

# БИТВА ЗА ДОМЕН

PROTECT

DETECT

RESPOND

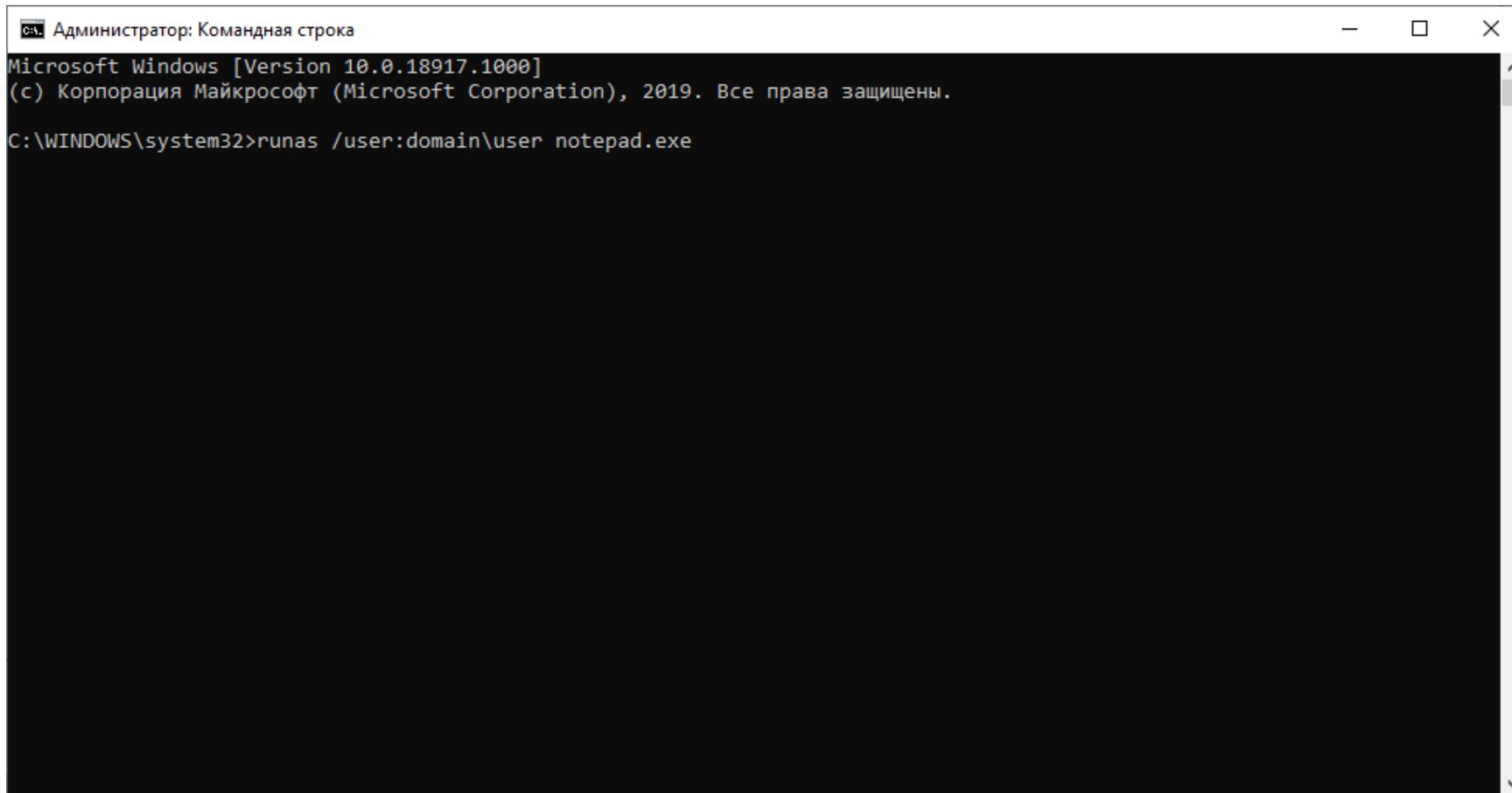


# Администрирование из командной строки

Дмитрий Узлов

Компания «ТЕХНОПОЛИС»

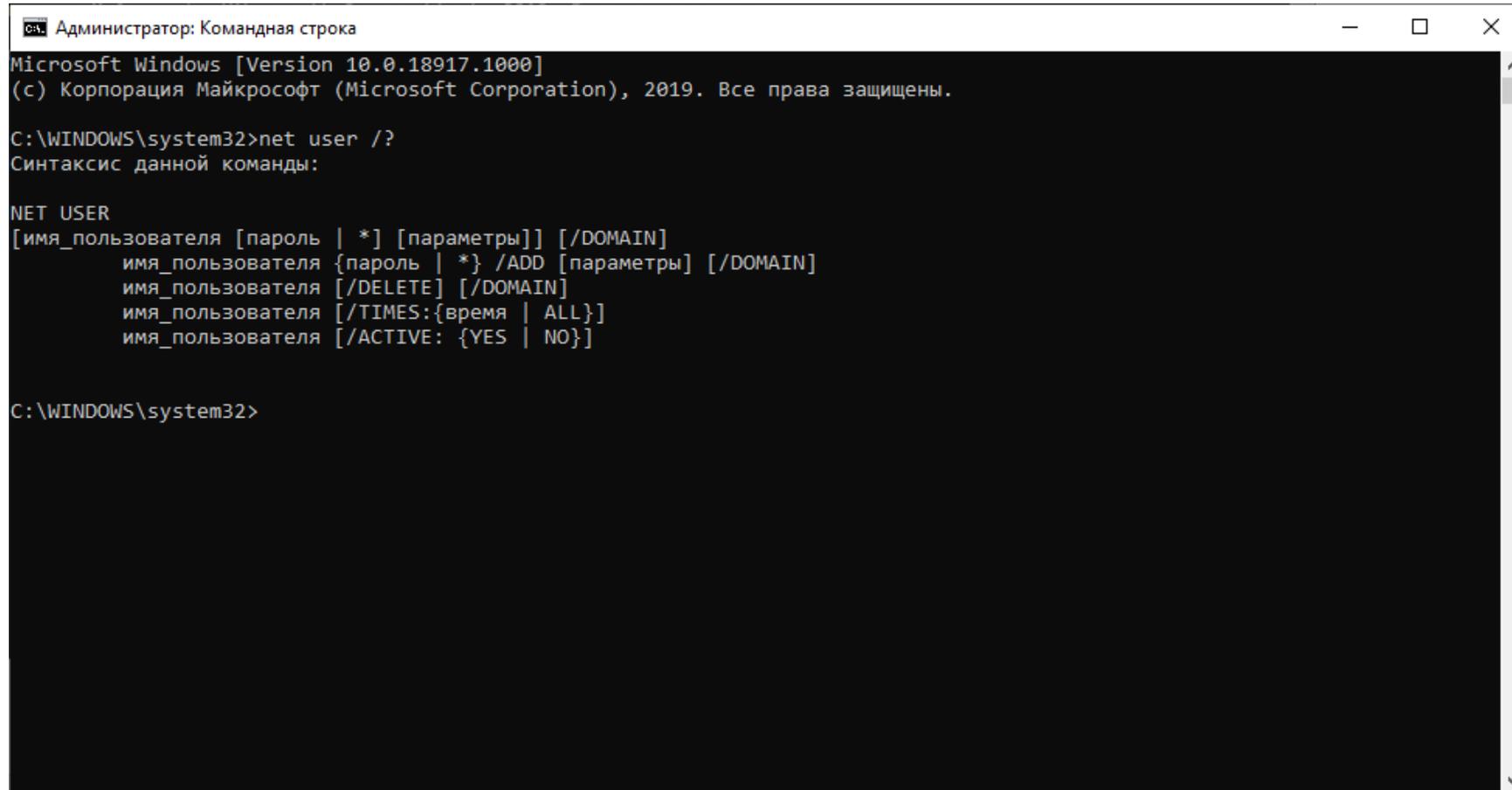
# Запуск от имени другого пользователя



```
Администратор: Командная строка
Microsoft Windows [Version 10.0.18917.1000]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\WINDOWS\system32>runas /user:domain\user notepad.exe
```

# Работа с учетными данными пользователей



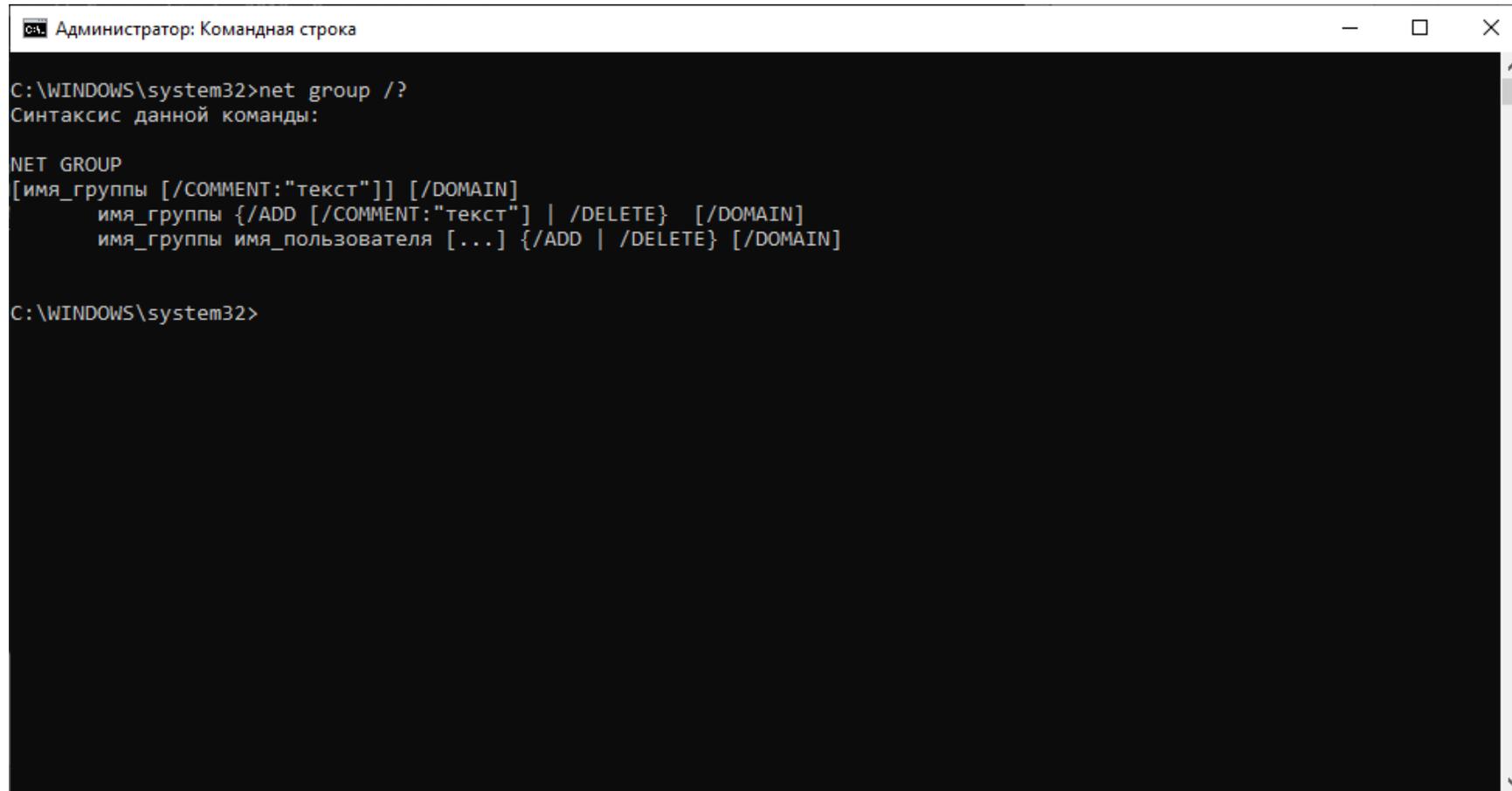
```
Администратор: Командная строка
Microsoft Windows [Version 10.0.18917.1000]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\WINDOWS\system32>net user /?
Синтаксис данной команды:

NET USER
[имя_пользователя [пароль | *] [параметры]] [/DOMAIN]
    имя_пользователя {пароль | *} /ADD [параметры] [/DOMAIN]
    имя_пользователя [/DELETE] [/DOMAIN]
    имя_пользователя [/TIMES:{время | ALL}]
    имя_пользователя [/ACTIVE: {YES | NO}]

C:\WINDOWS\system32>
```

# Работа с группами пользователей



```
Администратор: Командная строка

C:\WINDOWS\system32>net group /?
Синтаксис данной команды:

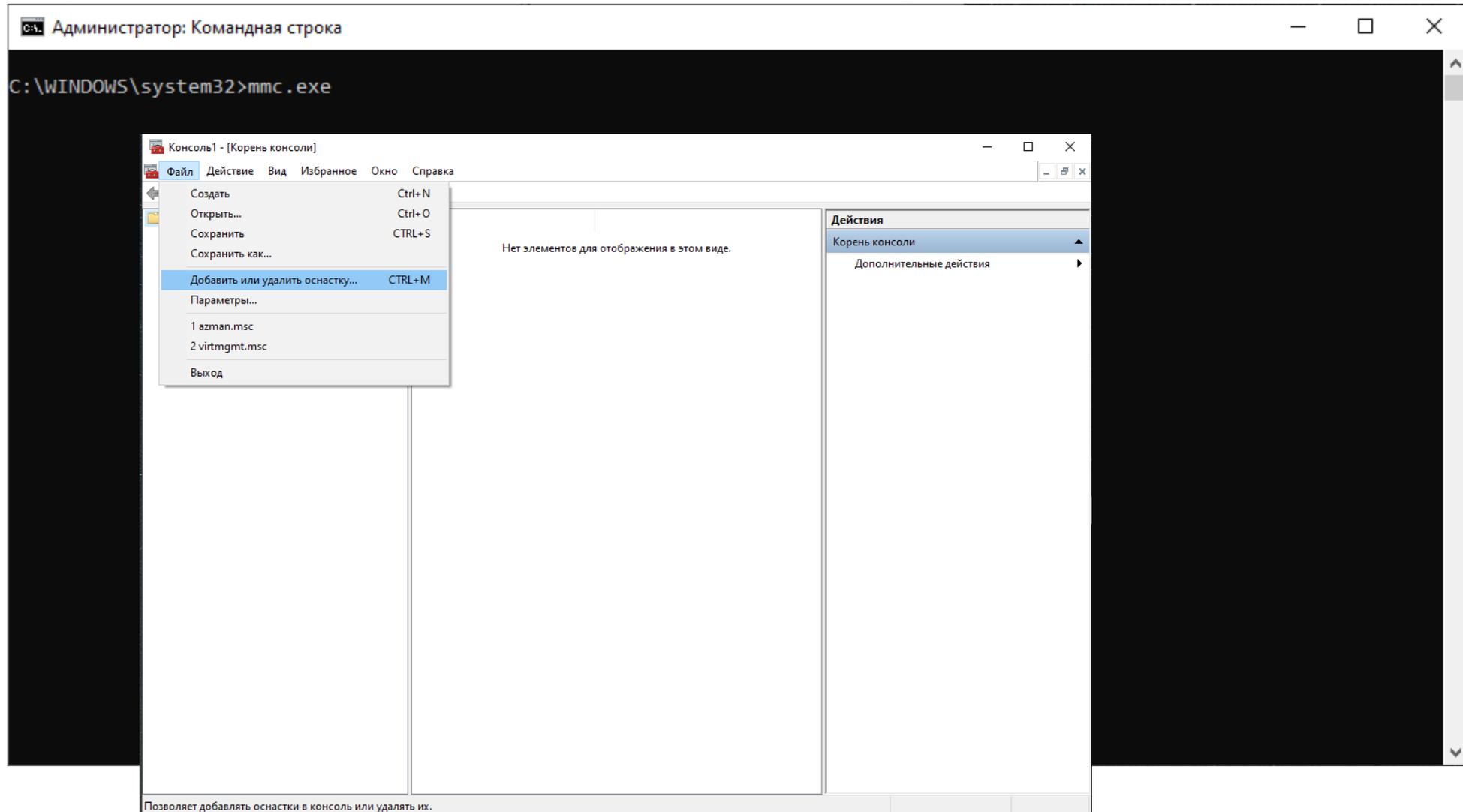
NET GROUP
[имя_группы [/COMMENT:"текст"]] [/DOMAIN]
    имя_группы {/ADD [/COMMENT:"текст"] | /DELETE} [/DOMAIN]
    имя_группы имя_пользователя [...] {/ADD | /DELETE} [/DOMAIN]

C:\WINDOWS\system32>
```

# Элементы панели управления

- Сетевые подключения: ncpa.cpl
- Свойства системы: sysdm.cpl
- Установка и удаление программ: appwiz.cpl
- Учетные записи пользователей: nusrmgr.cpl
- Дата и время: timedate.cpl
- Свойства экрана: desk.cpl
- Брандмауэр Windows: firewall.cpl
- Мастер установки оборудования: hdwwiz.cpl
- Свойства Интернет: inetcpl.cpl
- Специальные возможности: access.cpl
- Свойства мыши: control Main.cpl
- Свойства клавиатуры: control Main.cpl,@1
- Язык и региональные возможности: intl.cpl
- Игровые устройства: joy.cpl
- Свойства: Звуки и аудиоустройства: mmsys.cpl
- Мастер настройки сети: netsetup.cpl
- Управление электропитанием: powercfg.cpl
- Центр обеспечения безопасности: wscui.cpl
- Автоматическое обновление: wuaucpl.cpl
- control - Панель управления
- control admintools — Администрирование
- control desktop — Настройки экрана / Персонализация
- control folders — Свойства папок
- control fonts — Шрифты
- control keyboard — Свойства клавиатуры
- control mouse — Свойства мыши
- control printers — Устройства и принтеры
- control schedtasks — Планировщик заданий

# Запуск оснастки администрирования



# Популярные оснастки

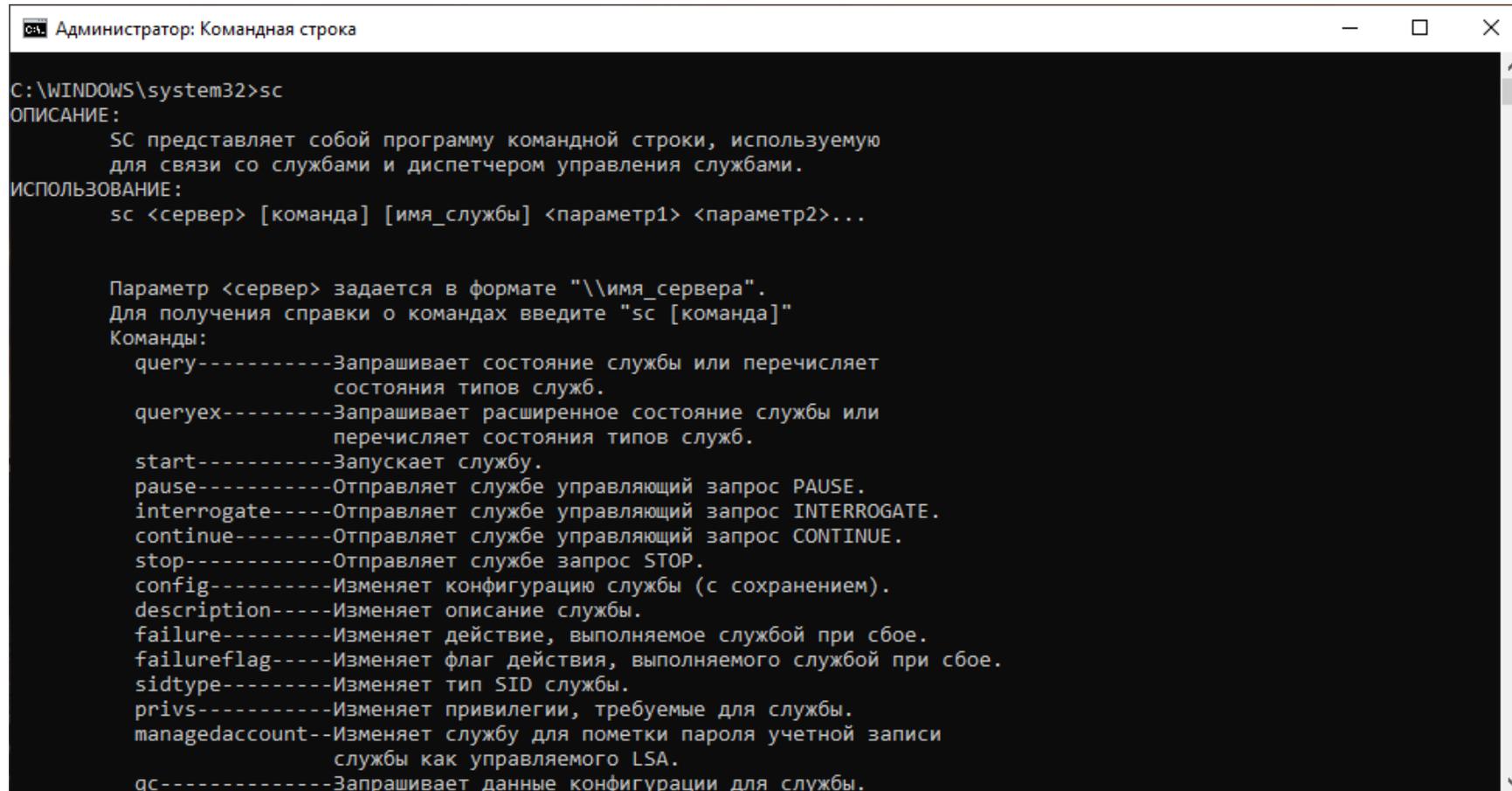
## Оснастки компьютера:

- Управление компьютером (Computer Management): compmgmt.msc
- Редактор объектов локальной политики (Group Policy Object Editor): gpedit.msc
- Результирующая политика (результат применения политик): rsop.msc
- Службы (Services): services.msc
- Общие папки (Shared Folders): fsmgmt.msc
- Диспетчер устройств (Device Manager): devmgmt.msc
- Локальные пользователи и группы (Local users and Groups): lusrmgr.msc
- Локальная политика безопасности (Local Security Settings): secpol.msc
- Управление дисками (Disk Management): diskmgmt.msc
- eventvwr.msc: Просмотр событий
- certmgr.msc: Сертификаты - текущий пользователь

## Серверные оснастки:

- Active Directory Пользователи и компьютеры (AD Users and Computers): dsa.msc
- Диспетчер служб терминалов (Terminal Services Manager): tsadmin.msc
- Консоль управления GPO (Group Policy Management Console): gpmc.msc
- Маршрутизация и удаленный доступ (Routing and Remote Access): rrasmgmt.msc
- Политика безопасности домена (Domain Security Settings): dompol.msc
- Политика безопасности контроллера домена (DC Security Settings): dcpol.msc
- Распределенная файловая система DFS (Distributed File System): dfsgui.msc

# Работа со службами

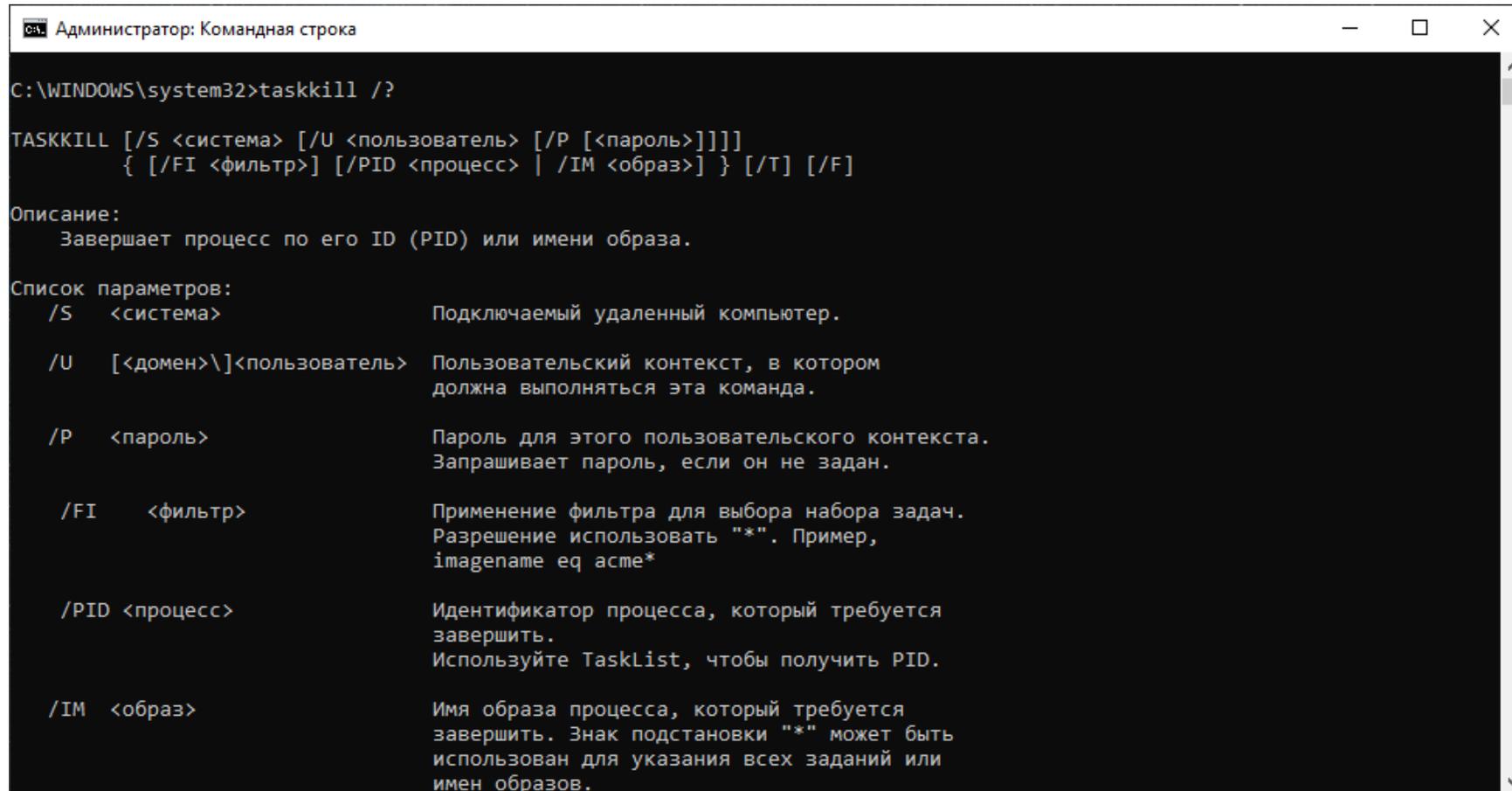


```
Администратор: Командная строка
C:\WINDOWS\system32>sc
ОПИСАНИЕ :
    SC представляет собой программу командной строки, используемую
    для связи со службами и диспетчером управления службами.
ИСПОЛЬЗОВАНИЕ :
    sc <сервер> [команда] [имя_службы] <параметр1> <параметр2>...

    Параметр <сервер> задается в формате "\\имя_сервера".
    Для получения справки о командах введите "sc [команда]"
Команды:
    query-----Запрашивает состояние службы или перечисляет
                  состояния типов служб.
    queryex-----Запрашивает расширенное состояние службы или
                  перечисляет состояния типов служб.
    start-----Запускает службу.
    pause-----Отправляет службе управляющий запрос PAUSE.
    interrogate----Отправляет службе управляющий запрос INTERROGATE.
    continue-----Отправляет службе управляющий запрос CONTINUE.
    stop-----Отправляет службе запрос STOP.
    config-----Изменяет конфигурацию службы (с сохранением).
    description----Изменяет описание службы.
    failure-----Изменяет действие, выполняемое службой при сбое.
    failureflag----Изменяет флаг действия, выполняемого службой при сбое.
    sidtype-----Изменяет тип SID службы.
    privs-----Изменяет привилегии, требуемые для службы.
    managedaccount--Изменяет службу для пометки пароля учетной записи
                  службы как управляемого LSA.
    qc-----Запрашивает данные конфигурации для службы.
```



# Работа с процессами



```
Администратор: Командная строка

C:\WINDOWS\system32>taskkill /?

TASKKILL [/S <система> [/U <пользователь> [/P [<пароль>]]]]
        { [/FI <фильтр>] [/PID <процесс> | /IM <образ>] } [/T] [/F]

Описание:
    Завершает процесс по его ID (PID) или имени образа.

Список параметров:
    /S    <система>          Подключаемый удаленный компьютер.

    /U    [<домен>\]<пользователь> Пользовательский контекст, в котором
        должна выполняться эта команда.

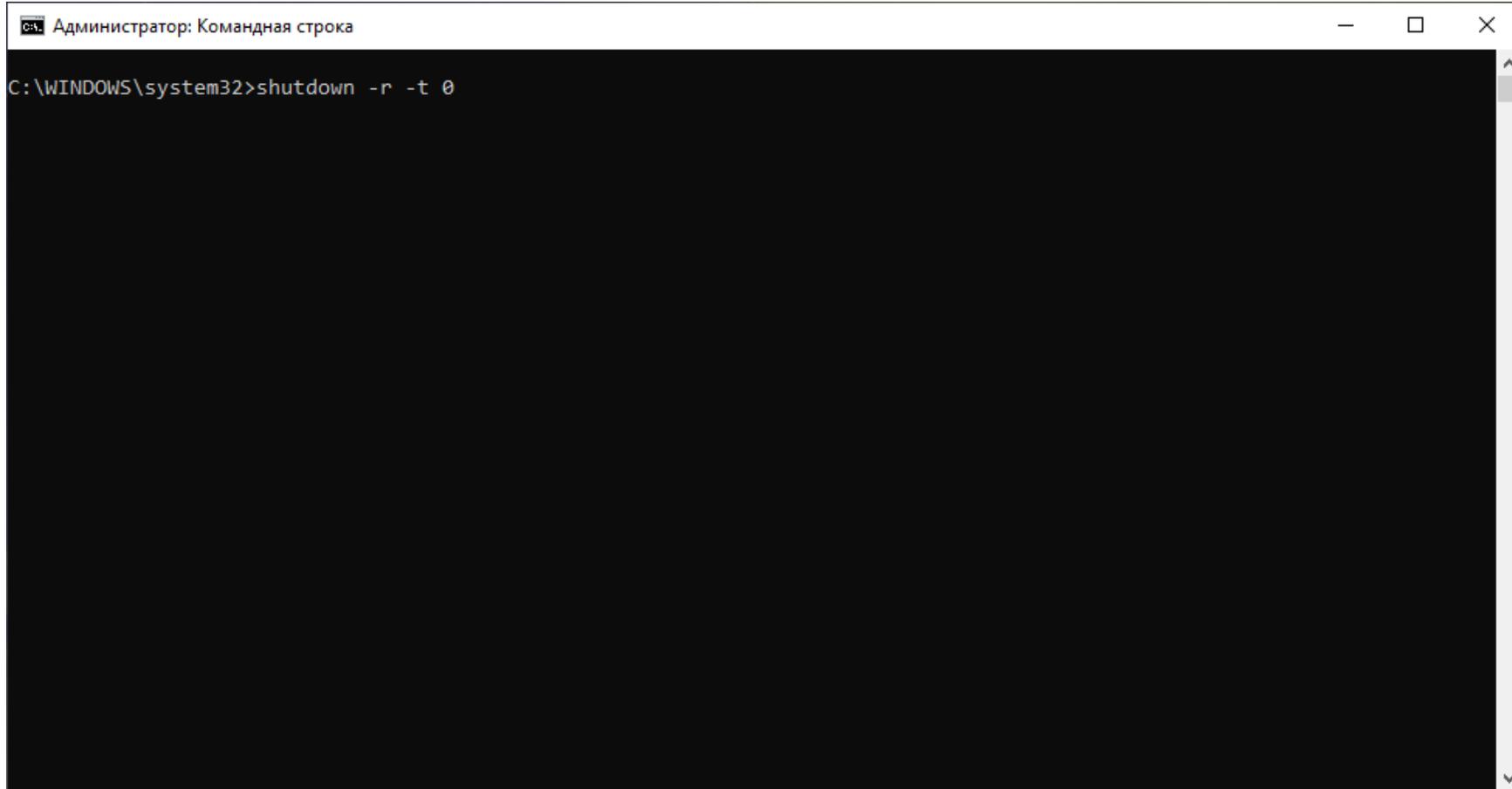
    /P    <пароль>          Пароль для этого пользовательского контекста.
        Запрашивает пароль, если он не задан.

    /FI    <фильтр>        Применение фильтра для выбора набора задач.
        Разрешение использовать "*". Пример,
        imagename eq асме*

    /PID  <процесс>        Идентификатор процесса, который требуется
        завершить.
        Используйте TaskList, чтобы получить PID.

    /IM   <образ>          Имя образа процесса, который требуется
        завершить. Знак подстановки "*" может быть
        использован для указания всех заданий или
        имен образов.
```

# Перезагрузка компьютера

A screenshot of a Windows command prompt window. The title bar at the top reads "Администратор: Командная строка" (Administrator: Command Prompt). The window contains the command `C:\WINDOWS\system32>shutdown -r -t 0` entered at the prompt. The rest of the window is black, indicating the command has been executed.

```
Администратор: Командная строка
C:\WINDOWS\system32>shutdown -r -t 0
```