date.txt
23.10.2009
20.10.2009
19.10.2009

C:\Documents and Settings\Administrator>
```

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).

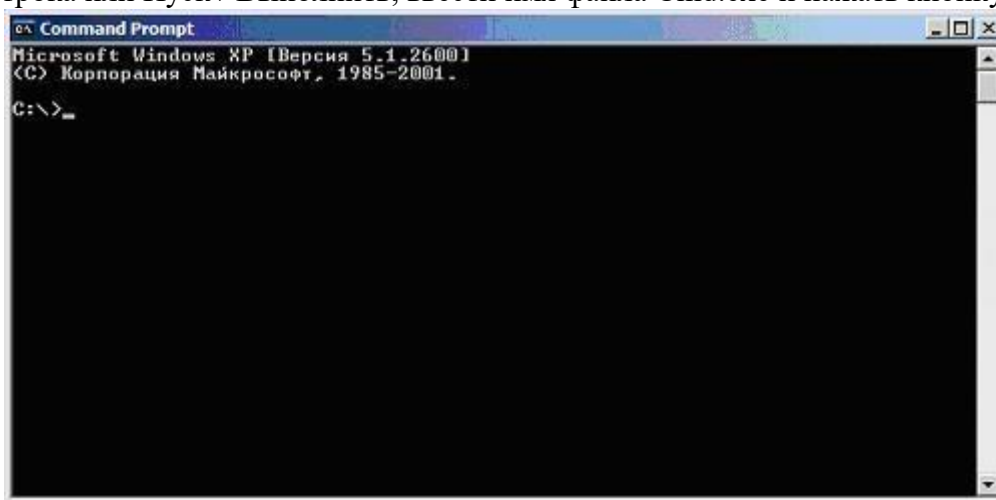
### Сетевая активность

Неожиданно возросшая сетевая активность может служить ярким свидетельством работы на компьютере подозрительной программы, производящей несанкционированную рассылку писем, связывающейся со своим автором и передающей ему конфиденциальную информацию или просто загружающую свои дополнительные модули или атакующей соседние компьютеры. Но при этом нужно не забывать, что ряд вполне легальных приложений также имеют свойство иногда связываться с сайтом фирмы-производителя, например для проверки наличия обновлений или более новых версий. Поэтому, прежде чем отключать сеть и выдергивать сетевой шнур, увидев необычно яркое мигание лампочки на сетевой карте, необходимо уметь определять какие программы и приложения вызвали эту подозрительную активность.

Изучить и проанализировать сетевую активность можно с помощью встроенных в операционную систему инструментов или же воспользовавшись специальными отдельно устанавливаемыми приложениями. Это можно сделать при помощи Диспетчера задач Windows, но он показывает только самую общую информацию. Для получения более подробных данных нужно воспользоваться утилитой *netstat*, которая выводит на экран мгновенную статистику сетевых соединений.

#### Задание 2. Сетевая активность

1. Воспользуйтесь системным меню Пуск / Программы / Стандартные / Командная строка или Пуск / Выполнить, ввести имя файла *Cmd.exe* и нажать кнопку ОК



2. В Командной строке наберите *netstat /?*
3. Прочитайте описание утилиты *netstat*. Убедитесь, что для вывода самой полной информации нужно использовать ключ *-a*



```

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.

```

4. В Командной строке наберите

*netstat -a*

5. Результатом выполнения команды является список активных подключений, в который входят установленные соединения и открытые порты.

```

C:\WINDOWS\system32\cmd.exe

компонентов, участвующих в создании подключения, или ожидающий
порт для всех исполняемых файлов.
интервал Повторный вывод статистических данных через указанный
промежуток времени в секундах. Для прекращения вывода данных
нажмите клавиши CTRL+C. Если параметр не задан, сведения о
текущей конфигурации выводятся один раз.

C:\>netstat -a

Активные подключения

Имя      Локальный адрес      Внешний адрес      Состояние
TCP      ivan:ermap           ivan.lab.kl:0      LISTENING
TCP      ivan:microsoft-ds    ivan.lab.kl:0      LISTENING
TCP      ivan:1110            ivan.lab.kl:0      LISTENING
TCP      ivan:netbios-ssn     ivan.lab.kl:0      LISTENING
UDP      ivan:microsoft-ds    **
UDP      ivan:isakmp          **
UDP      ivan:4500            **
UDP      ivan:netbios-ns      **
UDP      ivan:netbios-dgm     **
UDP      ivan:1027            **

```

TCP-порты обозначаются строкой "TCP" в колонке Имя. 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.

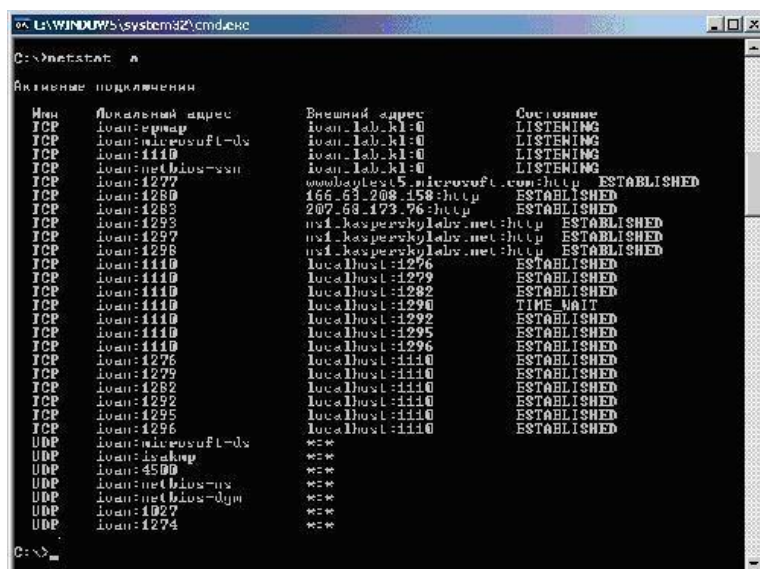
6. Команда *netstat*, в отличие от Диспетчера задач Windows, не работает в режиме реального времени, а отображает мгновенную статистику. Следовательно, для просмотра активности соединений, скажем, через минуту, нужно заново выполнить команду. В Командной строке наберите

*netstat -a*

и посмотрите не изменения

7. Исследуйте полученную статистику





8. Закройте окно командной строки. В Командной строке наберите *Exit*

**Оборудование и материалы:** для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows XP и программными продуктами: MS Word, Adobe Reader.

**Указания по технике безопасности:** к выполнению практических занятий допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

**Задания:** для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

**Содержание отчета:** отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выровнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчета приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

**Контрольные вопросы:**

1. Что такое командный интерпретатор или оболочка командной строки?
2. Как запустить командную строку?
3. Какие команды называются внутренними, а какими внешними?
4. Что необходимо сделать, чтобы выполнить команду?
5. Как можно получить справку о команде?
6. Как прочитать входные данные для заданной команды не с клавиатуры, а из определенного файла?
7. Что такое сетевая активность? Назовите ее особенности.
8. Как можно изучить и проанализировать сетевую активность?
9. Для чего нужна команда netstat?