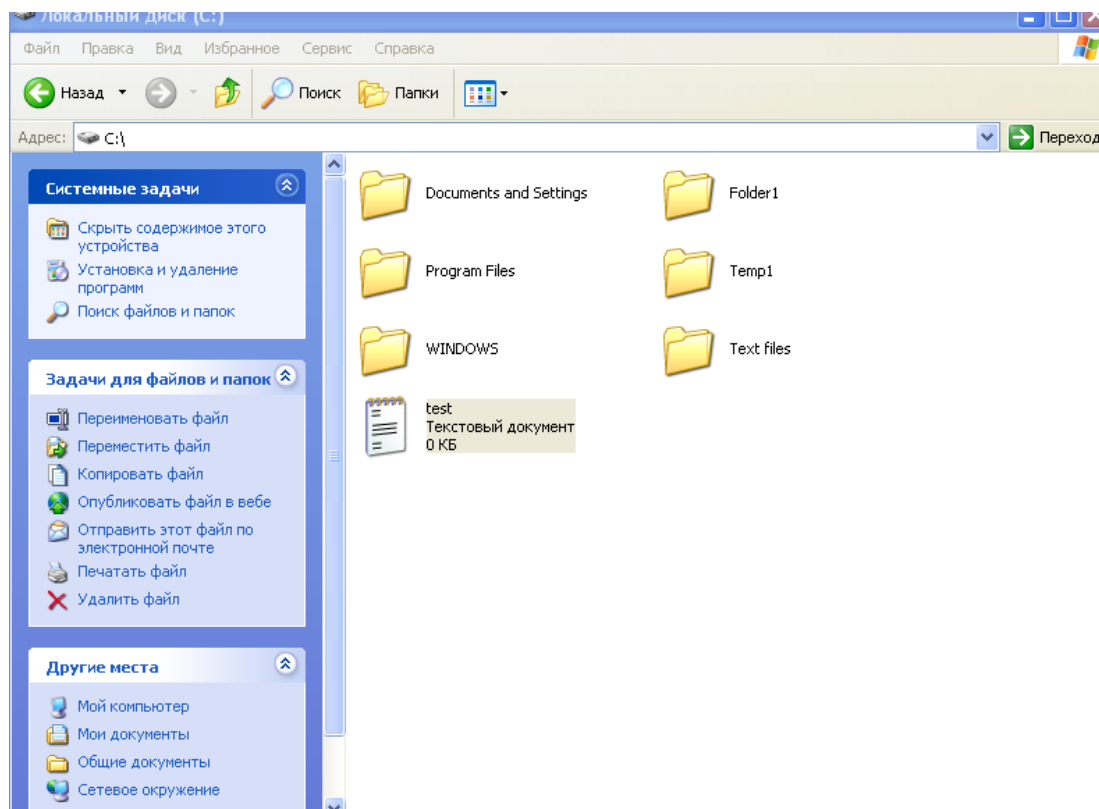
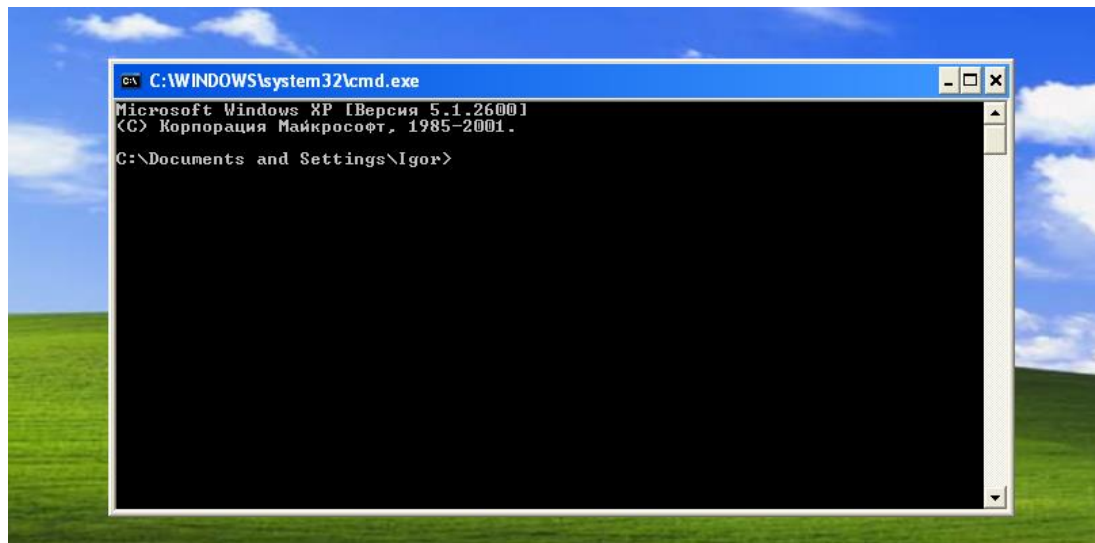


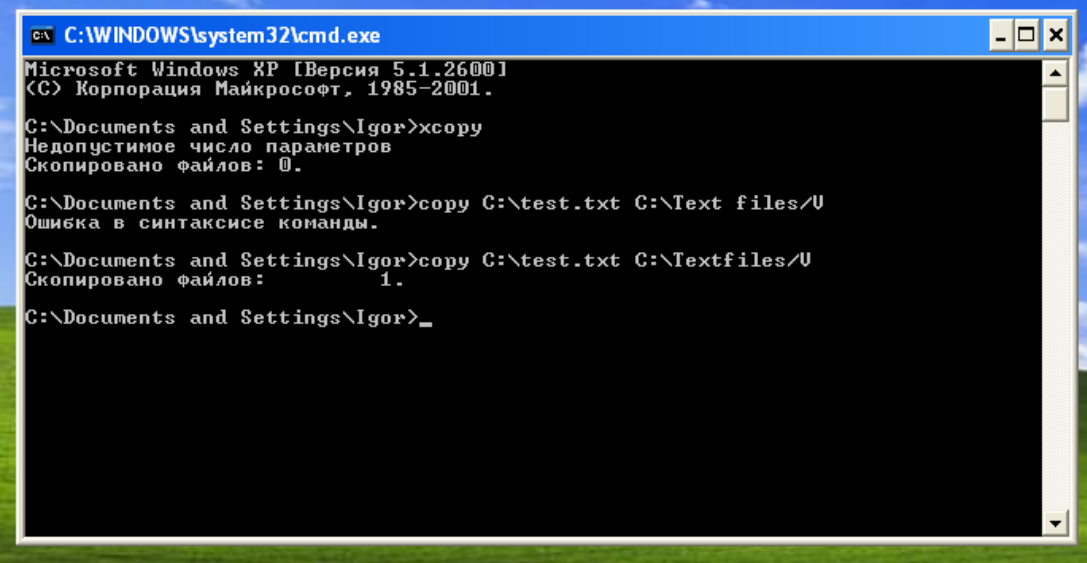
Лабораторная работа №3

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





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

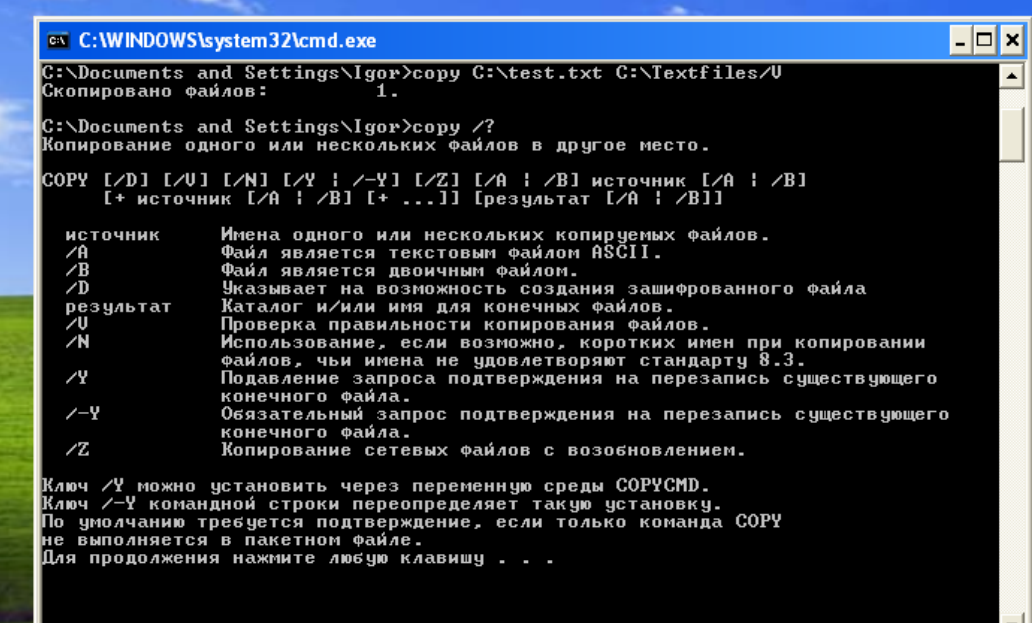
C:\Documents and Settings\Igor>xcopy
Недопустимое число параметров
Скопировано файлов: 0.

C:\Documents and Settings\Igor>copy C:\test.txt C:\Text files/U
Ошибка в синтаксисе команды.

C:\Documents and Settings\Igor>copy C:\test.txt C:\Textfiles/U
Скопировано файлов: 1.

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

copy /?



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Igor>copy C:\test.txt C:\Textfiles/U
Скопировано файлов: 1.

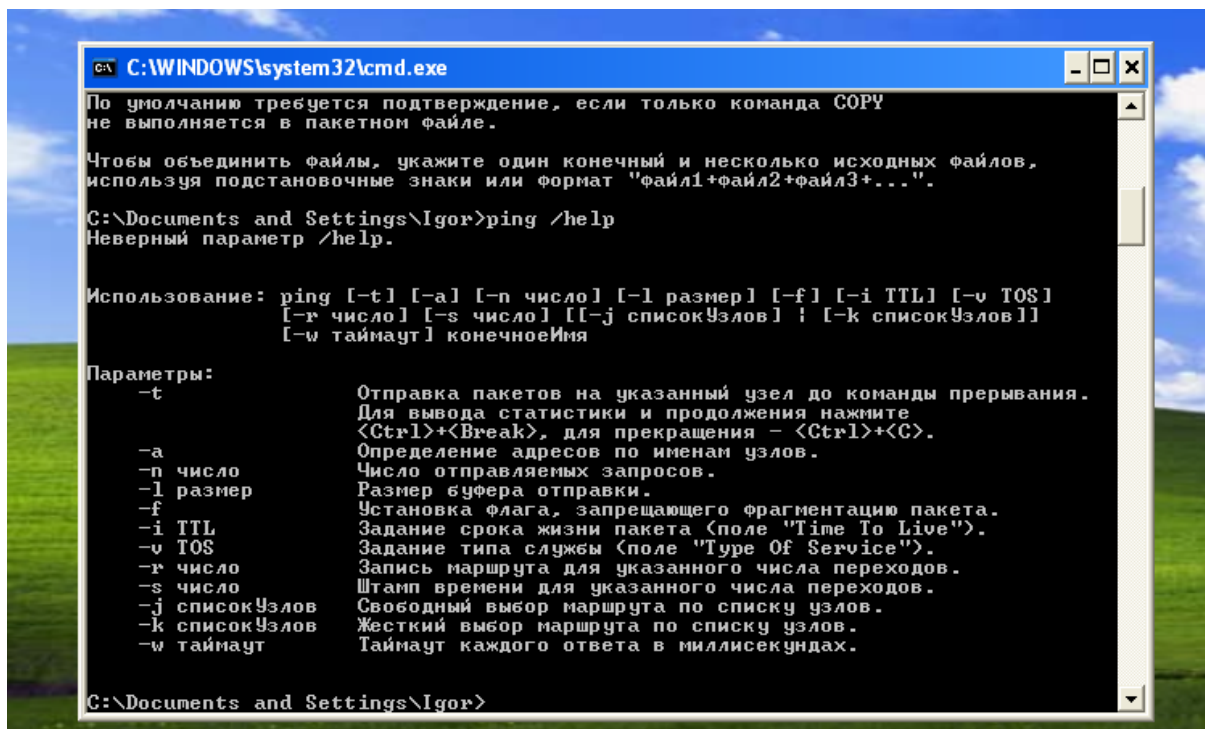
C:\Documents and Settings\Igor>copy /?
Копирование одного или нескольких файлов в другое место.

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.
По умолчанию требуется подтверждение, если только команда COPY
не выполняется в пакетном файле.
Для продолжения нажмите любую клавишу . . .
```

ping /help



```
C:\WINDOWS\system32\cmd.exe

По умолчанию требуется подтверждение, если только команда COPY
не выполняется в пакетном файле.

Чтобы объединить файлы, укажите один конечный и несколько исходных файлов,
используя подстановочные знаки или формат "файл1+файл2+файл3+...".

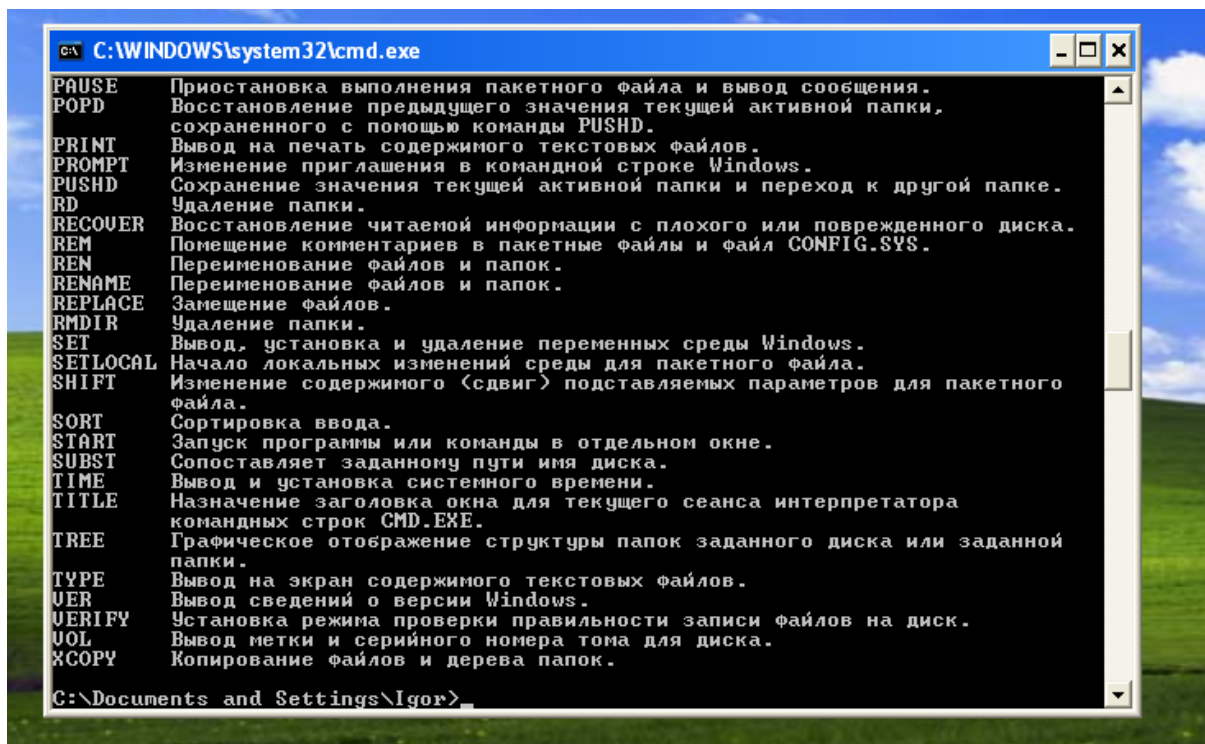
C:\Documents and Settings\Igor>ping /help
Неверный параметр /help.

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.
  -w таймаут       Таймаут каждого ответа в миллисекундах.

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

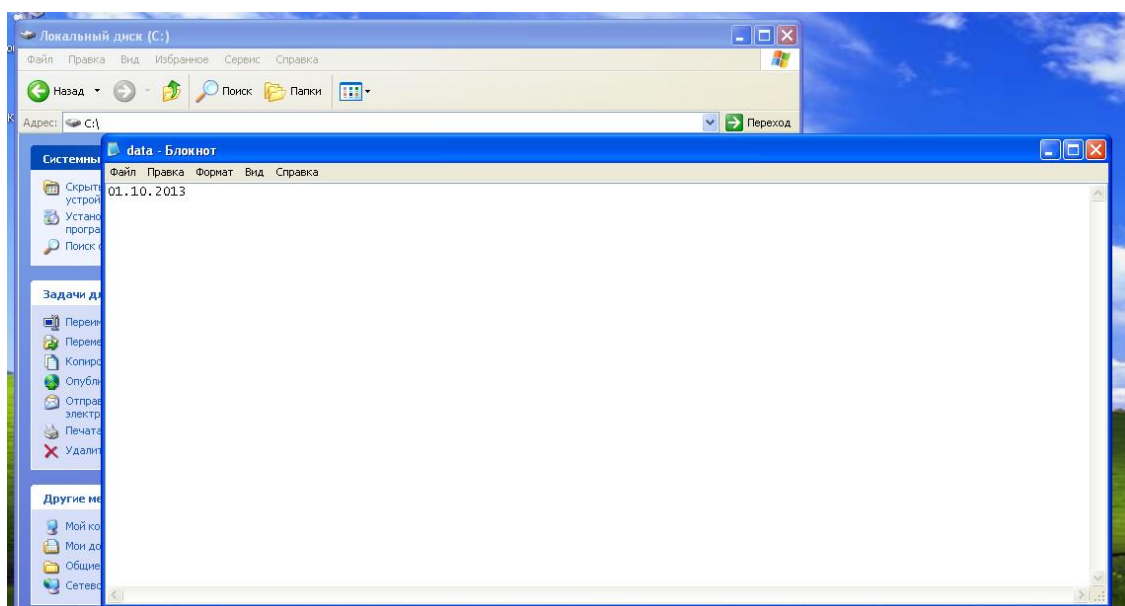
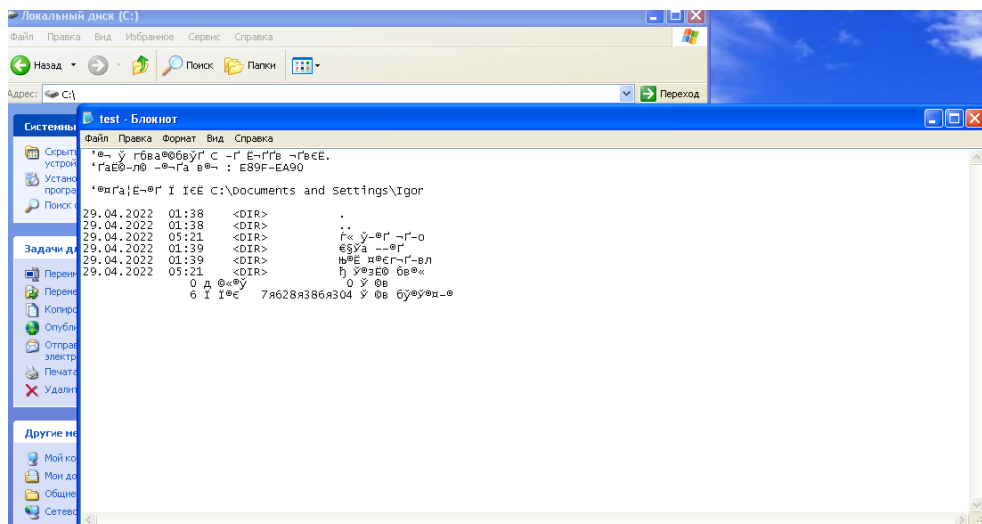
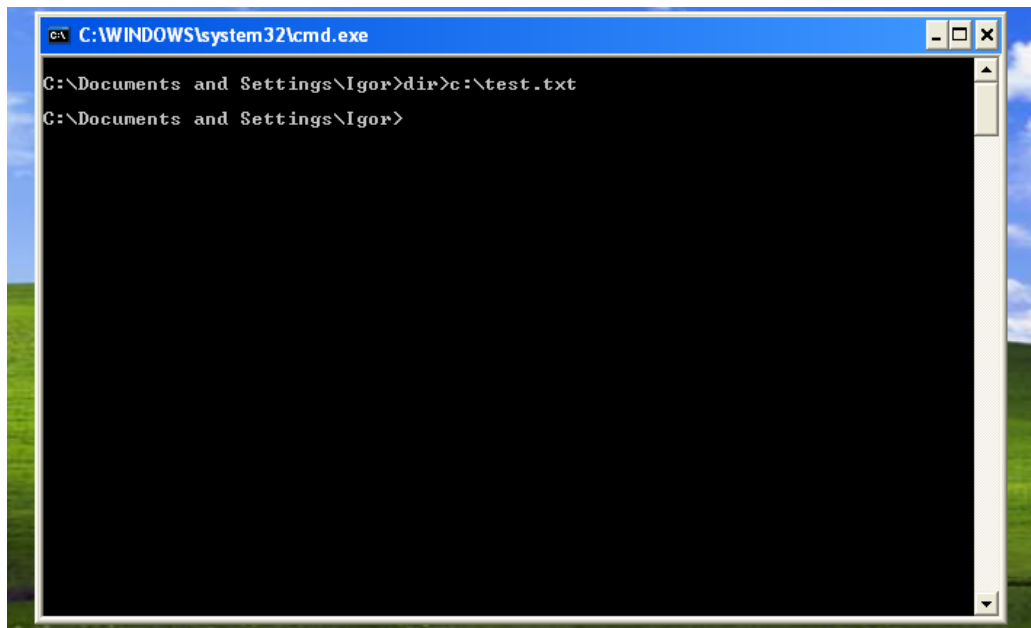
help

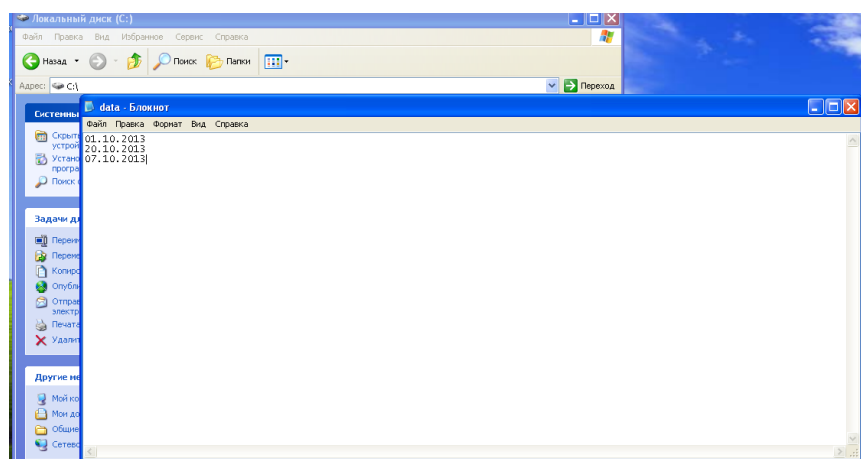
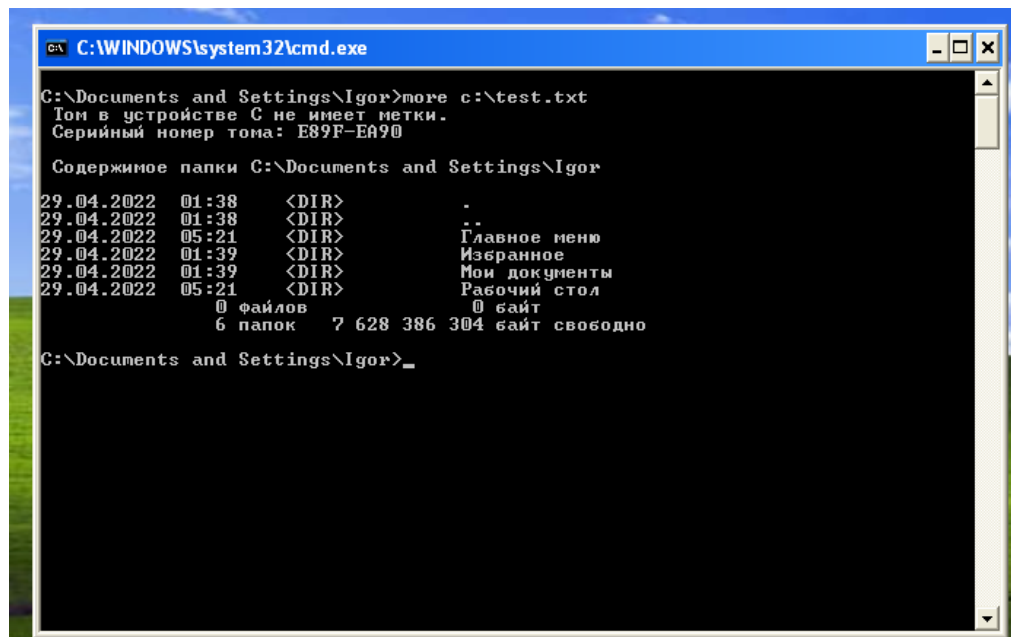
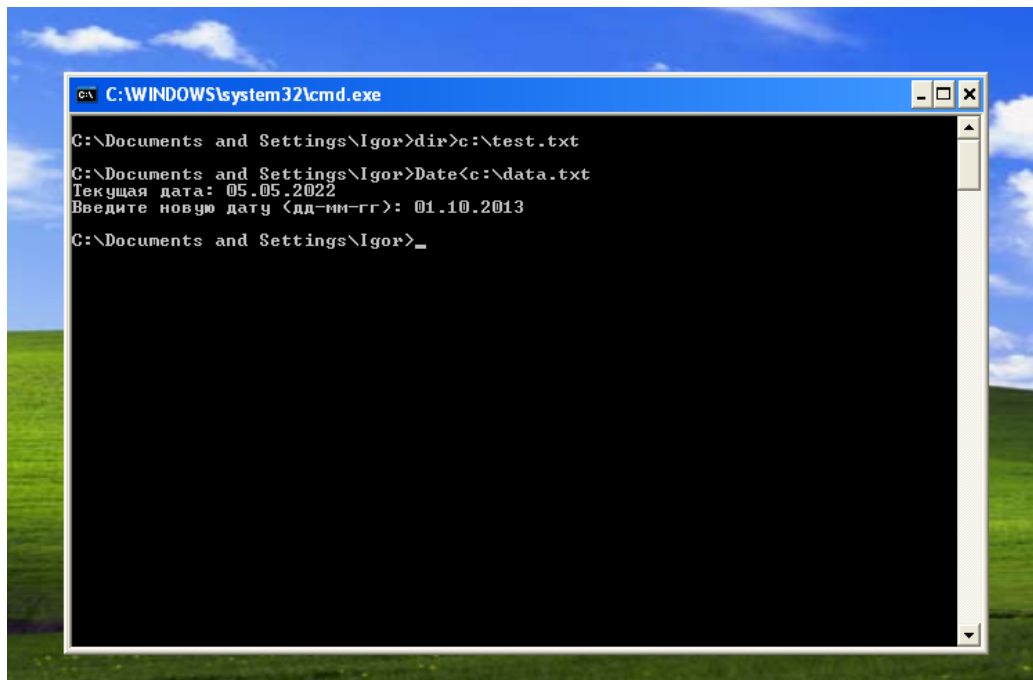


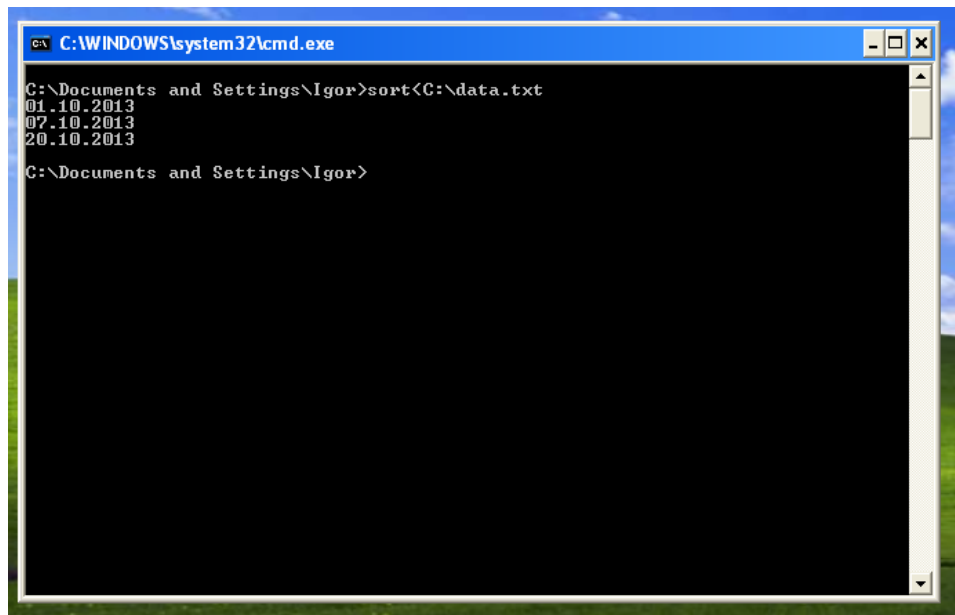
```
C:\WINDOWS\system32\cmd.exe

PAUSE    Приостановка выполнения пакетного файла и вывод сообщения.
POPD     Восстановление предыдущего значения текущей активной папки,
сохраненного с помощью команды PUSH.D.
PRINT    Вывод на печать содержимого текстовых файлов.
PROMPT   Изменение приглашения в командной строке Windows.
PUSHD    Сохранение значения текущей активной папки и переход к другой папке.
RD       Удаление папки.
RECOVER  Восстановление читаемой информации с плохого или поврежденного диска.
REM      Помещение комментариев в пакетные файлы и файл CONFIG.SYS.
REN      Переименование файлов и папок.
RENAME   Переименование файлов и папок.
REPLACE  Замещение файлов.
RMDIR    Удаление папки.
SET      Вывод, установка и удаление переменных среды Windows.
SETLOCAL Начало локальных изменений среды для пакетного файла.
SHIFT    Изменение содержимого (сдвиг) подставляемых параметров для пакетного
файла.
SORT     Сортировка ввода.
START    Запуск программы или команды в отдельном окне.
SUBST    Сопоставляет заданному пути имя диска.
TIME     Вывод и установка системного времени.
TITLE    Назначение заголовка окна для текущего сеанса интерпретатора
командных строк CMD.EXE.
TREE     Графическое отображение структуры папок заданного диска или заданной
папки.
TYPE     Вывод на экран содержимого текстовых файлов.
VER      Вывод сведений о версии Windows.
VERIFY   Установка режима проверки правильности записи файлов на диск.
VOL      Вывод метки и серийного номера тома для диска.
XCOPY    Копирование файлов и дерева папок.

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



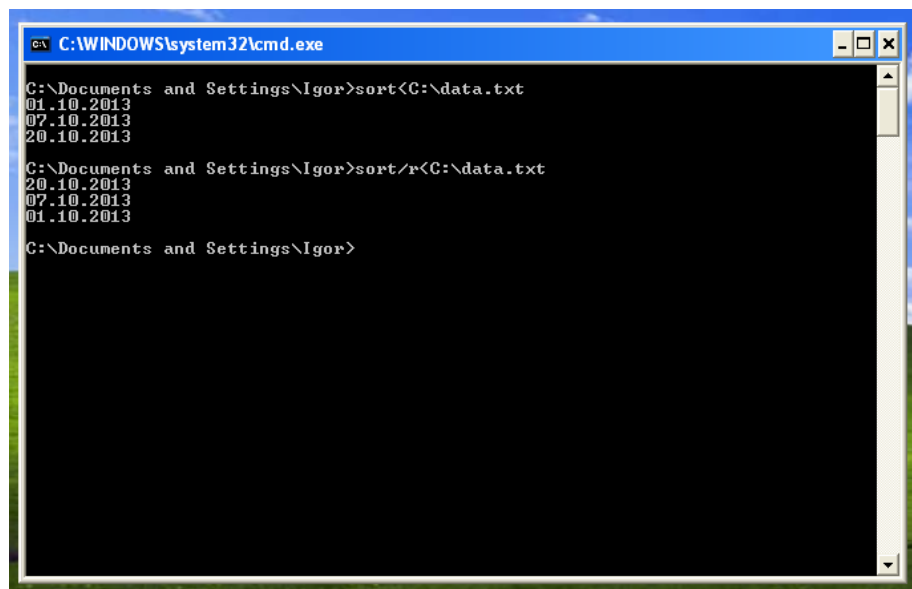




```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Igor>sort<C:\data.txt
01.10.2013
07.10.2013
20.10.2013

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



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Igor>sort<C:\data.txt
01.10.2013
07.10.2013
20.10.2013

C:\Documents and Settings\Igor>sort/r<C:\data.txt
20.10.2013
07.10.2013
01.10.2013

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

Задание 2

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Igor>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 выводимых
            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
            нажмите клавиши CTRL+C. Если параметр не задан, сведения о
            текущей конфигурации выводятся один раз.

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

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Igor>netstat/a

Активные подключения

Имя      Локальный адрес      Внешний адрес      Состояние
TCP      user:epmap            user:0              LISTENING
TCP      user:microsoft-ds     user:0              LISTENING
TCP      user:netbios-ssn      user:0              LISTENING
TCP      user:1025              user:0              LISTENING
UDP      user:microsoft-ds     *:                  LISTENING
UDP      user:isakmp            *:                  LISTENING
UDP      user:4500              *:                  LISTENING
UDP      user:ntp               *:                  LISTENING
UDP      user:netbios-ns        *:                  LISTENING
UDP      user:netbios-dgm       *:                  LISTENING
UDP      user:1900              *:                  LISTENING
UDP      user:ntp               *:                  LISTENING
UDP      user:1900              *:                  LISTENING

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

Задание 4 (Вариант 7)

