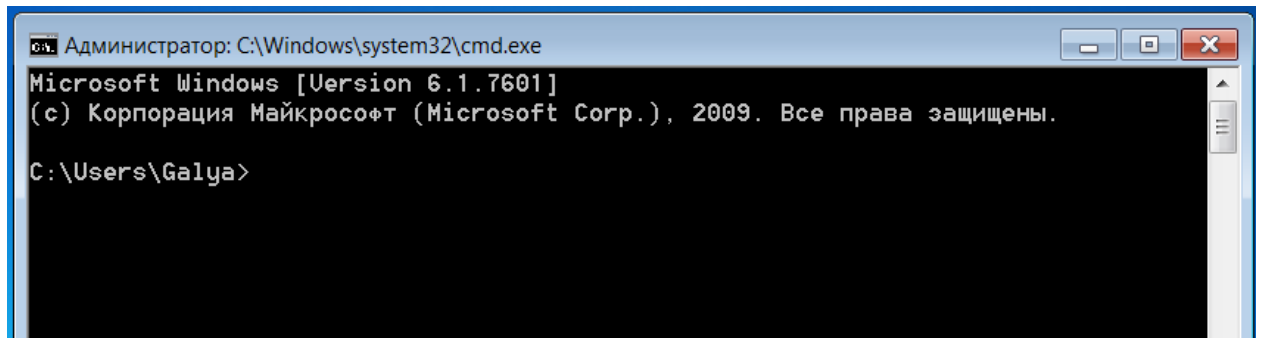


## Работа с командной строкой. Сетевая активность. Пакетные файлы.

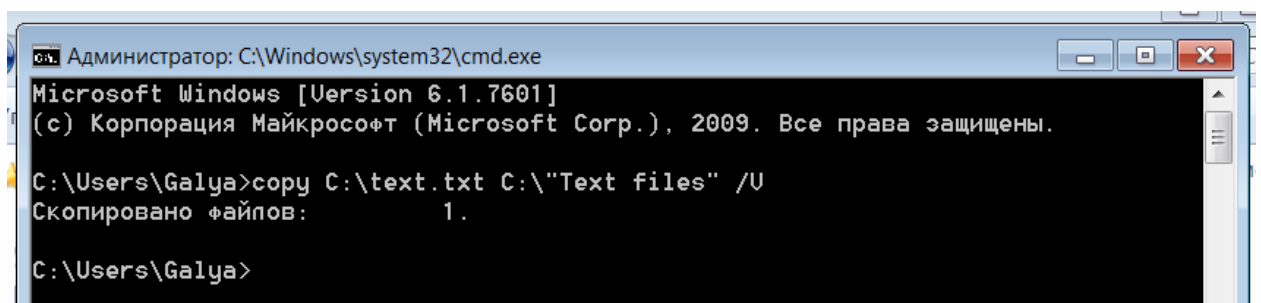
*Цель работы:* получение практических навыков по работе с Командной строкой и по выявлению вредоносных программ на компьютере с Microsoft Windows XP с помощью Командной строки.

### Задание 1. Работа с Командной строкой



```
Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

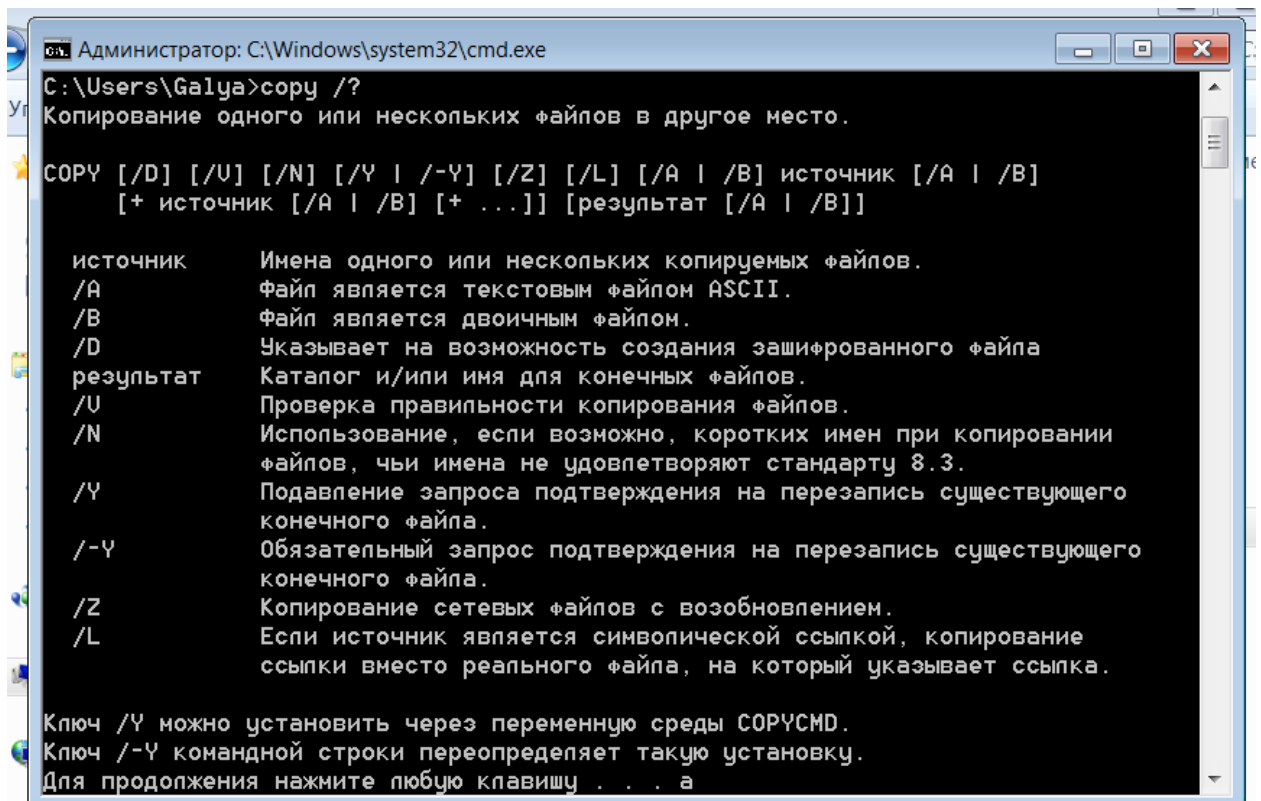
C:\Users\Galya>
```



```
Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\Galya>copy C:\text.txt C:\"Text files" /U
Скопировано файлов:      1.

C:\Users\Galya>
```



```
Администратор: C:\Windows\system32\cmd.exe
C:\Users\Galya>copy /?
Копирование одного или нескольких файлов в другое место.

COPY [/D] [/U] [/N] [/Y | /-Y] [/Z] [/L] [/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.
/L            Если источник является символической ссылкой, копирование
ссылки вместо реального файла, на который указывает ссылка.

Ключ /Y можно установить через переменную среды COPYCMD.
Ключ /-Y командной строки переопределяет такую установку.
Для продолжения нажмите любую клавишу . . . а
```

```
Администратор: C:\Windows\system32\cmd.exe

C:\Users\Galya>ping/help
Неверный параметр /help.

Использование:
ping [-t] [-a] [-n <число>] [-l <размер>] [-f] [-i <TTL>] [-v <TOS>]
[-r <число>] [-s <число>] [[-j <список узлов>] | [-k <список узлов>]]
[-w <тайм-аут>] [-R] [-S <адрес источника>] [-4] [-6] конечный_узел

Параметры
-t          Проверка связи с указанным узлом до прекращения.
            Для отображения статистики и продолжения проверки
            нажмите сочетание клавиш CTRL+BREAK;
            для прекращения нажмите CTRL+C.
-a          Определение имен узлов по адресам.
-n <число>  Число отправляемых запросов эха.
-l <размер>  Размер буфера отправки.
-f          Установка в пакете флага, запрещающего
            фрагментацию (только IPv4).
-i <TTL>     Задание срока жизни пакетов.
-v <TOS>     Задание типа службы (только IPv4. Этот параметр
            недоступен и не влияет на поле TOS в заголовке IP).
-r <число>   Запись маршрута для указанного числа прыжков
            (только IPv4).
```

```
Администратор: C:\Windows\system32\cmd.exe

C:\Users\Galya>dir>c:text.txt
C:\Users\Galya>dir>c:\text.txt
C:\Users\Galya>

text — Блокнот
Файл  Правка  Формат  Вид  Справка
'~ ̣ гбва®бвўг С -г Ё-ггв -гвЁЁ.
'ГаЁЁ-лθ -®-Га в® : FECA-4070

'®Гa!Ё-®г Ĩ ĨЁЁ C:\Users\Galya

20.06.2021 17:18 <DIR> .
20.06.2021 17:18 <DIR> ..
20.06.2021 12:29 <DIR> Contacts
20.06.2021 12:32 <DIR> Desktop
20.06.2021 12:52 <DIR> Documents
20.06.2021 12:29 <DIR> Downloads
20.06.2021 12:29 <DIR> Favorites
20.06.2021 12:29 <DIR> Links
20.06.2021 12:29 <DIR> Music
20.06.2021 12:29 <DIR> Pictures
20.06.2021 12:29 <DIR> Saved Games
20.06.2021 12:29 <DIR> Searches
20.06.2021 17:18 835 text.txt
20.06.2021 12:29 <DIR> Videos
1 д ®«®ў 835 ў ®в
13 Ĩ Ĩ®Ё 44я787я486я720 ў ®в бў®ў®м-®
```

```
C:\>date<c:\date.txt
Текущая дата: 20.06.2021
Введите новую дату (дд-мм-гг): 19.06.2020

C:\>_
```

EN 17:23 19.06.2020

```
Администратор: C:\Windows\system32\cmd.exe

C:\>more text.txt
Том в устройстве C не имеет метки.
Серийный номер тома: FECA-4070

Содержимое папки C:\Users\Galya

20.06.2021 17:18 <DIR> .
20.06.2021 17:18 <DIR> ..
20.06.2021 12:29 <DIR> Contacts
20.06.2021 12:32 <DIR> Desktop
20.06.2021 12:52 <DIR> Documents
20.06.2021 12:29 <DIR> Downloads
20.06.2021 12:29 <DIR> Favorites
20.06.2021 12:29 <DIR> Links
20.06.2021 12:29 <DIR> Music
20.06.2021 12:29 <DIR> Pictures
20.06.2021 12:29 <DIR> Saved Games
20.06.2021 12:29 <DIR> Searches
20.06.2021 17:18      835 text.txt
20.06.2021 12:29 <DIR> Videos
                1 файлов      835 байт
                13 папок 44a787a486a720 байт свободно

C:\>
```

```
date — Блокнот
Файл Правка Формат Вид Справка
20.06.2021
19.10.2012
14.06.1999
```

```
C:\>sort < date.txt
14.06.1999
19.10.2012
20.06.2021
```

## Задание 2. Сетевая активность

```
Администратор: C:\Windows\system32\cmd.exe
C:\>netstat /?

Отображение статистики протокола и текущих сетевых подключений TCP/IP.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p протокол] [-r] [-s] [-t] [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. Может применяться вместе
            с параметром -s.
-f          Отображение полного имени домена (FQDN) для внешних адресов.
-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
```

```
Администратор: C:\Windows\system32\cmd.exe
C:\>netstat /a

Активные подключения

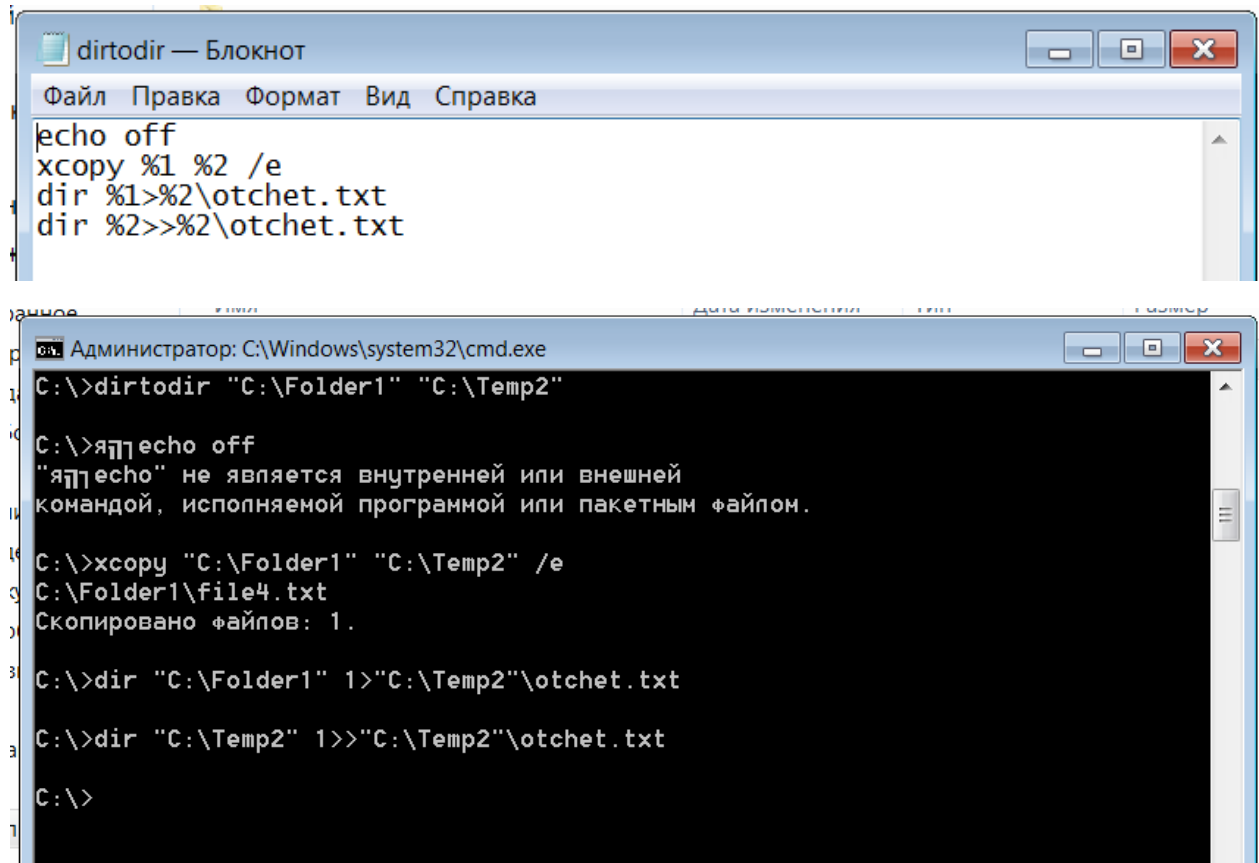
Имя      Локальный адрес      Внешний адрес      Состояние
TCP      0.0.0.0:135           Galya:0            LISTENING
TCP      0.0.0.0:445           Galya:0            LISTENING
TCP      0.0.0.0:554           Galya:0            LISTENING
TCP      0.0.0.0:5357          Galya:0            LISTENING
TCP      0.0.0.0:49152         Galya:0            LISTENING
TCP      0.0.0.0:49153         Galya:0            LISTENING
TCP      0.0.0.0:49154         Galya:0            LISTENING
TCP      0.0.0.0:49155         Galya:0            LISTENING
TCP      0.0.0.0:49157         Galya:0            LISTENING
TCP      192.168.58.128:139    Galya:0            LISTENING
TCP      [::]:135              Galya:0            LISTENING
TCP      [::]:445              Galya:0            LISTENING
TCP      [::]:554              Galya:0            LISTENING
TCP      [::]:5357             Galya:0            LISTENING
TCP      [::]:49152            Galya:0            LISTENING
TCP      [::]:49153            Galya:0            LISTENING
TCP      [::]:49154            Galya:0            LISTENING
TCP      [::]:49155            Galya:0            LISTENING
```

### Задание 3. Командные файлы.

Я ознакомилась с теоретической частью задания и просмотрела примеры выполнения файлов типа bat.

#### Задание 4. Создание пакетного файла, реализующего определенную последовательность действий в ОС Windows XP

*Пакетный файл, предназначенный для копирования каталога с его содержимым в заданное место назначения. Копируемый каталог и место назначения задаются в качестве пакетных параметров. После копирования каталога файл-отчет, содержащий информацию о количестве скопированных файлов и их месте расположения, в автоматическом режиме загружается в текстовый процессор «Блокнот».*



The image shows two windows from a Windows XP desktop. The top window is a Notepad application titled "dirtodir — Блокнот". It contains a batch script with the following commands:

```
echo off
xcopy %1 %2 /e
dir %1>%2\otchet.txt
dir %2>>%2\otchet.txt
```

The bottom window is a Command Prompt running as Administrator, titled "Администратор: C:\Windows\system32\cmd.exe". It shows the execution of the batch file "dirtodir.bat" with arguments "C:\Folder1" and "C:\Temp2". The output shows the execution of the commands and the creation of the report file:

```
C:\>dirtodir "C:\Folder1" "C:\Temp2"

C:\>яяecho off
"яяecho" не является внутренней или внешней
командой, исполняемой программой или пакетным файлом.

C:\>яяxcopy "C:\Folder1" "C:\Temp2" /e
C:\Folder1\file4.txt
Скопировано файлов: 1.

C:\>яяdir "C:\Folder1" 1>"C:\Temp2"\otchet.txt
C:\>яяdir "C:\Temp2" 1>>"C:\Temp2"\otchet.txt
C:\>
```

отер ▶ Локальный диск (C:) ▶ Temp2 ▶

Поиск: Temp2

Открыть ▶ Печать Новая папка

Имя

Дата изменения

Тип

Размер

Folder2

20.06.2021 15:21

Папка с файлами

file4

20.06.2021 15:27

Текстовый докум...

0 КБ

otchet

20.06.2021 18:32

Текстовый докум...

1 КБ

otchet — Блокнот

Файл Правка Формат Вид Справка

'@\_ ŷ гбва@бвŷГ С -Г Ё-ГГв -ГвЁЁ.  
'ГаЁ@-л@ -@-Га в@ : FECA-4070  
  
'@Гa|Ё-@Г İ İЁ C:\Folder1  
20.06.2021 18:31 <DIR> .  
20.06.2021 18:31 <DIR> ..  
20.06.2021 15:27 0 file4.txt  
20.06.2021 15:21 <DIR> Folder2  
1 д @«@ŷ 0 ŷ @в  
3 İ İЁ 44я786я933я760 ŷ @в бŷ@ŷ@п-@  
'@\_ ŷ гбва@бвŷГ С -Г Ё-ГГв -ГвЁЁ.  
'ГаЁ@-л@ -@-Га в@ : FECA-4070  
  
'@Гa|Ё-@Г İ İЁ C:\Temp2  
20.06.2021 18:32 <DIR> .  
20.06.2021 18:32 <DIR> ..  
20.06.2021 15:27 0 file4.txt  
20.06.2021 15:21 <DIR> Folder2  
20.06.2021 18:32 374 otchet.txt  
2 д @«@ŷ 374 ŷ @в  
3 İ İЁ 44я786я929я664 ŷ @в бŷ@ŷ@п-@