

Лабораторная работа 3

Тема :Работа с командной строкой. Сетевая активность. Пакетные файлы.

Цель работы: получение практических навыков по работе с Командной строкой и по выявлению вредоносных программ на компьютере с Microsoft Windows XP с помощью Командной строки.

Задание 1. Работа с Командной строкой

В операционной системе Windows 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**).

Таким образом, оболочка командной строки — это отдельный программный продукт, который обеспечивает прямую связь между пользователем и операционной системой. Текстовый пользовательский интерфейс командной строки предоставляет среду, в которой выполняются приложения и служебные программы с текстовым интерфейсом. В операционных системах Windows 9.x командный интерпретатор был представлен исполняемым файлом command.com (как и в MS-DOS). Начиная с Windows NT он реализован cmd.exe и обладает большими возможностями.

В Windows XP файл **Cmd.exe**, как и другие исполняемые файлы, соответствующие внешним командам операционной системы, находятся в каталоге SYSTEM32.

1. Для открытия сеанса работы с командной строкой выберите **Пуск->Выполнить**. В открывшемся окне наберите **cmd** и нажмите на ОК.

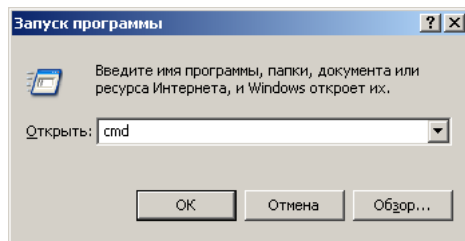


Рис. 1.

В результате откроется новое окно, в котором можно запускать команды и видеть результат их работы.

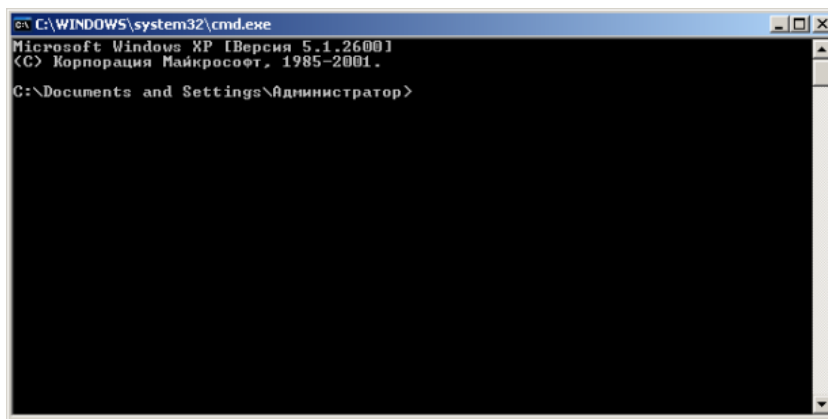
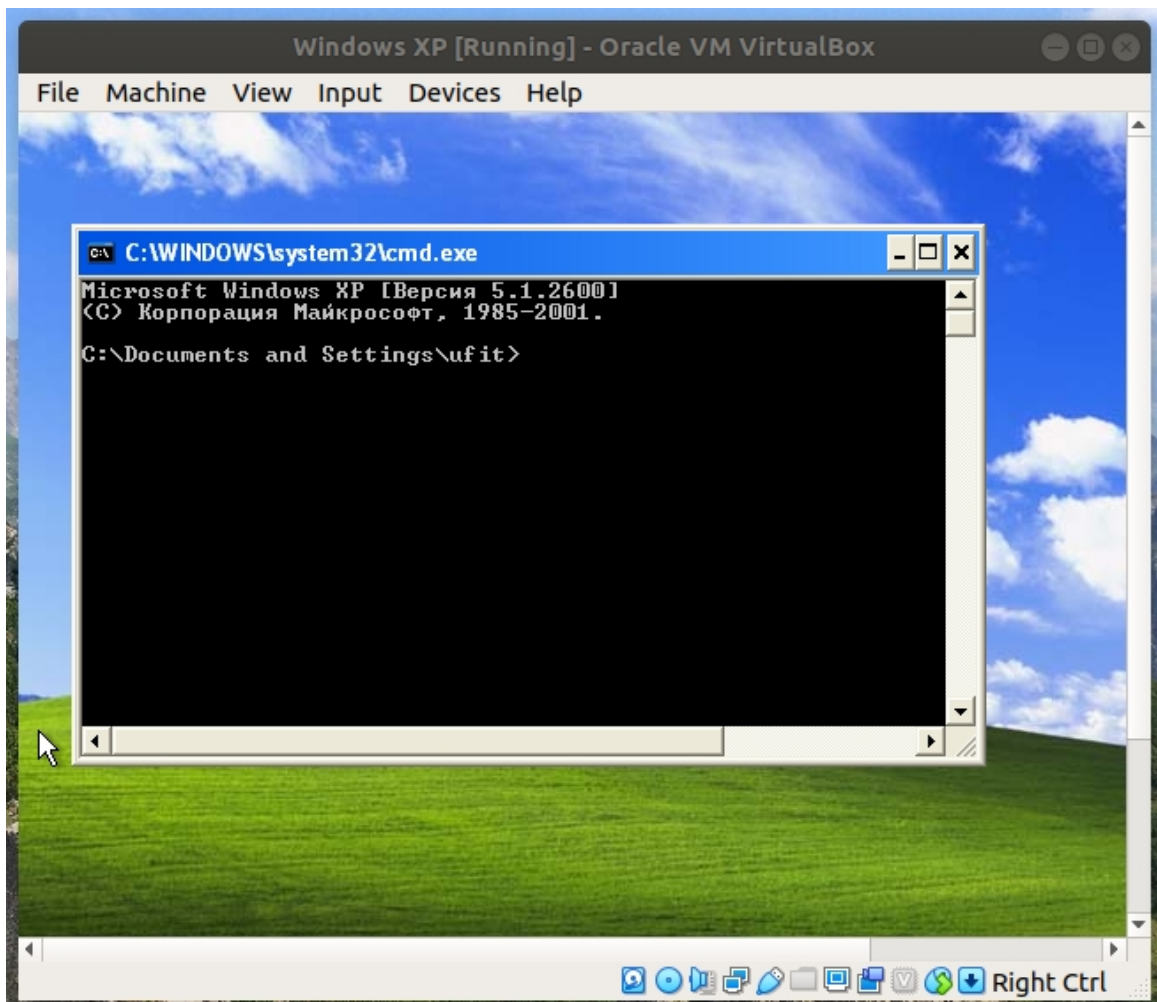


Рис. 2.

Некоторые команды распознаются и выполняются непосредственно самим командным интерпретатором — такие команды называются **внутренними** (например, `сору` 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 `хсорух`).

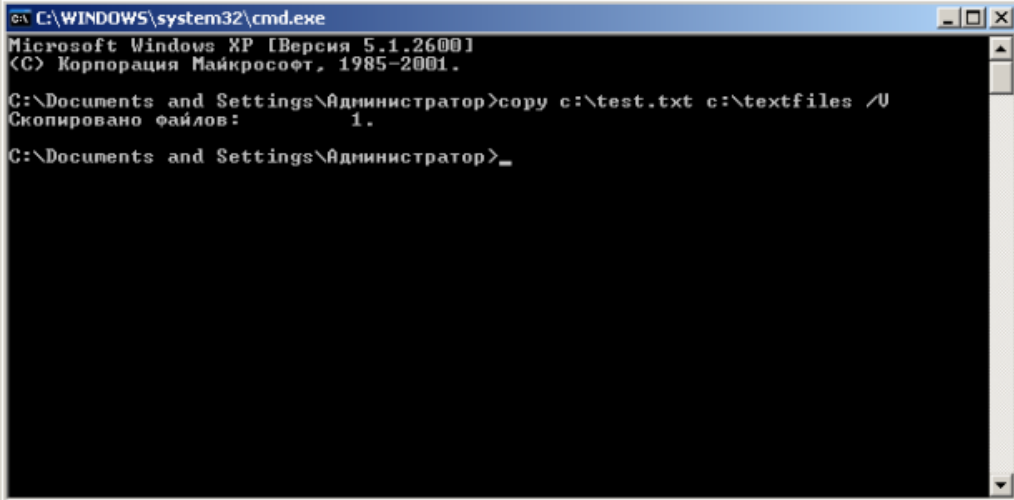


2. Для того чтобы выполнить команду введите имя этой команды (регистр не важен), ее параметры и ключи (если они необходимы) и нажмите клавишу Enter. Синтаксическая структура выводится в том порядке, в котором следует вводить команду и следующие за ней параметры, если они есть. Следующий пример команды хсору иллюстрирует разнообразие синтаксических форматов текста.

хсору источник [результат] [/w] [/p] [/c] [/v] [/q] [/f] [/l] [/g] [/d[:мм-дд-гггг]] [/u] [/i] [/s [/e]] [/t] [/k] [/r] [/h] [{/a/m}] [/n] [/o] [/x] [/exclude:файл1[+[файл2]][+[файл3]] [{/y/-y}] [/z]

Создайте на диске С файл **test.txt** и папку **Text files**. В Командной строке наберите

copy C:\test.txt C:\Textfiles /V

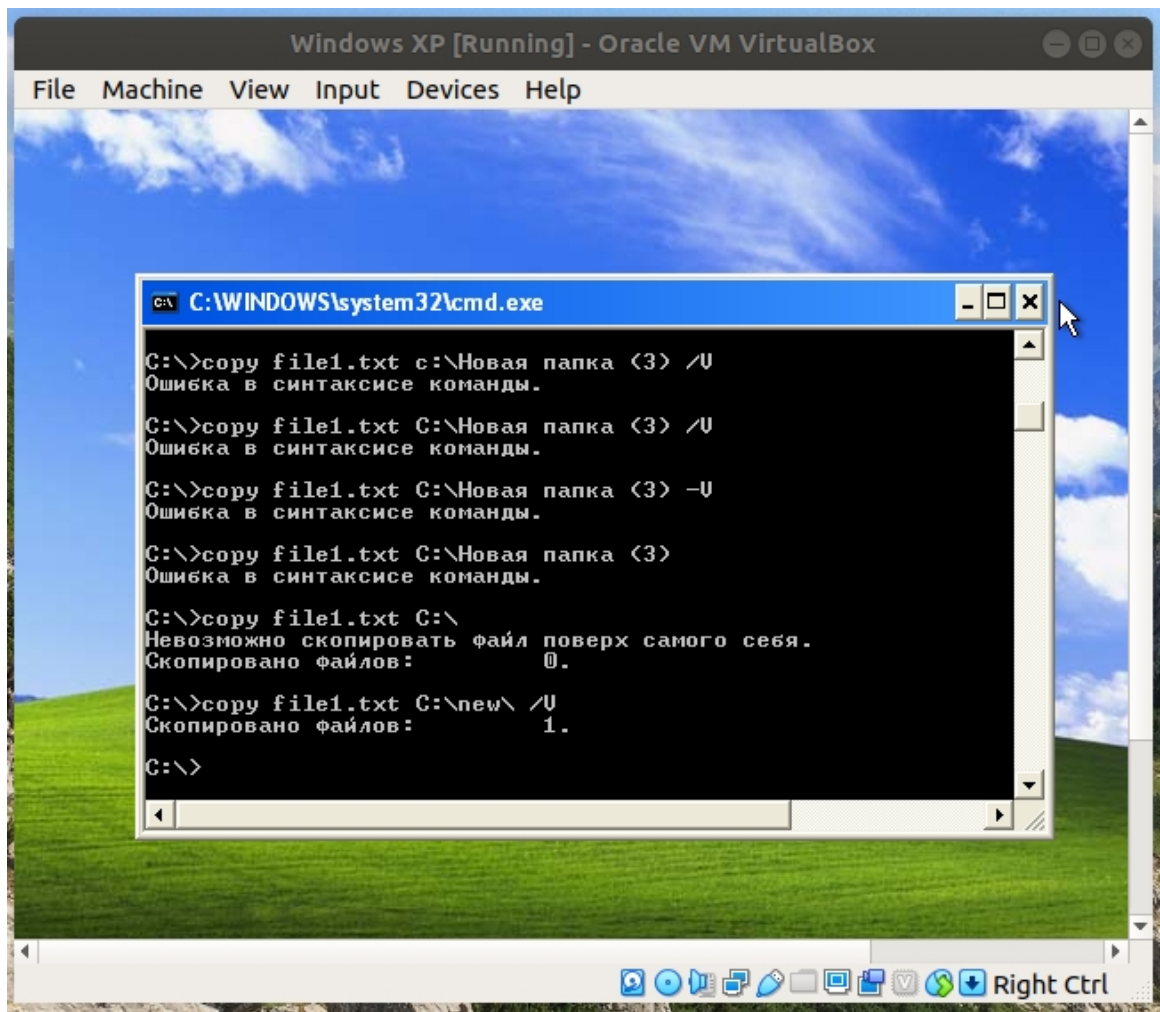


```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.
C:\Documents and Settings\Администратор>copy c:\test.txt c:\textfiles /V
Скопировано файлов:
1.
C:\Documents and Settings\Администратор>
```

Рис. 3.

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

Следует обратить внимание, что если в имени папки есть пробел, в команде его быть не должно, как в указанном примере.



3. Многие команды Windows имеют большое количество дополнительных параметров и ключей, и запомнить их все невозможно или по крайней мере очень 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
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Администратор>copy/?
Копирование одного или нескольких файлов в другое место.

COPY [/D] [/U] [/N] [/Y | /-Y] [/Z] [/A | /B] источник [/A | /B]
[+ источник [/A | /B] [+ ...]] [результат [/A | /B]]

источник      Имена одного или нескольких копируемых файлов.
/A            Файл является текстовым файлом ASCII.
/B            Файл является двоичным файлом.
/D            Указывает на возможность создания зашифрованного файла
результат     Каталог и/или имя для конечных файлов.
/U            Проверка правильности копирования файлов.
/N            Использование, если возможно, коротких имен при копировании
              файлов, чьи имена не удовлетворяют стандарту 8.3.
/Y            Подавление запроса подтверждения на перезапись существующего
              конечного файла.
/-Y           Обязательный запрос подтверждения на перезапись существующего
              конечного файла.
/Z            Копирование сетевых файлов с возобновлением.

Ключ /Y можно установить через переменную среды COPYCMD.
Ключ /-Y командной строки переопределяет такую установку.

```

Рис. 4.

ping /help

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Администратор>ping/help
Неверный параметр /help.

Использование: ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS]
                 [-r число] [-s число] [[-j списокУзлов] ; [-k списокУзлов]]
                 [-w таймаут] конечноеИмя

Параметры:
-t            Отправка пакетов на указанный узел до команды прерывания.
              Для вывода статистики и продолжения нажмите
              <Ctrl>+<Break>, для прекращения - <Ctrl>+<C>.
-a            Определение адресов по именам узлов.
-n число     Число отправляемых запросов.
-l размер     Размер буфера отправки.
-f            Установка флага, запрещающего фрагментацию пакета.
-i TTL       Задание срока жизни пакета (поле "Time To Live").
-v TOS       Задание типа службы (поле "Type Of Service").
-r число     Запись маршрута для указанного числа переходов.
-s число     Штамп времени для указанного числа переходов.
-j списокУзлов Свободный выбор маршрута по списку узлов.
-k списокУзлов Жесткий выбор маршрута по списку узлов.

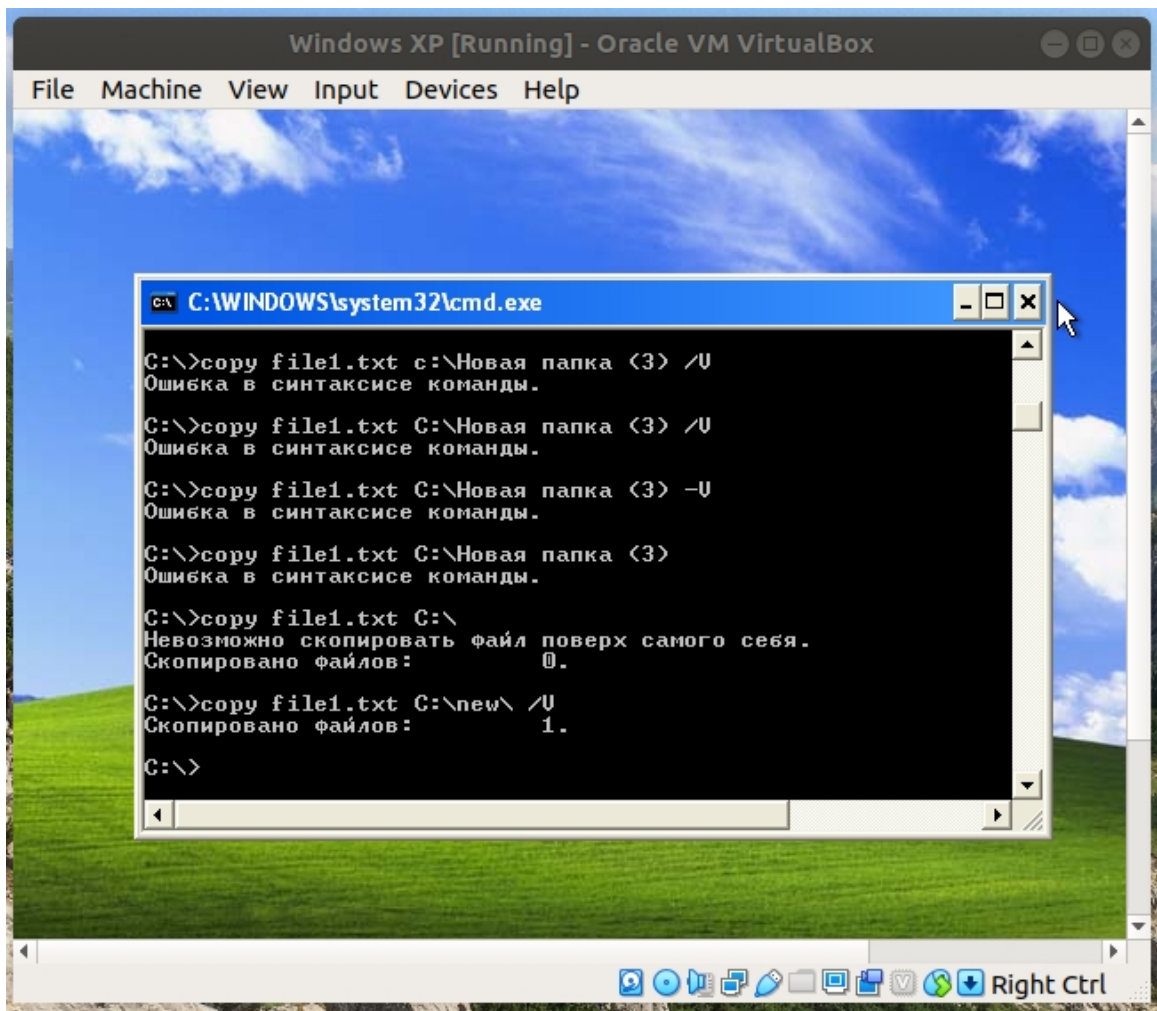
```

Рис. 5.

Команда **help** выводит список основных команд Командной строки

```
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.
EVENTQUERY Displays event log entries for specified criteria.
EXIT       Quits 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.
```

Рис. 6.



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, а в файл, читать входные данные не с клавиатуры, а из заранее подготовленного файла, передавать сообщения, выводимые одной программой, в качестве входных данных для другой программы.

Выходные данные практически всех команд высвечиваются в окне командной строки. Даже команды, выводящие данные на диск или принтер, выдают сообщения и запросы в окне командной строки.

Для перенаправления вывода команд из окна командной строки в файл или на устройство применяется оператор ">". Этот оператор используется с большинством команд. Например, для перенаправления вывода команды `dir` в файл `test.txt` введите в Командной строке:

dir>c:test.txt

Если указанный файл не существует, интерпретатор команд Cmd.exe создаст его. Если файл существует, Cmd.exe заменит информацию в файле на данные, полученные от команды dir.

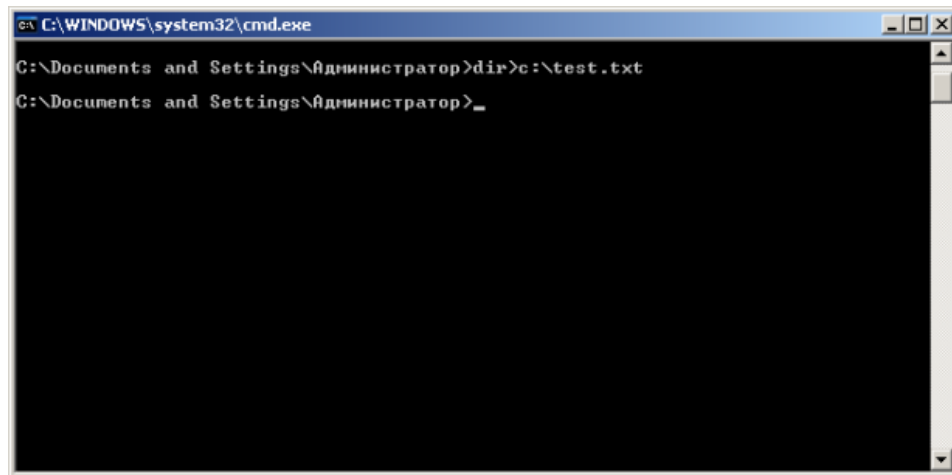


Рис. 7.

Откройте файл test.txt . В нем будет содержаться результат команды dir.

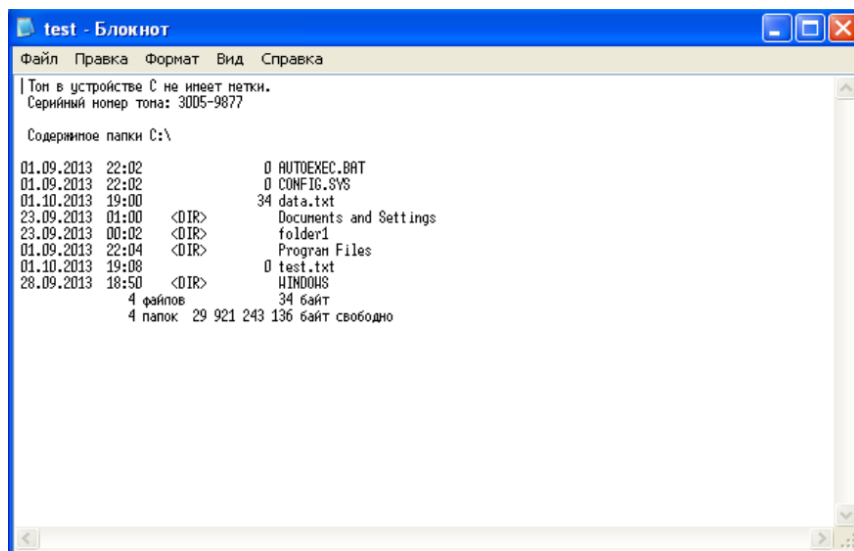


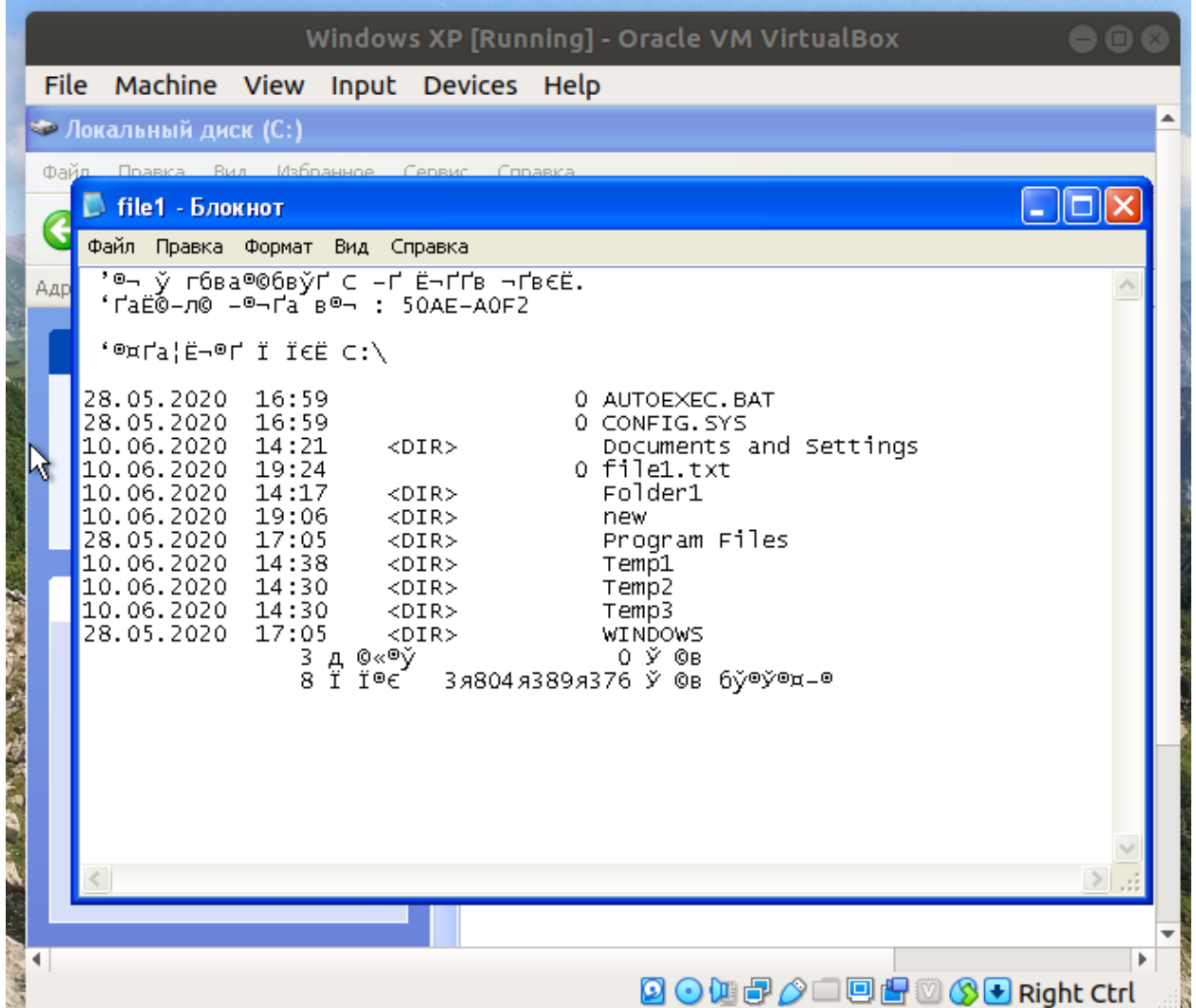
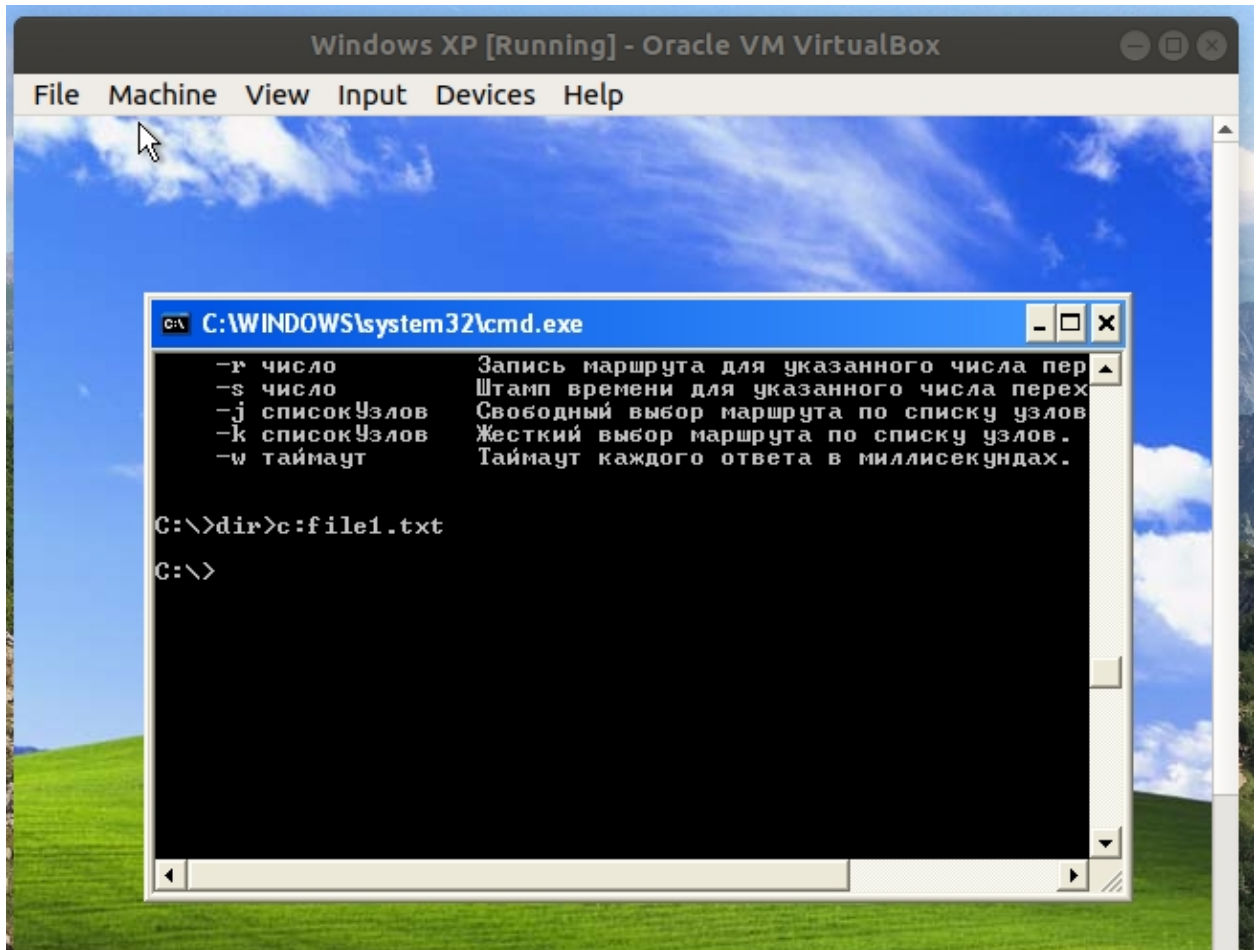
Рис. 8.

Следует отметить, что информация, которая была в файле до этого, будет стерта. Для того чтобы выходные файлы команды добавлялись в конец файла, необходимо использовать символ >>, а не > в синтаксисе команды.

Местоположение потоков ввода и вывода называется дескриптор.

В [таблице 1](#) описаны операторы перенаправления потоков ввода и вывода команд.

Таблица 1.	
Оператор перенаправления	Описание
>	Записывает данные на выходе команды вместо командной строки в файл или на устройство, например, на принтер.
<	Читает поток входных данных команды из файла, а не с клавиатуры.
>>	Добавляет выходные данные команды в конец файла, не удаляя при этом существующей информации из файла.
>&	Считывает данные на выходе одного дескриптора как входные данные для другого дескриптора.
<&	Считывает входные данные одного дескриптора как выходные данные другого дескриптора.
	Считывает выходные данные одной команды и записывает их на вход другой команды. Эта процедура известна под названием "канал".



5. С помощью символа < можно прочитать входные данные для заданной команды не с клавиатуры, а из определенного (заранее подготовленного) файла. На диске С создайте файл data.txt и напишите в нем 01.10.2013. В Командной строке наберите

Date < c:\data.txt

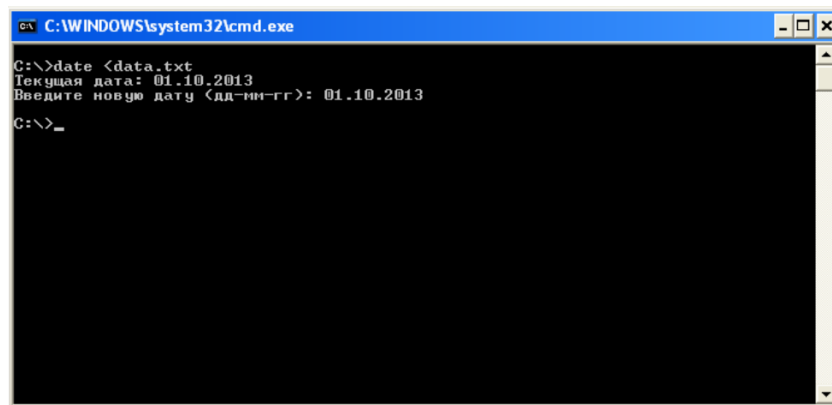
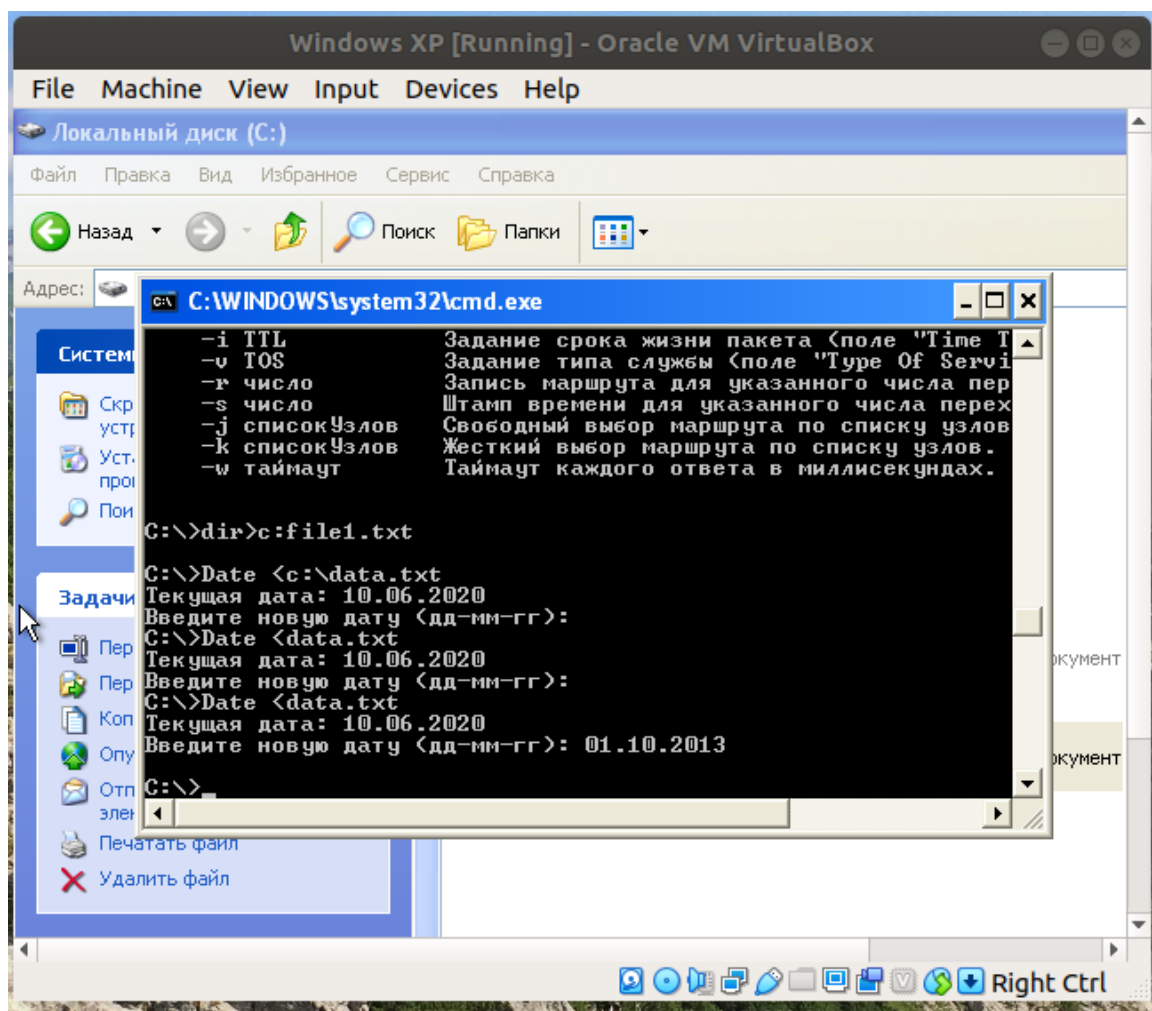


Рис. 9.

Проверьте дату на вашем компьютере – она изменилась на 01.10.2013



6. Команда **more** выводит содержимое файла или выхода команды в одном окне командной строки за раз. Например, чтобы отобразить содержимое файла test.txt в одном окне командной строки за раз, введите следующую команду:

more c:\ test.txt

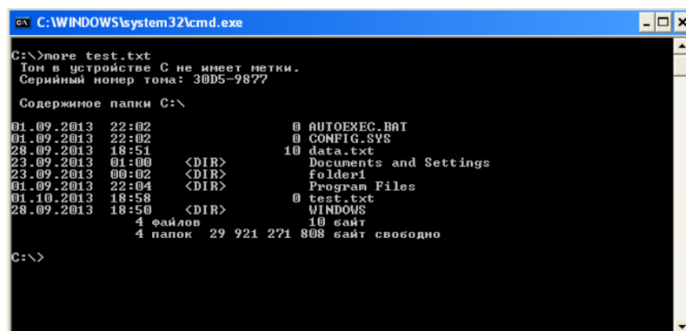
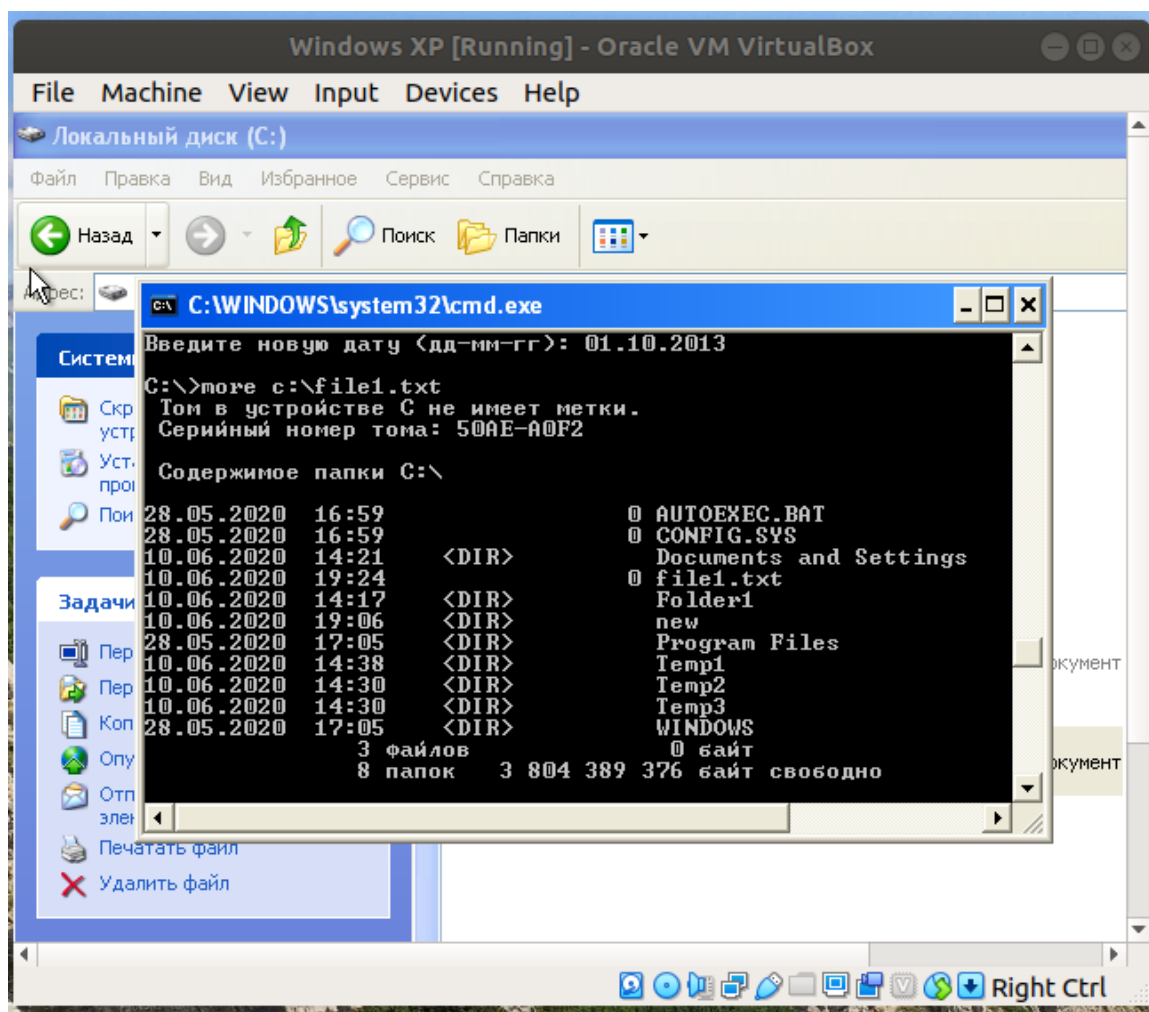


Рис. 10.

Если файл большой, то отображается одно окно командной строки со сведениями, а затем в нижней части окна командной строки отображается строка **-- More --**. Для остановки просмотра следует ввести комбинацию **CTRL+C**.

Команда **more** полезна при работе с командами, создающими выход более одного окна командной строки. Например, при выводе дерева каталогов жесткого диска.



7. Другой распространенной командой фильтрации является **sort** - она выполняет сортировку по алфавиту текстового файла или выхода команды.

Отредактируйте файл `data.txt`, добавив туда две другие даты, например, 20.10.2013 и 07.10.2013. В командной строке наберите:

```
sort < C:\data.txt
```

```
C:\WINDOWS\system32\cmd.exe
C:\>sort c:\data.txt
01.10.2013
07.10.2013
20.10.2013
C:\>
```

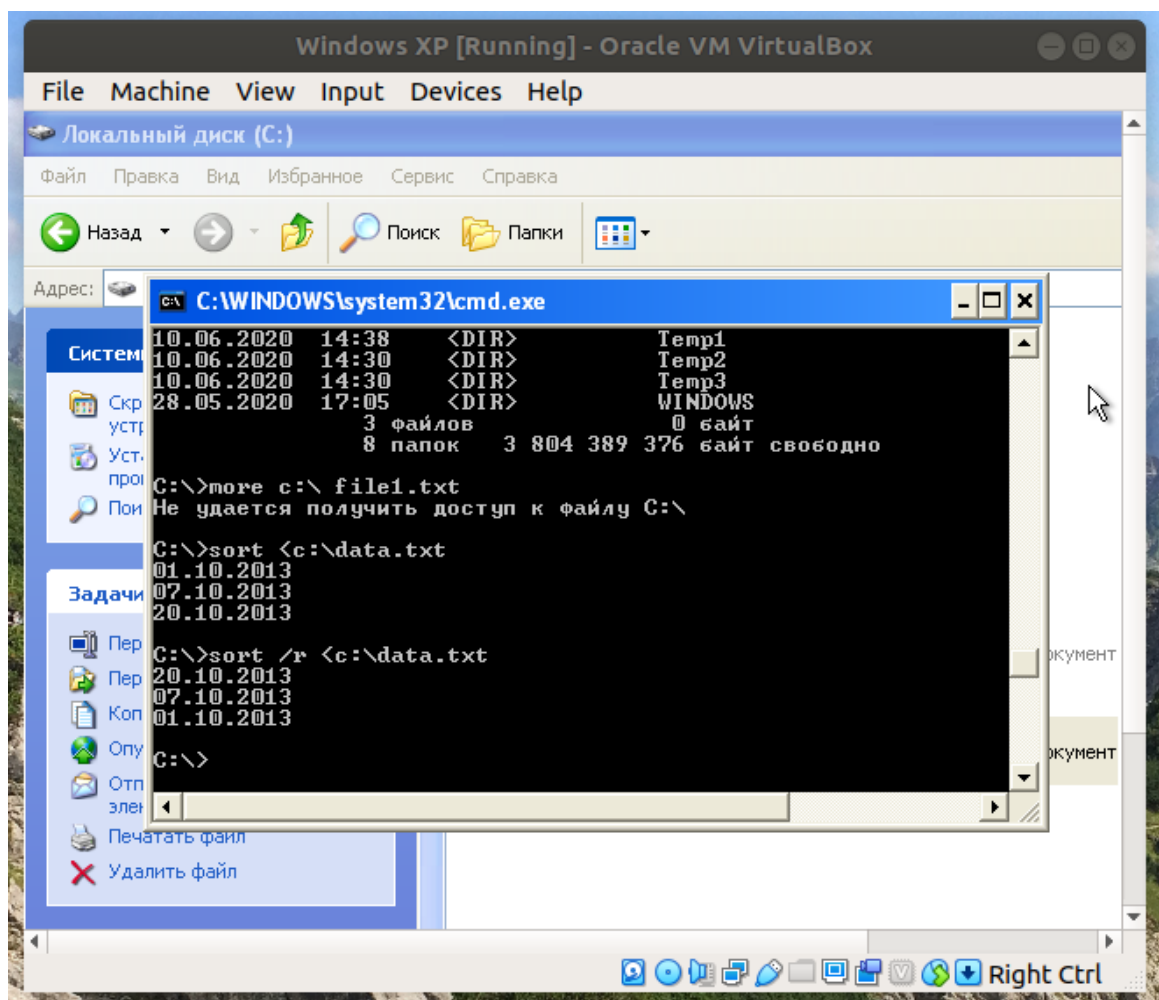
Рис. 11.

`sort /r < C:\data.txt`

```
C:\WINDOWS\system32\cmd.exe
C:\>sort c:\data.txt
01.10.2013
07.10.2013
20.10.2013
C:\>sort /r c:\data.txt
20.10.2013
07.10.2013
01.10.2013
C:\>
```

Рис. 12.

Ключ `/R` позволяет изменить порядок сортировки на обратный.



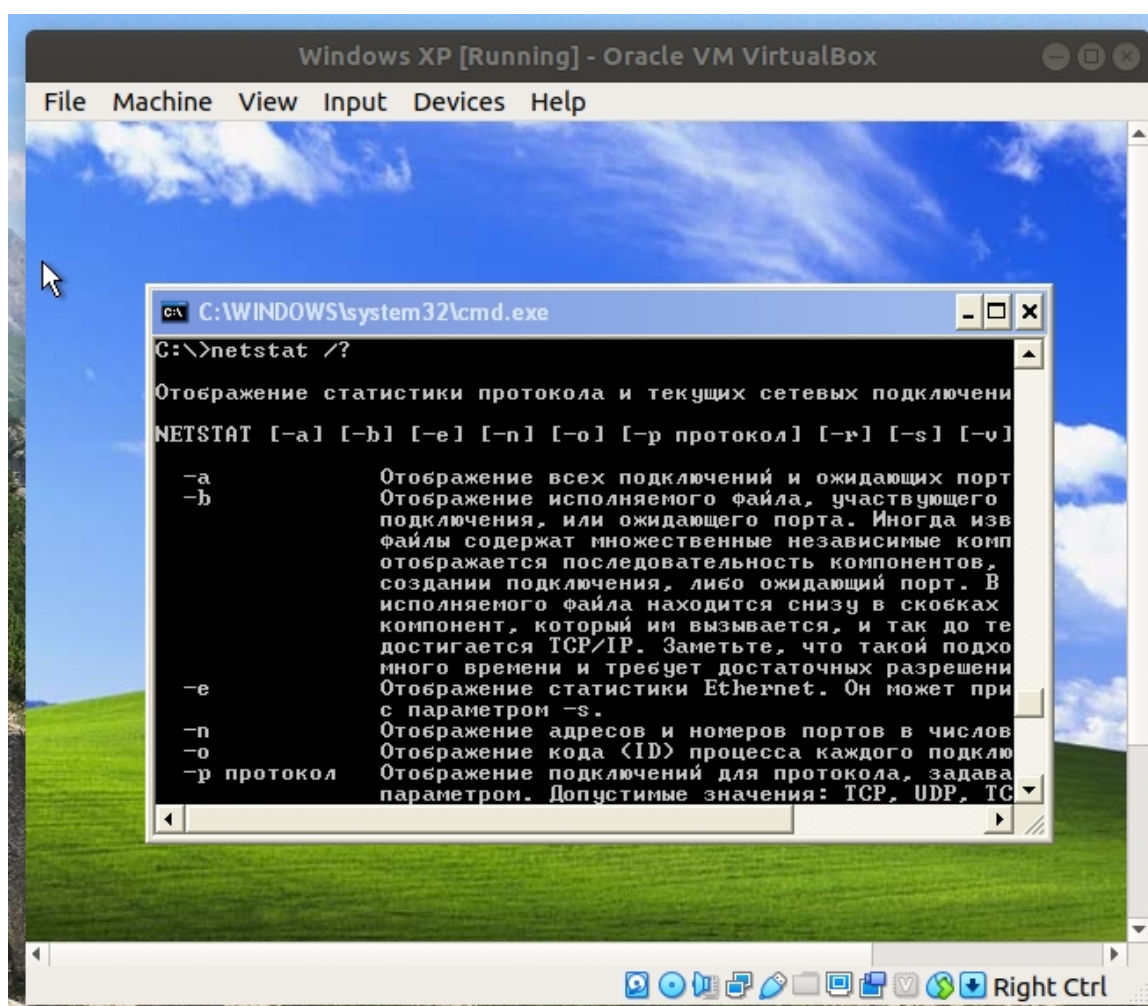
Задание 2. Сетевая активность

Одним из проявлений наличия вредоносной программы может быть возросшая сетевая активность. Вредоносная программа может отправлять письма, скачивать информацию из Интернета, передавать кому-то по сети конфиденциальную информацию и многое другое. При этом необходимо помнить, что легальные приложения также могут использовать Интернет без действий пользователя – например, антивирусная программа может скачивать обновления антивирусной базы данных.

Для получения полной информации о сетевой активности можно использовать команду **netstat**, которая выводит на экран мгновенную статистику сетевых соединений.

1. В Командной строке наберите:

netstat /?



2. Прочитайте описание утилиты netstat. Убедитесь, что для вывода самой полной информации нужно использовать ключ **-a**

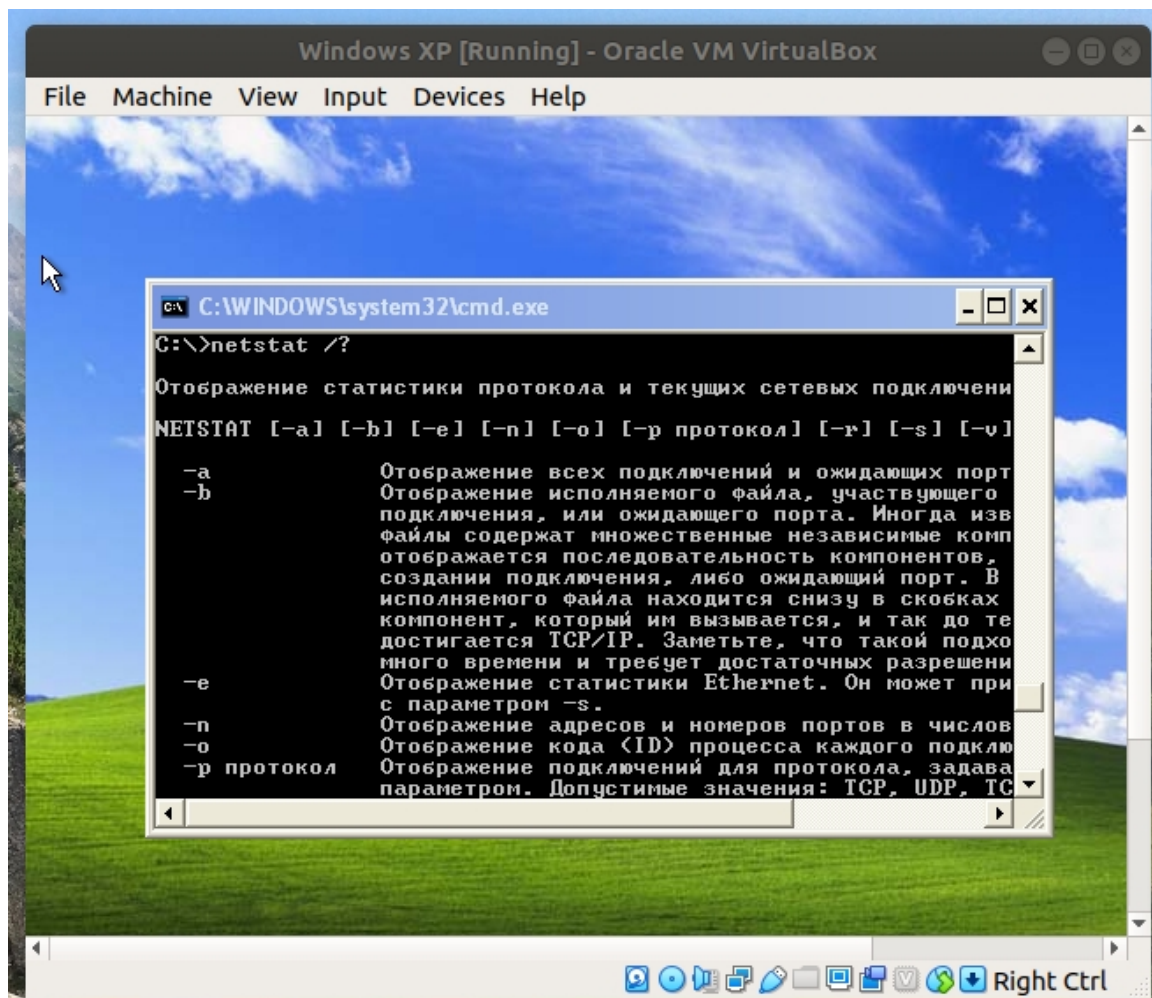
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Администратор>netstat/?

Отображение статистики протокола и текущих сетевых подключений TCP/IP.

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

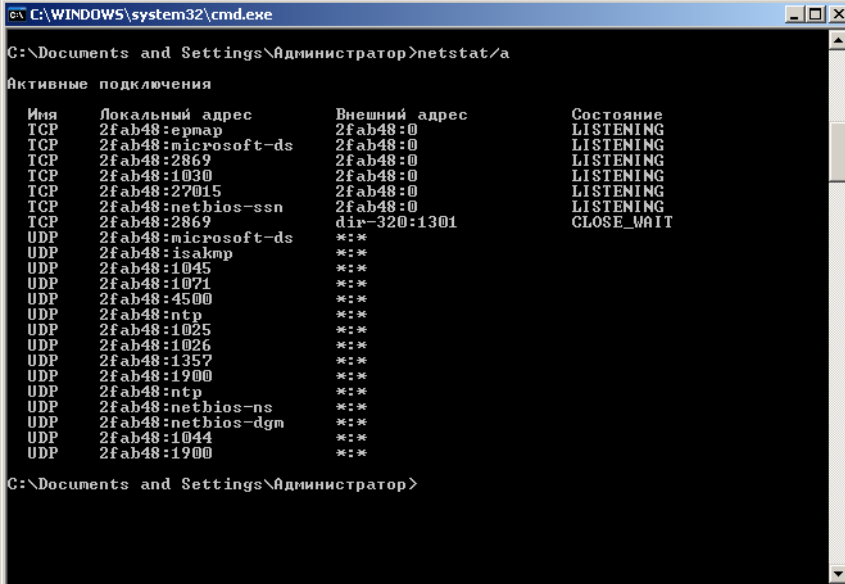
-a      Отображение всех подключений и ожидающих портов.
-b      Отображение исполняемого файла, участвующего в создании каждого
        подключения, или ожидающего порта. Иногда известные исполняемые
        файлы содержат множественные независимые компоненты. Тогда
        отображается последовательность 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.
        Используется вместе с параметром -s для отображения статистики
        по протоколам. Допустимые значения: IP, IPv6, ICMP, ICMPv6,
        TCP, TCPv6, UDP или UDPv6
-r      Отображение содержимого таблицы маршрутов.
-s      Отображение статистических данных по протоколам. По умолчанию
        данные отображаются для IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP
        и UDPv6. Параметр -p позволяет указать подмножество выводимыхся
        данных.
-v      При использовании с параметром -b, отображает последовательность
        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
```

Рис. 13.



3. В Командной строке наберите:

netstat /a



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Администратор>netstat/a

Активные подключения
Имя      Локальный адрес      Внешний адрес      Состояние
TCP      2fab48:epmap          2fab48:0           LISTENING
TCP      2fab48:microsoft-ds   2fab48:0           LISTENING
TCP      2fab48:2869           2fab48:0           LISTENING
TCP      2fab48:1030           2fab48:0           LISTENING
TCP      2fab48:27015          2fab48:0           LISTENING
TCP      2fab48:netbios-ssn    2fab48:0           LISTENING
TCP      2fab48:2869           dir-320:1301       CLOSE_WAIT
UDP      2fab48:microsoft-ds   ***
UDP      2fab48:isakmp         ***
UDP      2fab48:1045           ***
UDP      2fab48:1071           ***
UDP      2fab48:4500           ***
UDP      2fab48:ntp            ***
UDP      2fab48:1025           ***
UDP      2fab48:1026           ***
UDP      2fab48:1357           ***
UDP      2fab48:1700           ***
UDP      2fab48:ntp            ***
UDP      2fab48:netbios-ns     ***
UDP      2fab48:netbios-dgm    ***
UDP      2fab48:1044           ***
UDP      2fab48:1700           ***

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

Рис. 14.

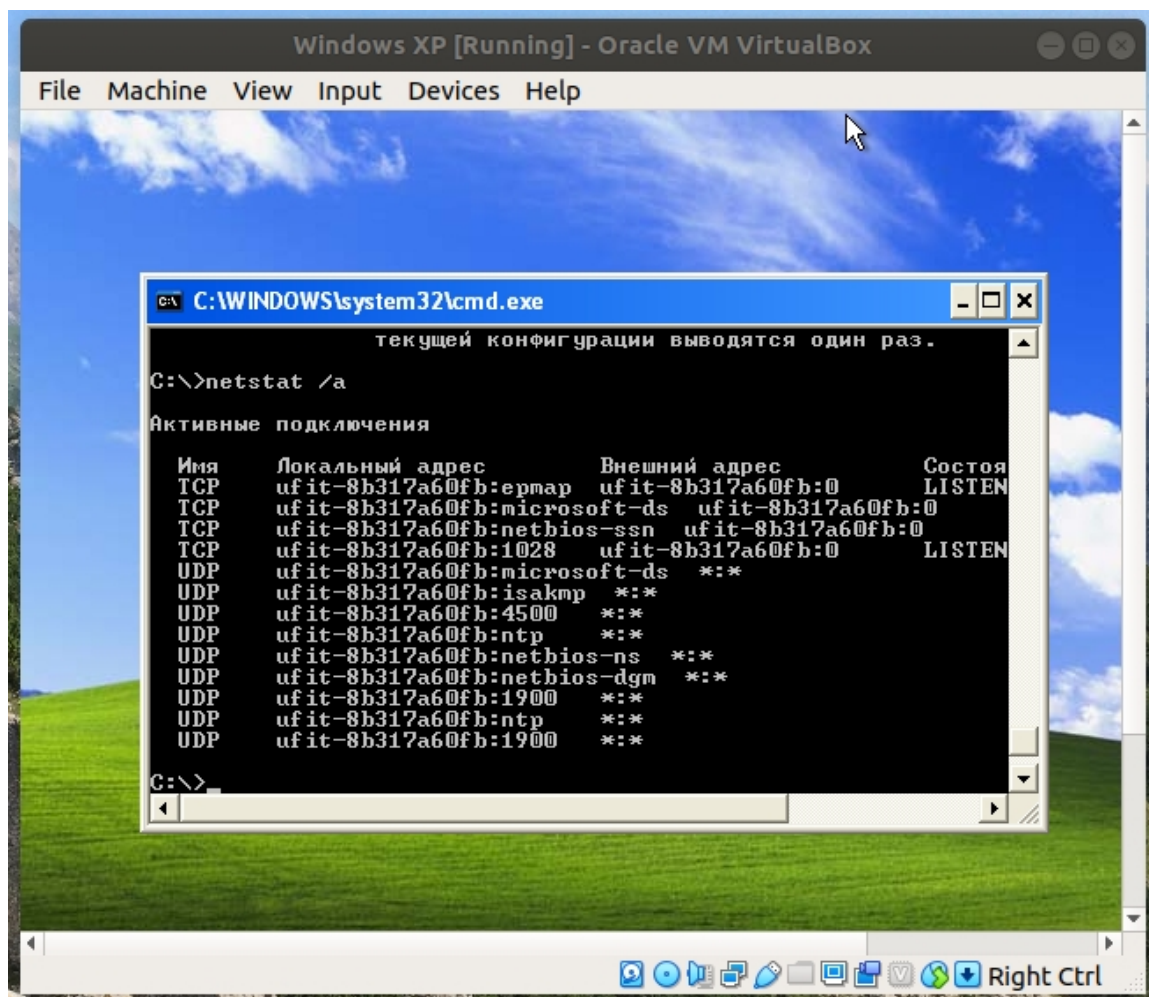
Результатом выполнения команды является список активных подключений, в который входят установленные соединения и открытые порты.

TCP(Transmission Control Protocol)-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 - epmap, microsoft-ds, netbios-ssn. Порты, не относящиеся к стандартным службам, отображаются по номерам.

UDP(User Datagram Protocol)-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.

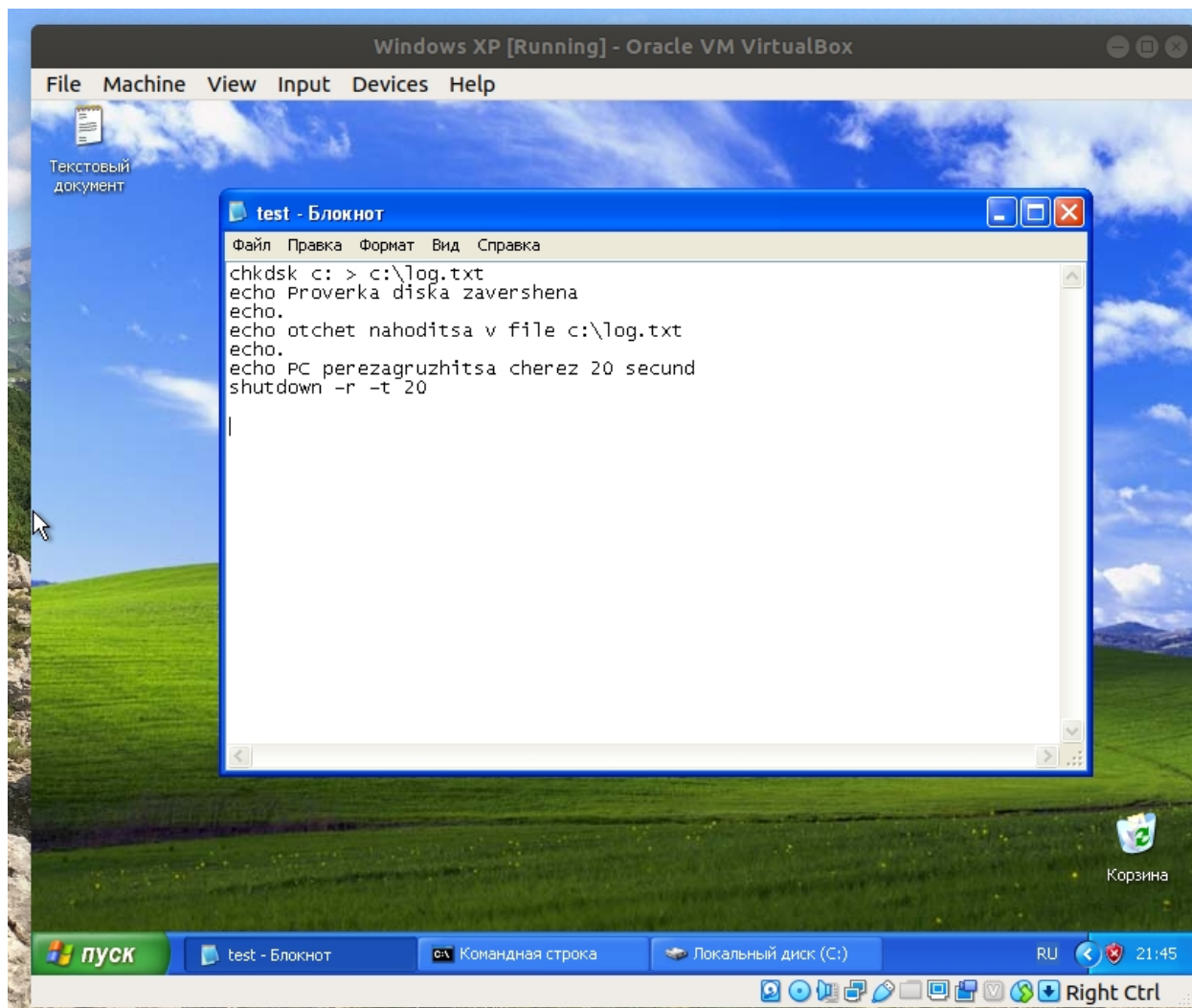
Порты, используемые вредоносными программами, чаще всего являются нестандартными и поэтому отображаются согласно их номерам. Впрочем, могут встречаться троянские программы, использующие для маскировки стандартные для других приложений порты, например 80, 21, 443 - порты, используемые на файловых и веб-серверах.

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.

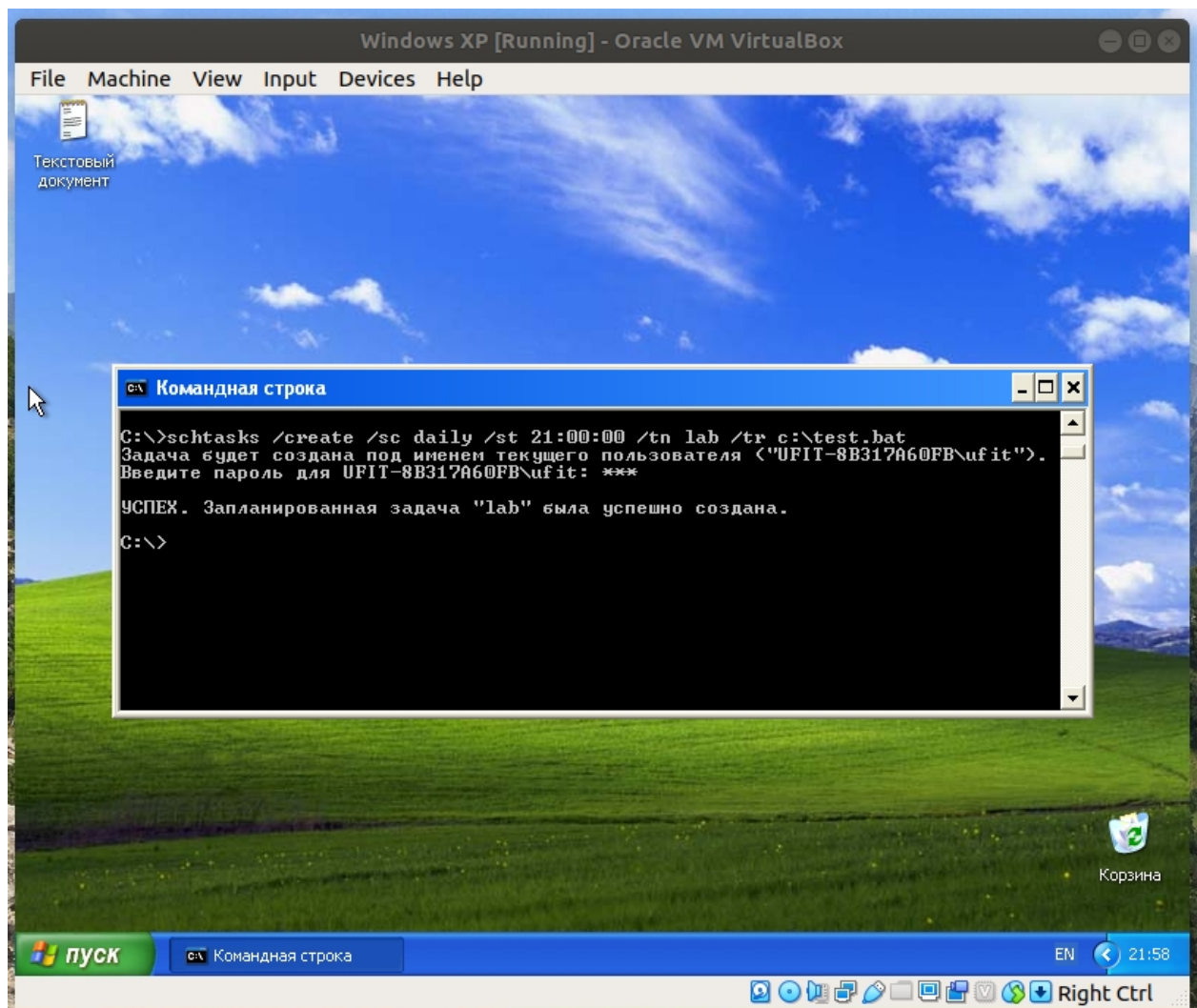


Задание 4	
Вар. №	Описание пакетного файла
7	<p>Пакетный файл, предназначенный для углубленной проверки жесткого диска с созданием файла отчета, путь к которому задается в качестве пакетного параметра. Проверка жесткого диска осуществляется ежедневно в 21:00. В течение 20 секунд по окончании проверки диска выводится сообщение «Проверка диска завершена. Файл-отчет находится в каталоге <путь >» и далее осуществляется автоматическая перезагрузка системы.</p>

Ниже представлен код пакетного файла.



Для ежедневной работы файла необходимо добавить его в планировщик событий. Например, следующей командой.



В результате будет создан файл с результатом проверки диска, а на экране появится следующее сообщение

