**ОСНОВНЫЕ ПОНЯТИЯ**

Командная оболочка - программа, которая действует как интерфейс между пользователем и ОС. Командная оболочка является интерпретатором командной строки, которая читает и выполняет команды, вводимые пользователем, а затем выводит результат.

**ОСНОВНЫЕ КОМАНДЫ**

**https://ab57.ru/cmdlist.html**

**Help имя\_команды –** получить справочную информацию по конкретной команде.

**CHCP номер –** переключение между кодовыми страницами. Например 866 - DOS, 1251 – Windows, 65001 – UTF-8

**COLOR Fo –** изменить внешний вид cmd. Две шестнадцатиричные цифры задают цвет фона и цвет символов.

**COPY –** копирование одного или нескольких файлов в командной строке. Позволяет объединить несколько файлов в один. Можно использовать подстановочные знаки. По умолчанию требуется подтверждение перезаписи существующих фалов, если только copy не выполняется в пакетном файле либо не указан флаг **/Y**.

**copy \*.txt D:\oldfiles\\*.txt -** копирование всех файлов с расширением txt из текущего каталога в каталог D:\oldfiles.

**copy file1.txt + file2.txt +file3.txt file123.txt** - копировать содержимое файлов **file1.txt**, **file2.txt** и **file3.txt** в файл **file123.txt**

**Copy con myfile.txt** - копирование с устройства **con** (console , консоль) в файл **myfile.txt** - т.е. ввод символов непосредственно с клавиатуры в файл. Для завершения ввода используется признак конца файла **CTRL+Z**

**copy NUL newfile.txt** - копирование с фиктивного устройства **nul** в файл, т.е. создание пустого файла с именем **newfile.txt**

**XCOPY –** используется для копирования файлов и каталогов с сохранением структуры. В отличии от COPY позволяет

* Копировать системные и скрытые файлы.
* Копировать каталоги.
* XCOPY – внешняя команда, COPY встроеная

**XCOPY источник [целевой\_объект] [/A | /M] [/D[:дата]] [/P] [/S [/E]] [/V] [/W] [/C] [/I] [/Q] [/F] [/L] [/G] [/H] [/R] [/T] [/U] [/K] [/N] [/O] [/X] [/Y] [/-Y] [/Z] [/B] [/EXCLUDE:файл1[+файл2][+файл3]...]**

* **/D:m-d-y** - Копирование файлов, измененных не ранее указанной даты. Если дата не указана, заменяются только конечные файлы, более старые, чем исходные.
* **/EXCLUDE:файл1[+файл2][+файл3]...** - Список файлов, содержащих строки с критериями для исключения файлов и папок из процесса копирования. Каждая строка должна располагаться в отдельной строке файла.
* **/P** - Вывод запросов перед созданием каждого нового файла.
* **/S** - Копирование только непустых каталогов с подкаталогами.
* **/E** - Копирование каталогов с подкаталогами, включая пустые.
* **/W** - Вывод запроса на нажатие клавиши перед копированием.
* **/C** - Продолжение копирования вне зависимости от наличия ошибок.
* **/Q** - Запрет вывода имен копируемых файлов.
* **/L** - Вывод имен копируемых файлов.
* **/G** - Копирование зашифрованных файлов в целевой каталог, не поддерживающий шифрование.
* **/H** - Копирование, среди прочих, скрытых и системных файлов.
* **/R** - Перезапись файлов, предназначенных только для чтения.
* **/T** - Создание структуры каталогов без копирования файлов. Пустые каталоги и подкаталоги не включаются в процесс копирования. Для создания пустых каталогов и подкаталогов используйте сочетание ключей /T /E.
* **/K** - Копирование атрибутов. При использовании команды XСOPY обычно сбрасываются атрибуты "Только для чтения".
* **/O** - Копирование сведений о владельце и данных ACL.
* **/Y** - Подавление запроса подтверждения на перезапись существующего целевого файла.
* **/-Y** - Запрос подтверждения на перезапись существующего целевого файла.
* **/B** - Копирование символической ссылки вместо ее целевого объекта.

**CD –** смена каталога. Без параметров отображает имя текущего каталога. Чтобы сменить диск нужно просто указать его имя и двоеточие **D:**. Перейти в родительский каталог **cd ..**

**CLS –** очистить экран командной строки

**COMP file1 file2 –** сравнить содержимое двух или нескольких файлов.

**CMD –** запуск новой копии командного процессора Windows. Как правило, используется при необходимости переопределить текущие настройки командной строки, задаваемые профилем пользователя и параметрами компьютера.

**CMD [/A | /U] [/Q] [/D] [/E:ON | /E:OFF] [/F:ON | /F:OFF] [/V:ON | /V:OFF] [[/S] [/C | /K] строка]**   
Параметры командной строки:  
**/C**  Выполнение указанной команды (строки) с последующим завершением.  
**/K**  Выполнение указанной команды (строки) без последующего завершения.  
**/S**  Изменение поведения после /C или /K (см. ниже)  
**/Q**  Отключение режима вывода команд на экран (ECHO).  
**/D**  Отключение выполнения команд AutoRun из реестра (см. ниже)  
**/A**  Вывод результатов выполнения команд в формате ANSI.  
**/U**  Вывод результатов выполнения команд в формате UNICODE.  
**/T:fg**  Выбор цвета переднего плана/фона (более подробно см. COLOR /?)  
**/E:ON**  Разрешение расширенной обработки команд (см. ниже)  
**/E:OFF**  Запрет расширенной обработки команд (см. ниже)  
**/F:ON**  Разрешение символов завершения имен файлов и папок (см. ниже)  
**/F:OFF**  Запрет символов завершения имен файлов и папок (см. ниже)  
**/V:ON**  Разрешение отложенного расширения переменных среды с применением символа '!' в качестве разделителя. Например, /V:ON разрешает использовать !var! в качестве расширения переменной var во время выполнения. Синтаксис var служит для расширения переменных при вводе, что приводит к совсем другим результатам внутри цикла FOR.  
  
**/V:OFF**  Запрет отложенного расширения переменных среды.

**DATE и TIME** - используются для отображения или изменения текущей даты или времени. без параметров отображает текущую дату и запрашивает ввод новой даты. Для сохранения текущей даты нажмите клавишу ENTER. С параметром устанавливают новое значение сразу.

**DEL(ERASE) –** используется для удаления одного или нескольких файлов.

**DEL [/P] [/F] [/S] [/Q] [/A[[:]атрибуты]] имена**

**имена** - Имена одного или нескольких файлов. Для удаления сразу нескольких файлов используются подстановочные знаки. Если указан каталог, из него будут удалены все файлы.

**/P** - Запрос на подтверждение перед удалением каждого файла.  
**/F** - Принудительное удаление файлов, доступных только для чтения.  
  
**/S** - Удаление указанных файлов из всех подкаталогов.  
**/Q** - Отключение запроса на подтверждение при удалении файлов.  
**/A** - Отбор файлов для удаления по атрибутам.

Атрибуты :  
**S** - Системные файлы  
**R** - Доступные только для чтения  
**H** - Скрытые файлы  
**A** - Файлы для архивирования  
Префикс "-" имеет значение НЕ - например **-H** - не скрытый файл.

**DIR –** отобразить список файлов и подкаталогов для указанного каталога.

**DIR [диск:][путь][имя\_файла] [/A[[:]атрибуты]] [/B] [/C] [/D] [/L] [/N] [/O[[:]порядок]] [/P] [/Q] [/S] /T[[:]время]] [/W] [/X] [/4]**   
Параметры командной строки:   
**[диск:][путь][имя\_файла]** - Диск, каталог и/или файлы, которые следует включить в список.  
**/A** - Вывод файлов с указанными атрибутами:  
**D** Каталоги   
**R** Доступные только для чтения  
**H** Скрытые файлы  
**A** Файлы для архивирования  
**S** Системные файлы  
Префикс "-" имеет значение **НЕ**  
**-S** НЕ системные файлы.  
  
**/B** - Вывод только имен файлов.  
**/C** - Применение разделителя групп разрядов для вывода размеров файлов (по умолчанию). Для отключения этого режима служит ключ /-C.  
**/D** - Вывод списка в несколько столбцов с сортировкой по столбцам.  
**/L** - Использование нижнего регистра для имен файлов.  
**/N** - Отображение имен файлов в крайнем правом столбце.  
**/O** - Сортировка списка отображаемых файлов.  
Порядок: **N** По имени (алфавитная), **S** По размеру (сперва меньшие), **E** По расширению (алфавитная), **D** По дате (сперва более старые), **G** Начать список с каталогов. Префикс "-" имеет значение **НЕ**

**dir /o:d**  
  
**/P** - Пауза после заполнения каждого экрана.  
**/Q** - Вывод сведений о владельце файла.  
**/R** - Отображение альтернативных потоков файлов.  
**/S** - Вывод списка файлов из указанного каталога и его подкаталогов.  
**/T** - Выбор поля времени для отображения и сортировки  
время:  
**C** Создание (время создания - Create )  
**A** Последнее использование (последний доступ - Accsess )  
**W** Последнее изменение (последняя модификация Write)  
**/W** - Вывод списка в несколько столбцов.  
**/X** - Отображение коротких имен для файлов, чьи имена не соответствуют стандарту 8.3. Формат аналогичен выводу с ключом /N, но короткие имена файлов выводятся слева от длинных. Если короткого имени у файла нет, вместо него выводятся пробелы.   
**/4** - Вывод номера года в четырехзначном формате  
  
Стандартный набор ключей можно записать в переменную среды **DIRCMD**. Для отмены их действия введите в команде те же ключи с префиксом "-", например: /-W.

**SET DIRCMD=/O:N /B /P**

**ECHO –** применяется для вывода текстовых сообщений на стандартный вывод и для переключения режима отображения команд на экране. Можно использовать для записи в текстовый файл с использованием перенаправления вывода. Добавляет возврат каретки и перевод строки.

Чтобы вывести служебные символы, интерпретируемые командным процессором, используется символ ^.

**ECHO [ON | OFF]** - включить / выключить режим отображения вводимых команд на экране.  
**ECHO [сообщение]** отобразить текст сообщения на экране.

**ECHO** - при вводе команды без параметров, отображается текущий режим отображения команд

**ECHO. –** вывод пустой строки.

**EXIT exitCode –** используется для завершения пакетных файлов с установкой значения переменной ERRORLEVEL или завершения командного процессора, если он выполняется вне пакетного файла.

**/B** - Предписывает завершить текущий пакетный файл-сценарий вместо завершения CMD.EXE. Если вызываем один батник из другого, и вызываем exit то завершится и вызывающий.

**fc** - сравнение содержимого файлов

**FIND.EXE –** утилита для поиска текстовой строки.

**FIND [/V] [/C] [/N] [/I] [/OFF[LINE]] "строка" [[диск:][путь]имя\_файла[ ...]]**  
**/V** Вывод всех строк, НЕ содержащих заданную строку.  
**/C** Вывод только общего числа строк, содержащих заданную строку.  
**/N** Вывод номеров отображаемых строк.  
**/OFF[LINE]** Не пропускать файлы с установленным атрибутом "Автономный".  
**/I** Поиск без учета регистра символов.  
**"строка"** - Искомая строка, обязательно в двойных кавычках.  
**[диск:][путь]имя\_файла** - Один или несколько файлов, в которых выполняется поиск.   
Если путь не задан, поиск выполняется в тексте, введенном с клавиатуры  
либо переданном по конвейеру другой командой.

**FINDSTR –** поиск текстовой строки в одном или нескольких файлах с использованием регулярных выражений.

**FINDSTR [/B] [/E] [/L] [/R] [/S] [/I] [/X] [/V] [/N] [/M] [/O] [/P] [/F:файл] [/C:строка] [/G:файл] [/D:список\_папок] [/A:цвета] [/OFF[LINE]] строки [[диск:][путь]имя\_файла[ ...]]**   
**/B** - Искать образец только в началах строк.  
**/E** - Искать образец только в конце строк.  
**/L** - Поиск строк дословно.  
**/R** - Поиск строк как регулярных выражений.  
**/S** - Поиск файлов в текущей папке и всех ее подпапках.  
**/I** - Определяет, что поиск будет вестись без учета регистра.  
**/X** - Печатает строки, которые совпадают точно.  
**/V** - Печатает строки, не содержащие совпадений с искомыми.  
**/N** - Печатает номер строки, в которой найдено совпадение, и ее содержимое.  
**/M** - Печатает только имя файла, в которой найдено совпадение.  
**/O** - Печатает найденный строки через пустую строку.  
**/P** - Пропускает строки, содержащие непечатаемые символы.  
**/OFF[LINE]** - Не пропускает файлы с установленным атрибутом "Автономный".  
**/A:цвета** - Две шестнадцатеричные цифры - атрибуты цвета. См. "COLOR /?"  
**/F:файл** - Читает список файлов из заданного файла (/ для консоли).  
**/C:строка** - Использует заданную строку как искомую фразу поиска.  
**/G:файл** - Получение строк из заданного файла (/ для консоли).  
**/D:список\_папок** - Поиск в списке папок (разделяются точкой с запятой).  
**строка** - Искомый текст.  
**[диск:][путь]имя\_файла** - Задает имя файла или файлов.

**FOR –** используется для циклической обработки строк, файлов, каталогов.

**FOR %переменная IN (набор) DO команда [параметры]**   
Параметры:  
**%переменная** - Однобуквенный подставляемый параметр.  
**(набор)** - Определяет набор, состоящий из одного или нескольких элементов, обрабатываемых командой.   
**команда** - Команда, которую следует выполнить для каждого элемента набора.  
**параметры** - Параметры для команды, выполняемой по отношению к элементам набора.

**FOR /D %переменная IN (набор) DO команда [параметры]**

Ключ /D задает в качестве набора имена каталогов (не файлов).

**FOR /R [[диск:]путь] %переменная IN (набор) DO команда [параметры]**

Ключ /R задает выполнение команды для каталога [диск:]путь, а также для всех подкаталогов этого пути.

**FOR /L %переменная IN (начало,шаг,конец) DO команда [параметры]**

Ключ /L задает обработку набора из последовательности чисел с заданными началом, концом и шагом приращения. Так, набор (1,1,5) раскрывается в (1 2 3 4 5)

**FOR /F ["ключи"] %переменная IN ('команда' | “строка” | набор-файлов) DO команда [параметры]**

Ключ /F задает обработку файлов, строковых значений или результатов стандартного вывода другой команды.

Ключи:

**skip=n** - число пропускаемых при обработке строк от начала файла.

**GOTO метка –** выполнение безусловного перехода к указанной метке в командном файле.

Метка представляет собой строку символов, начинающихся с двоеточия (**:metka**).

В качестве метки можно использовать **:EOF**, в результате произойдет переход в конец исполняемого файла.

**HOSTNAME –** отобразить имя компьютера в командной строке windows.

**IF –** оператор условного ветвления в командных файлах.

**NOT –** отрицание в условии.

**Val1** == **val2** - сравнение нескольких значений.

**EXIST file\_name –** условие истинно, если файл с таким именем существует

**ELSE –** блок, который выполняется если условие ложно. Должен располагаться в той же строке, что и команда, следующая за ключевым словом **IF.**

Условие **DEFIND –** проверяет, определена ли переменная окружения.

**Операторы сравнения,** которые можно использовать в IF:

**EQU** - равно  
**NEQ** - не равно  
**LSS** - меньше  
**LEQ** - меньше или равно  
**GTR** - больше  
**GEQ** - больше или равно

**IF EXIST имя\_файла. (del имя\_файла.) ELSE echo имя\_файла. Missing**

**IF EXIST имя\_файла. (  
del имя\_файла.  
) ELSE (  
echo имя\_файла. missing.  
)**

**IPCONFIG –** отображение текущих настроек протокола TCP/IP и обновление некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола Dynamic Host Configuration Protocol (DHCP).

**ipconfig [/allcompartments] [/? | /all | /renew [адаптер] | /release [адаптер] | /renew6 [адаптер] | /release6 [адаптер] | /flushdns | /displaydns | /registerdns | /showclassid адаптер | /setclassid адаптер [идентификатор\_класса] ] /showclassid6 адаптер | /setclassid6 адаптер [идентификатор\_класса] ]**

**/all -** Вывод подробных сведений о конфигурации. **/release -** Освобождение адреса IPv4 для указанного адаптера. **/release6 -** Освобождение адреса IPv6 для указанного адаптера. **/renew -** Обновление адреса IPv4 для указанного адаптера. **/renew6 -** Обновление адреса IPv6 для указанного адаптера. **/flushdns -** Очистка кэша сопоставителя DNS. **/registerdns -** Обновление всех DHCP-аренд и перерегистрация DNS-имен **/displaydns -** Отображение содержимого кэша сопоставителя DNS. **/showclassid -** Отображение всех допустимых для этого адаптера идентификаторов классов DHCP.  **/setclassid -** Изменение идентификатора класса DHCP. **/showclassid6 -** Отображение всех допустимых для этого адаптера идентификаторов классов DHCP IPv6. **/setclassid6 -** Изменение идентификатора класса DHCP IPv6. **адаптер -** Имя подключения (можно использовать знаки подстановки \* и ? )

**MD(MKDIR)**  - создание каталогов в командной строке Windows.

**MD [диск:]путь**

создает при необходимости все промежуточные каталоги пути.

**MORE –** предназначена для постраничного вывода текстовых данных в окне консоли. Можно читать данные из файла (нескольких файлов), либо перенаправить вывод из другой команды.

**MORE [/E [/C] [/P] [/S] [/Tn] [+n]] < [диск:][путь]имя\_файла**

* **/E -** Разрешение использования дополнительных возможностей. **/C -** Очистка экрана перед выводом каждой страницы. **/P -** Учет символов перевода страницы. **/S -** Сжатие нескольких пустых строк в одну строку. **/Tn -** Замена символов табуляции n пробелами (по умолчанию n = 8).
* **+n -** Начало вывода первого файла со строки с номером n.

**в ответ на приглашение -- More --** можно вводить следующие команды: **P n -** Вывод следующих n строк. **S n -** Пропуск следующих n строк. **F -** Вывод следующего файла. **Q -** Завершение работы. **= -** Вывод номера строки. **? -** Вывод строки подсказки. **пробел -** Вывод следующей страницы. **ENTER -** Вывод следующей строки.

**MOVE –** перемещение или переименование файлов и каталогов.

Перемещение одного или более файлов: **MOVE [/Y | /-Y] [диск:][путь]имя\_файла1[,...] назначение**   
Переименование папки:  
**MOVE [/Y | /-Y] [диск:][путь]имя\_папки новое\_имя\_папки**

**/Y** - Перезаписывать существующие файлы назначения без предупреждения.  
**/-Y** - Предупреждать при перезаписи существующего файла назначения.

*При перемещении папки в несуществующий каталог он не будет создан автоматически и команда завершится ошибкой. Команда* ***move*** *не работает с файлами, имеющими атрибуты "скрытый " и "системный".*

**move folder1 folder2** - переименовать папку с именем **folder1** в **folder2** в текущем каталоге.  
  
**move E:\test\folder1 E:\test\folder2** - переименование с указанием абсолютных путей.  
  
**move C:\file1.txt D:\** - переместить файл **file1.txt** с диска **C:** на диск **D:**  
  
**move c:\test\file1.txt D:\folder2\file2.txt** - перенести файл **file1.txt** из каталога **test** диска **C:** в каталог **folder2** диска **D:** под именем **file2.txt**  
  
**move C:\Folder1\\*.\* D:\Folder2\** - переместить все файлы из каталога **Folder1** диска C: в каталог **Folder2** диска D:

**NET –** управление сетевой конфигурацией. утилита для остановки и запуска служб из командной строки.

**Команды:**

* **ACCOUNTS –** обновление базы данных учетных записей пользователей, а также для изменения параметров входа в систему для всех учетных записей. Без параметров отображаются текущие параметры паролей, ограничения на вход и сведения о домене.
* **COMPUTER \\имя\_компьютера {/ADD | /DEL} –** добавляет или удаляет компьютеры из базы данных домена.
* **CONFIG –** отображает информацию о настройке служб рабочей станции или сервера
* **FILE -** отображает список открытых по сети файлов и может принудительно закрывать общий файл и снимать файловые блокировки.
* **GROUP | LOCALGROUP** – добавляют, выводят на экран или изменяют группы. Первая используется для работы с группами домена, а вторая с локальными группами компьютера.
* **HELPMSG -** выводит информацию о сетевых сообщениях Windows (например, сообщения об ошибках и предупреждающие сообщения). Если ввести команду NET HELPMSG и номер ошибки, то Windows выведет пояснения для этого сообщения и предложит возможные варианты действий, которые можно предпринять для устранения ошибки.
* **HELP command -** отобразить подробную справку по использованию команды NET.
* **PAUSE имя\_службы –** приостановить выполнение службы
* **CONTINUE имя\_службы –** продолжить работу службы.
* **SESSION –** завершает текущие сеансы связи между данным компьютером и другими компьютерами (DELETE) сети или выводит их список.
* **SHARE –** разрешает использовать серверные ресурсы другим пользователям сети.

**NET SHARE общий\_ресурс=диск:путь [/GRANT:пользователь,[READ | CHANGE | FULL]] [/USERS:число | /UNLIMITED] [/REMARK:"текст"] [/CACHE:Manual | Documents| Programs | BranchCache | None]**

* **STATISTICS –** выводит журнал статистики для локальной службы рабочей станции или сервера.
* **START service –** запуск системных служб
* **STOP service –** остановка системных служб
* **TIME –** синхронизирует часы компьютера с часами другого компьютера или домена, либо отображает время компьютера или домена.
* **USE –** подключает компьютер к общему ресурсу или отключает компьютер от общего ресурса.
* **USER –** просмотр, создание и изменение учетных записей пользователей на компьютерах.
* **VIEW –** отображает список общих ресурсов компьютера. При использовании без параметров отображается список всех компьютеров в текущем домене или рабочей группе.

**NETSTAT –** предназначена для получения сведений о состоянии сетевых соединений и слушаемых на данном компьютере портах TCP и UDP, а также, для отображения статистических данных по сетевым интерфейсам и протоколам.

**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 по протоколам. Допустимые значения: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP или UDPv6.
* **-r** - Отображение содержимого таблицы маршрутов.
* **-s** - Отображение статистики протокола. По умолчанию статистика отображается для протоколов IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP и UDPv6. Параметр -p позволяет указать подмножество выводимых данных.
* **-t** - Отображение текущего подключения в состоянии переноса нагрузки с процессора на сетевой адаптер при передаче данных ( "offload" ).
* **-v** - Подробный вывод информации, если это возможно.  
  **интервал** - Повторный вывод статистических данных через указанный интервал в секундах. Для прекращения вывода данных нажмите клавиши CTRL+C. Если параметр не задан, сведения о текущей конфигурации выводятся один раз.

**netstat -a | more** - отобразить все соединения в постраничном режиме вывода на экран.  
  
**netstat -a -n| more** - то же, что и в предыдущем примере, но с отображением номеров портов и IP-адресов в числовом формате. В отличие от предыдущего примера, команда **netstat** с параметром **-t** отрабатывает намного быстрее.   
  
**netstat -a -f | more** - то же, что и в предыдущем примере, но с отображением полных DNS-имен узлов, участвующих в соединениии.  
  
**netstat -a > C:\netstatall.txt** - отобразить все соединения с записью результатов в файл C:\netstatall.txt.  
  
**netstat -a | find /I "LISTENING"** - отобразить все соединения со статусом LISTENING, т.е. отобразить список сетевых интерфейсов и портов, ожидающих входящие соединения ( "слушаемых" портов ). Ключ **/I** в команде **find** указывает, что при поиске текста, не нужно учитывать регистр символов.   
  
**netstat -a | find /I "listening" > C:\listening.txt** - отобразить все соединения со статусом LISTENING с записью результатов в файл C:\listening.txt.

**PATH –** используется для указания или просмотра путей поиска исполняемых файлов.

**PATH ;** - очистить путь поиска используемых файлов, ограничив его текущим каталогом.

Команда PATH без параметров отображает текущий путь поиска. В командную строку допускается включение переменной **%PATH%** , задающей прежний путь поиска.

**PAUSE –** приостановить выполнение командного файла с выводом сообщения «Для продолжения нажмите любую клавишу…». Может быть использована для отладки, либо предотвращения закрытия консоли.

**RMDIR (RD) [/S] [/Q] [диск:]путь -** предназначена для удаления каталогов файловой системы Windows. Не поддерживает шаблоны.

**/S –** Удаление каталога вместе с подкаталогами и файлами. **/Q -** Отключение запроса подтверждения при удалении дерева каталогов с помощью ключа /S.

**RENAME (REN) [диск:][путь]имя\_файла1 имя\_файла2 –** переименование фалов и каталогов.

**Диск:** - диск на котором находится исходный файл или каталог;  
**путь** - путь к исходному файлу или каталогу;  
**имя\_файла1** - исходное имя файла или каталога;  
**имя\_файла2** - новое имя файла или каталога;

**rename file1.txt file2.txt** - переименовать файл **file1.txt** , находящийся в текущем каталоге, присвоив ему имя **file2.txt**

**ren "My Programms" "Мои программы"** - переименовать папку текущего каталога **My Programms** в **Мои программы**. Имена и пути, содержащие пробелы, должны заключаться в двойные кавычки. Символы русского языка должны быть представлены в DOS-кодировке.  
  
**ren "C:\My files\\*.\*" \*.saved** - переименовать все файлы, находящиеся в папке **C:\My Files** изменив только их расширение на **.saved**.   
  
**rename "C:\My files\My Folder" "My New Folder"** - переименовать папку **C:\My files\My Folder"** в **My New Folder**.  
  
**rename "C:\My files\My Folder\data1.db" data2.db** - переименовать файл **data1.db**, находящийся в папке **C:\My files\My Folder**, присвоив ему имя **data2.db**

**SC.EXE –** используется для конфигурирования, опроса состояния, остановки, запуска и добавления системных служб, а также работать не только с системными службами, но и с драйверами. Позволяет управлять службами даже на удаленной машине.

**sc сервер [команда] [имя службы] параметр1 параметр2 ...**

**сервер** - имя или IP-адрес удаленной системы в формате "\\cервер".

**команды**:

* **Query state** -Запрос состояния службы или перечисление состояний типов служб.
* **queryex** - Запрос расширенного состояния службы или перечисление состояний типов служб.
* **start** - Запуск службы.
* **pause** - Отправка службе управляющего запроса PAUSE для приостановки ее работы.
* **interrogate** - Отправка службе управляющего запроса INTERROGATE.
* **continue** - Отправка службе управляющего запроса CONTINUE для возобновления ее работы.
* **stop** - Отправка службе запроса STOP.
* **config** - Изменение конфигурации службы (постоянное).
* **description** - Изменение описания службы.
* **failure** - Изменение действия, выполняемого службой при сбое.
* **failureflag** - Изменение флага действия, выполняемого службой при сбое.
* **sidtype** - Изменение типа SID службы.
* **privs**- Изменение привилегий, требуемых для службы.
* **qc** - Запрос данных конфигурации для службы.
* **qdescription** - Запрос описания службы.
* **qfailure** - Запрос действия, выполняемого службой при сбое.
* **qfailureflag** - Запрос флага действия, выполняемого службой при сбое.
* **qsidtype** - Запрос типа SID службы.
* **qprivs** - Запрос привилегий, требуемых для службы.
* **qtriggerinfo** - Запрос параметров службы.
* **qpreferrednode** - Запрос предпочтительного узла NUMA службы.
* **delete** - Удаление службы (из реестра).
* **create** - Создание службы (добавление ее в реестр).
* **control** - Отправка службе управляющего сигнала.
* **sdshow** - Отображение дескриптора безопасности службы.
* **sdset** - Установка дескриптора безопасности службы.
* **showsid** - Отображение строки SID службы, соответствующей произвольному имени.
* **triggerinfo** - Настройка параметров триггеров службы.
* **preferrednode** - Задание предпочтительного узла NUMA службы.
* **GetDisplayName** - Получение параметра DisplayName для службы.
* **GetKeyName** - Получение имени раздела для службы (ServiceKeyName).
* **EnumDepend** - Перечисление зависимостей службы.

**SHUTDOWN.EXE -** Завершение сеанса пользователя, перезагрузка компьютера, перевода его в спящий режим или выключения питания.

**SORT \R –** сортировка в алфавитном порядке строк текстового файла или стандартного вывода. \R – в обратном порядке.

**START –** запуск указанной команды или программы в отдельном окне, с возможностью указания параметров их выполнения.

**START ["заголовок"] [/D путь] [/I] [/MIN] [/MAX] [/SEPARATE | /SHARED] [/LOW | /NORMAL | /HIGH | /REALTIME | /ABOVENORMAL | /BELOWNORMAL] [/NODE < узел NUMA >] [/AFFINITY < маска сходства >] [/WAIT] [/B] [команда/программа] [параметры]**

Параметры командной строки:  
**"заголовок"** - заголовок окна. Обязательно в двойных кавычках.  
**путь** - рабочий каталог для запускаемого приложения.  
**B** - запуск приложения без создания нового окна с отключением обработки сочетания клавиш CTRL+C. Если приложение не обрабатывает сочетание клавиш CTRL+C самостоятельно, единственным способом его прерывания является использование сочетания клавиш CTRL+Break.  
**I** - Новой средой станет исходная среда, переданная cmd.exe, а не текущая среда.  
**MIN** - Запуск команды/программы в свернутом окне.  
**MAX** - Запуск команды/программы в развернутом окне.  
**LOW** - Запуск приложения с приоритетом IDLE (самый низкий приоритет).  
**NORMAL** - Запуск приложения с приоритетом NORMAL.  
**HIGH** - Запуск приложения с приоритетом HIGH.  
**REALTIME** - Запуск приложения с приоритетом REALTIME (самый высокий приоритет).  
**NODE** - Указывает предпочтительный узел NUMA в качестве десятичного целого числа.  
**WAIT** - Запуск приложения с ожиданием его завершения.  
**ABOVENORMAL** - Запуск приложения с классом приоритета ABOVENORMAL (выше стандартного)  
**BELOWNORMAL** - Запуск приложения с классом приоритета BELOWNORMAL (ниже стандартного)  
**команда/программа** - Если это внутренняя команда cmd.exe или пакетный файл, обработчик команд (cmd.exe) запускается с ключом /K. Это означает, что окно не будет закрыто после завершения команды. Если это не внутренняя команда cmd.exe и не пакетный файл, значит, это программа, которая будет запущена в графическом или текстовом окне.  
**параметры** - Параметры, передаваемые команде/программе.

*ПРИМЕРЫ:*

* **start** - при запуске без параметров будет открыто новое окно интерпретатора команд CMD.
* **start "My new CMD window"** - как и в предыдущем случае, выполнится запуск CMD в новом окне, но в качестве заголовка окна будет отображаться текст **My new CMD window**
* **start devmgmt.msc** - выполнится запуск по расширению **.msc** диспетчера устройств Windows.
* **start http://google.com** - выполнится запуск обозревателя Интернет и откроется страница поисковика Google.
* **start mailto:test@mail.ru** - выполнится запуск почтового клиента в режиме подготовки электронного письма для адреса **test@mail.ru**.
* **start /min notepad.exe** - выполнится запуск блокнота в свернутом окне.
* **start "Backup Files" /min /belownormal mybackup.bat** - запуск командного файла в свернутом окне с пониженным приоритетом.
* **start /abovenormal /MAX winword.exe** - запуск редактора Microsoft Word в новом окне, развернутом на весь экран и с повышенным приоритетом.
* **start "" /high /MAX "C:\Program Files\Good game\MyGame"** - запуск программы **MyGame** с высоким приоритетом.

**SYSTEMINFO –** отображает сведения о конфигурации операционной системы на локальном или удаленном компьютере.

**TASKKILL** – используется для завершения процессов по идентификаторам или именам исполняемых файлов. *При завершении процессов как локально, так и удаленно, результат выполнения команды* ***TASKKILL*** *зависит от прав пользователя, в контексте учетной записи которого выполняется команда.*

Можно завершать сразу несколько процессов, используя фильтры, такие же как и в tasklist с помощью опции **/FI**.

**TASKKILL /IM notepad.exe** - завершить процесс, исполняемым образом которого является **notepad.exe** . Если таких процессов более одного - то будут завершены все.

**taskkill /PID 1234 /T** - завершить процесс с идентификатором **1234** и все его дочерние процессы ( /T ) . Одной командой можно завершить несколько процессов, задавая их PID - **taskkill /PID 1234 /PID 2345 /PID 800**. Для определения идентификатора процессов используется команда **tasklist.**

**TASKKILL /F /FI "PID ge 2000" /FI "WINDOWTITLE eq Arc\*"** - принудительно (/F) завершить процесс, идентификатор которого больше или равен **2000** **и** заголовок окна которого , начинается с текста **Arc.**

**TASKLIST –** утилита для получения списка процессов, выполняющихся в системе. Позволяет получить список процессов удаленного компьютера.

Поиск по фильтрам осуществляется с помощью флага **/FI**.

**Фильтры:**

Имя фильтра Допустимые операторы Допустимые значения

----------- --------------- --------------------------

STATUS eq, ne RUNNING |

NOT RESPONDING | UNKNOWN

IMAGENAME eq, ne Имя образа

PID eq, ne, gt, lt, ge, le Значение PID

SESSION eq, ne, gt, lt, ge, le Номер сессии

SESSIONNAME eq, ne Имя сессии

CPUTIME eq, ne, gt, lt, ge, le Время CPU в формате

hh:mm:ss.

hh - часы,

mm - минуты, ss - секунды

MEMUSAGE eq, ne, gt, lt, ge, le Использование памяти в KБ

USERNAME eq, ne Имя пользователя в формате

[<домен>\<пользователь>]

SERVICES eq, ne Имя службы

WINDOWTITLE eq, ne Название окна

MODULES eq, ne Имя DLL

**tasklist -s 192.168.0.1 -U mydomain\admin -P mypass /FI "memusage gt 10000"** - отобразить список процессов, использующих более 10000кб ( 10 Мб) памяти на компьютере с IP-адресом 192.168.0.1 . При подключении к удаленному компьютеру используется имя пользователя **admin** в домене **mydomain** и пароль **mypass.**   
**tasklist /fi "username ne NT AUTHORITY\Система"** - отобразить список процессов, выполняющихся не от имени локальной системной учетной записи.

**TIMEOUT [/T] таймаут [/NOBREAK] –** используется для организации режима ожидания фиксированного интервала времени в секундах.

**/T таймаут** - Время ожидания в секундах. Допустимый интервал: от -1 до 99999 секунд.  
**/NOBREAK** - Игнорировать нажатия клавиш, ждать указанное время.

TIMEOUT /T -1 - ожидание нажатия любой клавиши. На экран выдается сообщение: «Нажмите любую клавишу для продолжения...».

**TRACERT.EXE –** утилита трассировки маршрута до заданного узла. Позволяет получить цепочку узлов, через которую проходит IP-пакет, адресованный конечному узлу. Указывать можно доменной имя либо IP-адрес.

**TREE –** позволяет отобразить иерархическую структуру каталогов в графическом виде. **/F** - Вывод имен файлов в каждой папке.

**TYPE –** вывод на экран содержимого текстового файла.

**WHOAMI –** получение сведений о текущем пользователе: его имени, группе, а также о соответствующих идентификаторах безопасности (SID), привилегиях, идентификаторах входа.

**В cmd можно использовать “шаблонные” символы:**

* **\* -** 0 или несколько символов
* **? –** один символ.

Например:

**DIR C:\WINDOWS\\*.dll** - отобразить список файлов с расширением **dll** из каталога C:\WINDOWS

**DIR C:\WINDOWS\system32\???t.\*** - отобразить список файлов, имя которых содержит 3 любых символа ( ??? ) и символ **t**

**Командные файлы** (пакетные файлы, скрипты, сценарии, ”батники”) - это обычные текстовые файлы с расширением **.bat** или **.cmd**, строки которых представляют собой специальные команды командного процессора (интерпретатора команд – CMD Windows ) и/или имена исполняемых файлов с параметрами.

Набор команд может хранится и в файле **txt**. Запустить их можно командой **cmd.exe < commands.txt.** Таким же образом можно запустить и bat с cmd.

**Отличие bat от cmd:**

Bat изначально был создан для систем Dos, подразумевается что он не будет содержать вызовов подпрограмм не включенных в Dos/

Cmd – пакетный файл специально для cmd.exe.

В файлах с расширением CMD ERRORLEVEL Для команд PATH/APPEND/PROMPT/SET/ASSOC будет установлен независимо от ошибок, то есть если ошибок не было, он перезапишется в 0. В файлах с расширением bat эта переменная будет установлена только при ошибке.

**com**

**Команды для использования в пакетных файлах, передача параметров в пакетный файл**

В пакетном файле можно запускать обычные команды. Для объединения команд могут использоваться следующие символы:

* **команда1 & команда2 -** используется для разделения нескольких команд в одной строке
* **команда1 && команда2 –** вторая команда выполнится только в том случае, если выполнена успешно первая команда (ее код возврата равен 0). Успешность выполнения команды определяется значением специальной переменной среды ERRORLEVEL.
* **команда1 || команда2 –** вторая команда выполнится только в том случае, если первая команда выполнилась с ошибкой.

**Переменные окружения –** переменные, значения которых определяют среду, в которой выполняется команда или пакетный файл.

Значения, принимаемые этими переменными формируются при загрузке Windows, регистрации пользователя в системе, старте или завершении некоторых приложений, и, кроме того, могут быть заданы с помощью специальной команды **SET.**

**SET имя\_переменной=значение**

Получить доступ к переменной среды можно заключив ее в %.

**Echo %date%**

Вывести список всех переменных окружения можно вызовом **SET** без параметров. Значения некоторых переменных не будут отображаться в SET. Их значение можно посмотреть через **echo**. В основном это переменные изменяемые динамически:

**%CD% -** Принимает значение строки текущего каталога.

**%DATE% -** Принимает значение текущей даты.

**%TIME% -** Принимает значение текущего времени.

**%RANDOM% -** Принимает значение случайного десятичного числа в диапазоне 1 -32767.

**%ERRORLEVEL% -** Принимает текущее значение кода завершения задачи ERRORLEVEL

**%CMDEXTVERSION% -** Принимает значение версии командного процессора CMD.EXE для расширенной обработки команд.

**%CMDCMDLINE% -** Принимает значение строки, которая вызвала командный процессор.

Наиболее часто используемой переменной окружения является **PATH**, которая указывает на пути к исполняемым файлам. Каталоги в переменной PATH разделяются точкой с запятой.

Значения переменных, установленных через SET действительны **только для текущего сеанса** командной строки. Чтобы установить постоянные переменные используется команда **SetX**, которая записывает переменные в реестр.

С помощью команды SET и опции /P можно запросить ввод пользователя.  
**set /p password="Enter password - ".** До того пока пользователь не введет ответ, выполнение командного файла будет приостановлено.

Для выделения части значения, принимаемого переменной, используется следующая конструкция:   
  
**переменная:~x,y** - где **x** - число пропускаемых символов от начала строки, а **y** - количество символов, используемых в качестве значения переменной.

Например **SET tm=%TIME:~0,5%** взять только часы и минуты из текущего времени.

**SETLOCAL | ENABLEDELAYEDEXPANSION | DISABLEDELAYEDEXPANSION –** используется для временного изменения значений переменных среды. Изменения переменных среды после выполнения SETLOCAL являются локальными относительно текущего пакетного файла. Они вернуться в прежнее значение после выполнения команды **ENDLOCAL**, либо по завершению командного файла.

ENABLEEXTENSIONS или DISABLEEXTENSIONS позволяют включить или отключить расширенную обработку команд до выполнения команды.

Присваиваемое переменным значение внутри команд, задаваемых скобками (например в командах IF или FOR), остается без изменений.

Для обхода данного ограничения используется запуск командного процессора с параметром /V:ON и вместо знаков процента, для получения принимаемого переменной значения, используются восклицательные знаки. Того же можно добиться используя **Setlocal EnableDelayedExpansion.**

**@echo off**

**set VAR=before**

**Setlocal EnableDelayedExpansion**

**if "%VAR%" == "before" (**

**set VAR=after**

**if "!VAR!" == "after" @echo with percent=%VAR% , with voskl=!VAR!**

**)**

**Параметры** в пакетный файл передаются следующим образом:

**BAT-файл параметр1 параметр2 ... параметрN**

В самом пекетном файле они будут доступны через знак **%** и порядковый номер переменной, %1, %2 и т.д. Путь и имя самого пакетного файла хранится в переменной %0. Таким образом можно получить только 9 параметров.

Чтобы получить доступ к большему количеству параметров можно использовать команду **SHIFT**, который сдвигает параметры влево, таким образом, что на месте первого оказывается второй, и т.д.

**Комментарии** задаются с помощью команды **rem** либо с помощью двух двоеточий



Если к имени команды добавить **@,** то текст самой команды не будет выводится в поток вывода (консоль или файл). Отключить вывод текста команд во всем файле можно командой **ECHO OFF.**

В командных файлах можно использовать команды условного перехода.

* **IF EXIST имя\_файла команда –** проверить, существует ли файл, и в зависимости от этого выполнить команду.
* **GOTO метка –** перейти к указанной метке. Метка начинается с двоеточия **:METKA**. Передав метку **:EOF**, можно перейти в конец файла.
* **CALL file.bat –** выполнить другой батник, затем продолжить выполнение текущего. Можно просто указать имя батника без CALL, но тогда не будет происходить возврата к вызывающему файлу.  
  Файл может вызывать и сам себя, вызывая зацикливание.Выйти из зацикливания можно Ctrl+Break.
* **PAUSE –** приостановить выполнение командного файла до нажатия любой клавиши.
* **SET name=value –** установить значение переменной окружения.

**СПЕЦИАЛЬНЫЕ УСТРОЙСТВА**

* **CON –** консоль. По умолчанию все стандартные потоки связаны с этим устройством.
* **NUL –** специальное нулевое устройство (чтобы вывод некуда не записывался)
* **PRN -** принтер

**ОТЛИЧИЯ start / cmd / call**

**Call –** обычно используется для вызова батника из батника. Он не создает новый процесс, и вызывающий батник будет ждать завершения вызываемого.

Call имеет так же синтаксис вызова метки, что помогает описывать аналоги функций в cmd. Exit /b – возврат из функции.

*@echo off*

*echo hochu kakat*

*call:func*

*echo pokakal*

*goto :eof*

*:func*

*echo kakayu*

*exit /b*

**start –** создает новый процесс, имеет несколько ключей для управления способом создания новой среды (окно, наследование переменных). При этом вызывающий файл не ждет завершения, и сразу переходит к следующей команде. Запущенный файл уже живет своей жизнью, выполняясь параллельно.

Start так же позволяет запускать оконные исполняемые файлы. При вызове start с неисполняемым файлом он будет открыт в связанном с типом файла приложении.

Если указан каталог, то он будет открыт в проводнике.

**Cmd –** запускает cmd.exe для выполнения указанной команды. Если вызов происходит из консоли, то используется имеющаяся, если нет – создается новая.

**Исполняемый файл** — набор инструкций, который заставляет компьютер выполнить определённую задачу. В отличие от текстового файла, который рассчитан на чтение человеком, исполняемый файл рассчитан на чтение (и выполнение) процессором. файл с расширением **exe, cmd, bat** и т.д.

Первая подгруппа - это бинарные файлы; они содержат в себе запись программы в виде специальных машинных кодов, которые, чаще всего, передаются непосредственно процессору. Такие файлы ещё сокращённо называют бинарниками. В противоположность им существуют исполняемые файлы, в которых программа записана в виде текста - то есть, в том самом виде, в каком с ней работал создавший её программист. Такие исполняемые файлы называют скриптами.