«Министерство образования и науки Российской Федерации Федеральное государственное бюджетное образовательное учреждение высшего образования «Алтайский государственный технический университет им. И.И. Ползунова»

Факультет информационных технологий

Кафедра прикладной математики

Отчёт защищён с оценкой\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Преподаватель Ненайденко А.С.

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2021 г.

Отчёт

Лабораторной работе №3

«Управление и мониторинг процессов и потоков в ОС Windows»

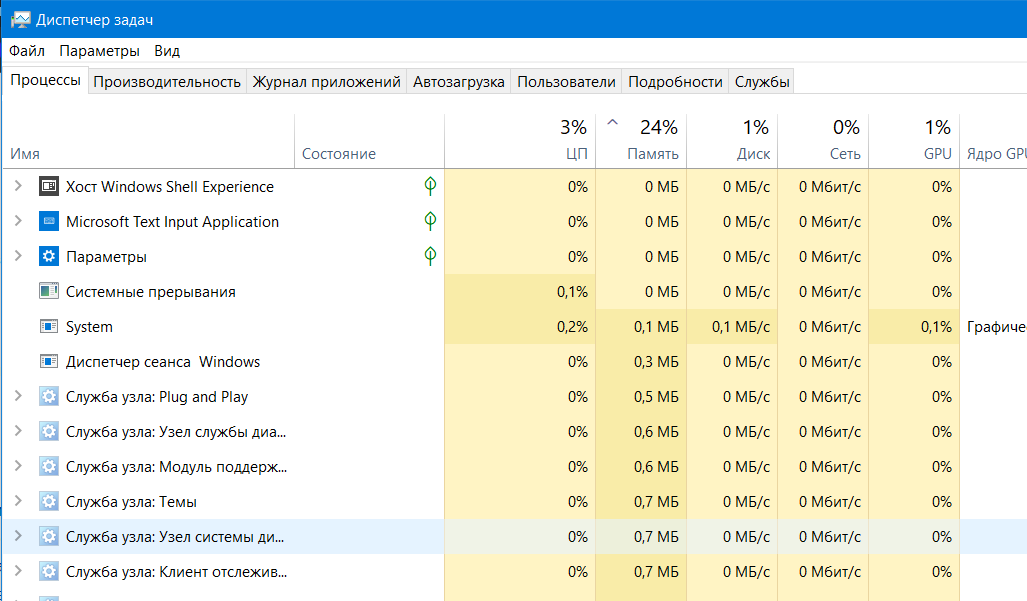
Студент группы ПИ 92 В.М. Шульпов

Преподаватель доцент, к.т. н. Ненайденко А.С.

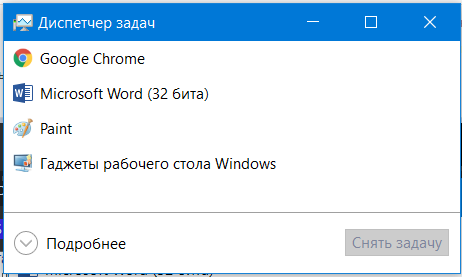
Барнаул 2021

**Цель:** изучить и разобраться с функционированием инструментов управления и мониторинга процессами и потоками в ОС Windows.

1. **Используя стандартные графические инструменты ОС;**

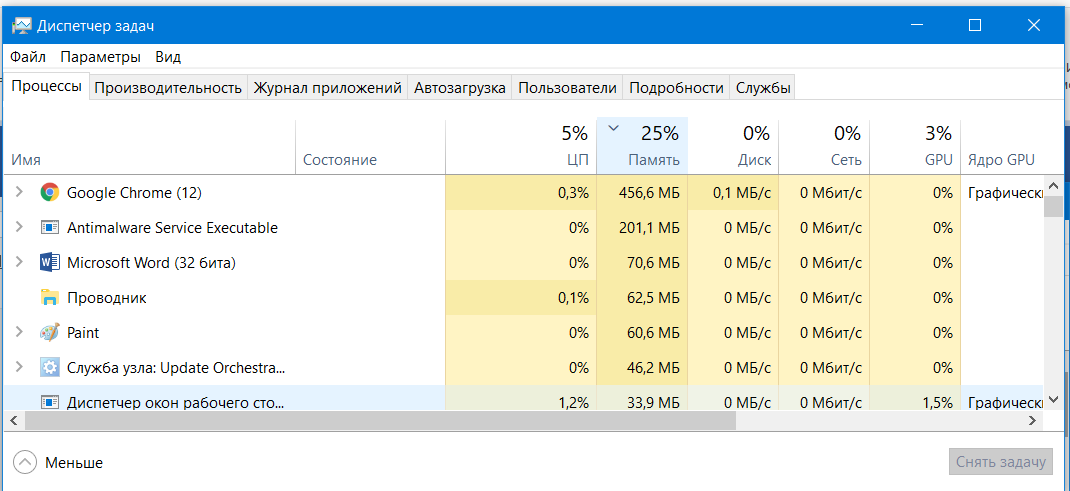
Основной графический инструмент для управления и мониторинга процессами и потоками в ОС Windows – это диспетчер задач.

По умолчанию, в диспетчере задач отображаются только те приложения и настольные программы, которые созданы текущим пользователем. С возможностью завершить не отвечающую задачу.

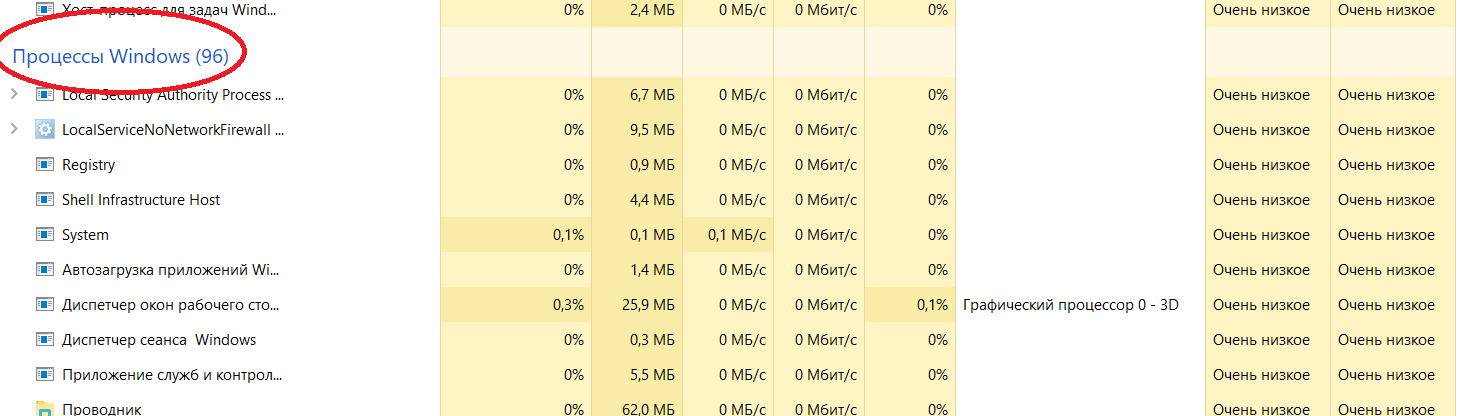
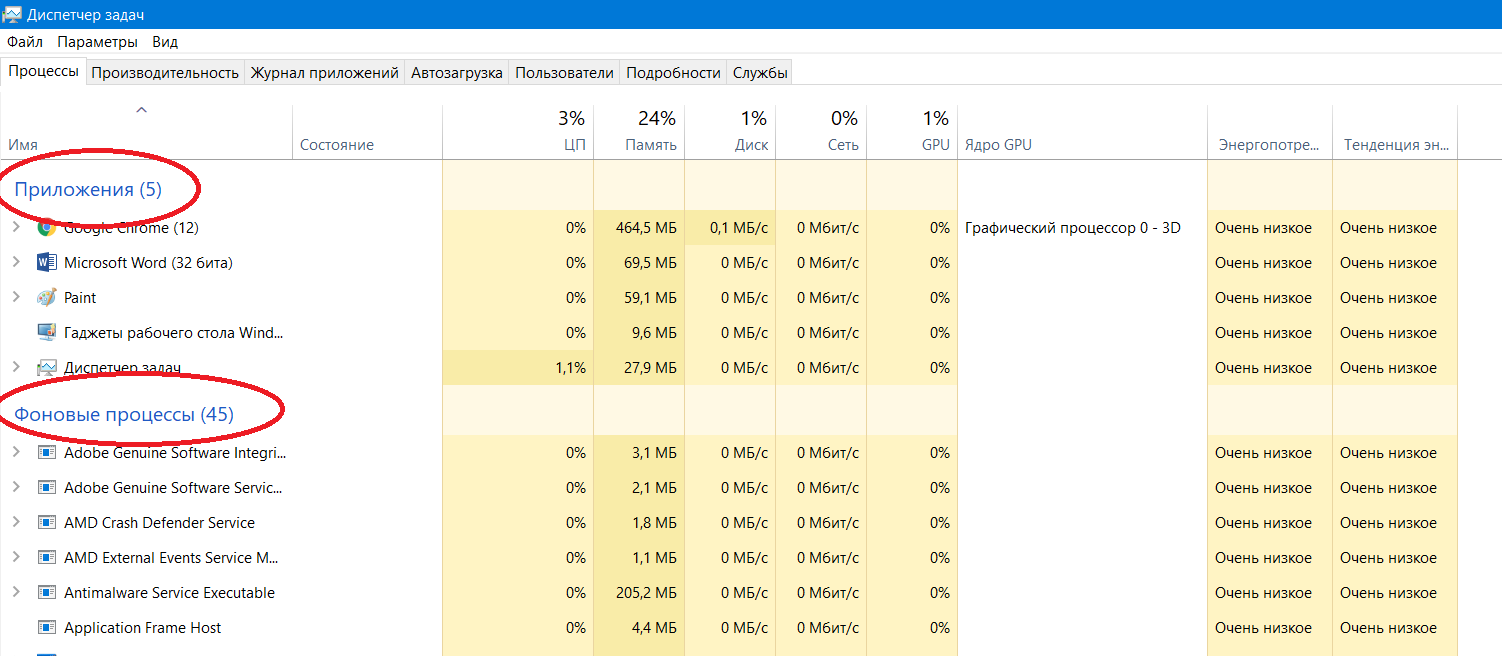


|  |
| --- |
| **Что это? Как открыть?** |
| **Диспетчер задач** **Windows** — [диспетчер задач](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BF%D0%B5%D1%82%D1%87%D0%B5%D1%80_%D0%B7%D0%B0%D0%B4%D0%B0%D1%87), системный монитор и менеджер запуска, входящий в состав [Windows](https://ru.wikipedia.org/wiki/Windows" \o "Windows). Он предоставляет информацию о производительности компьютера и запущенных приложениях, процессах и использовании [ЦП](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BD%D1%82%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D1%80), фиксирует нагрузку и сведения о памяти, сетевой активности и статистике, зарегистрированных пользователях и системных службах. Диспетчер задач также может использоваться для установки приоритетов процессов, свойства процессора, запуска и остановки служб и принудительного завершения процессов.  Диспетчер задач можно запустить либо комбинацией ⊞ Win+R и введя taskmgr.exe, либо комбинацией Ctrl+Alt+Delete и нажав «Запустить диспетчер задач», либо комбинацией Ctrl+⇧ Shift+Esc, либо щелкнув правой кнопкой мыши на панели задач Windows и выбрав пункт «Диспетчер задач». |

Нажатие на опцию "Подробнее" разворачивает диспетчер задач в гораздо более интересный монитор, с семи вкладками. Как показывает рисунок, вкладка "Процессы" отображает тот же набор процессов, как и вид по умолчанию (к которому вы можете вернуться, нажав "Меньше"). Но, в добавок к этому, здесь имеются сведения о дочерних окнах, а также четыре колонки информации об использовании системных ресурсов. Эти колонки, в заголовках столбцов, отображают общее использование системных ресурсов микропроцессора, памяти, диска и сети. Детали, справа от каждого процесса, показывает соответствующую активность для этого процесса.

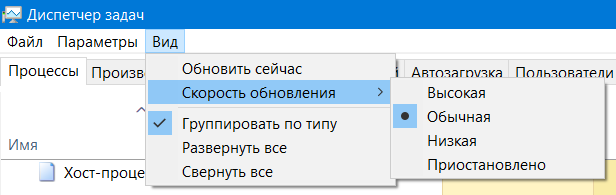


А также, вы найдёте дополнительную информацию о запущенных процессах. Вместо отображения только настольных программ и приложений, список расширен на три группы: приложения, фоновые процессы и процессы Windows.

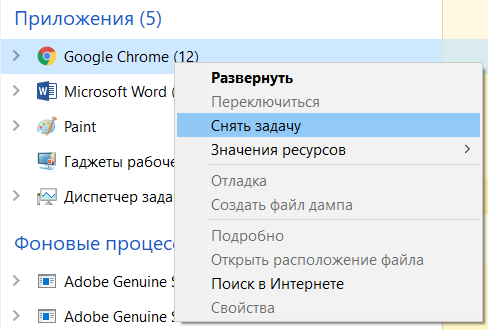


Нажмите вид > скорость обновления, чтобы выбрать более быструю (High) или медленную (Low) скорость опроса использования системных ресурсов. Нажмите кнопку "Приостановлено" и временно заморозьте значения так, чтобы их можно было исследовать, не испытывая резких изменений. Нажмите кнопку "Обновить сейчас", чтобы обновить приостановленный мониторинг и увидеть текущие значения.

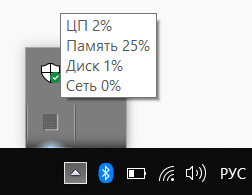
В меню "Вид", снимите флажок "Группировать по типу", чтобы увидеть алфавитный список процессов, без трёх групп.



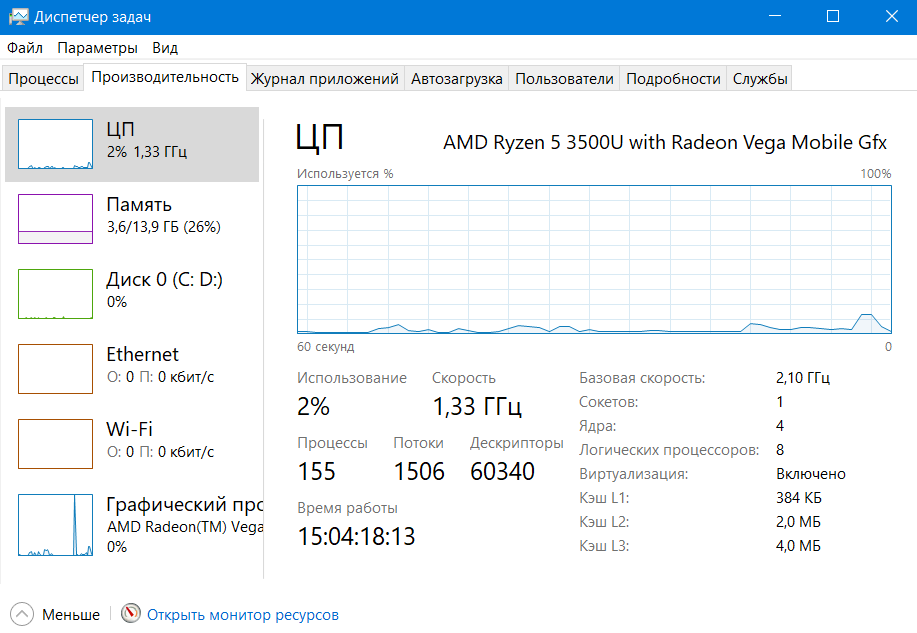
Выберите любой пункт в списке и нажмите кнопку "Завершить задачу", чтобы принудительно остановить этот процесс. Это эффективное действие для завершения не реагирующих на команды приложений (конечно с неизбежным риском потери не сохраненных данных). (Не каждый процесс можно завершить таким образом).



Наведя курсор на иконку в области уведомлений, можно просмотреть общие сведения об использования системных ресурсов.

****

Во вкладке «производительность» можно оценить, сколько памяти используется в данный момент, на сколько процентов загружен процессор, узнать текущее

количество процессов/потоков и другое****

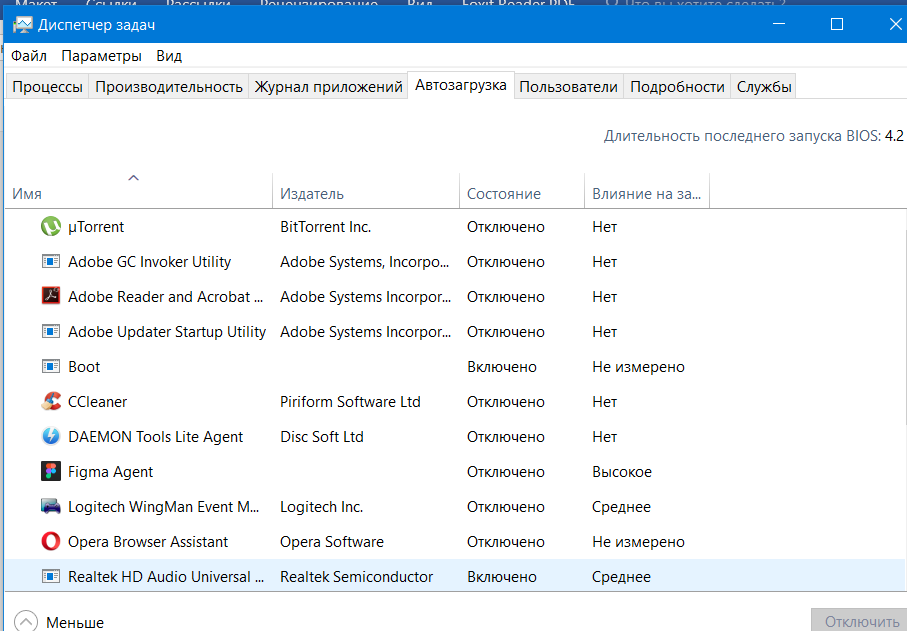
•**Загрузка ЦП (CPU Usage)**Нa сколько процентов в данный момент используются ресурсы процессора.

**• Хронология загрузки ЦП (CPU Usage History)** История использования процессора. Частоту обновления диаграммы можно изменить.

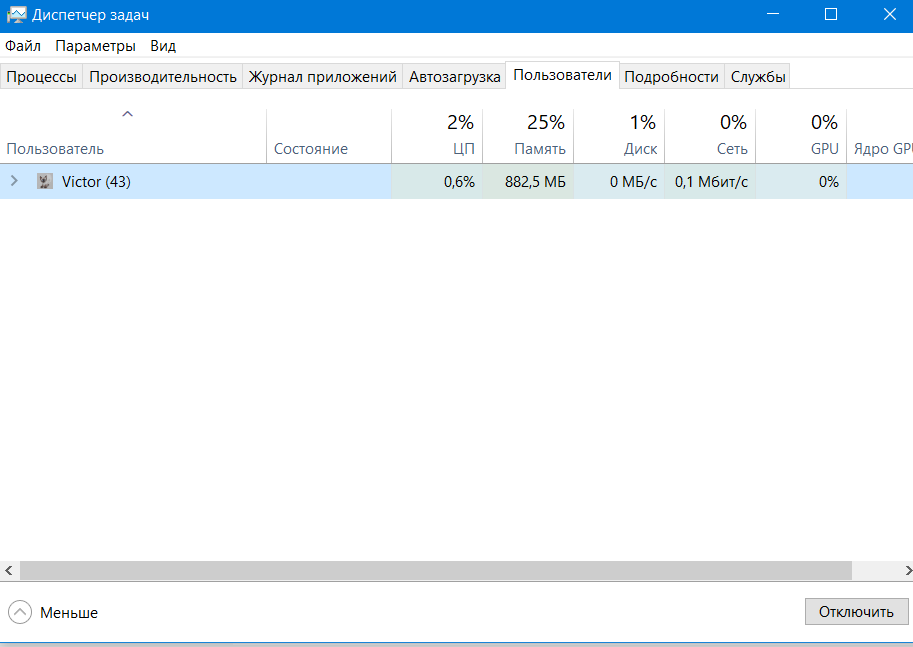
**• Память (Memory)** Объем физической памяти, используемый системой в данный момент.

**• Хронология использования физической памяти (Physical Memory Usage History)**История использования памяти.

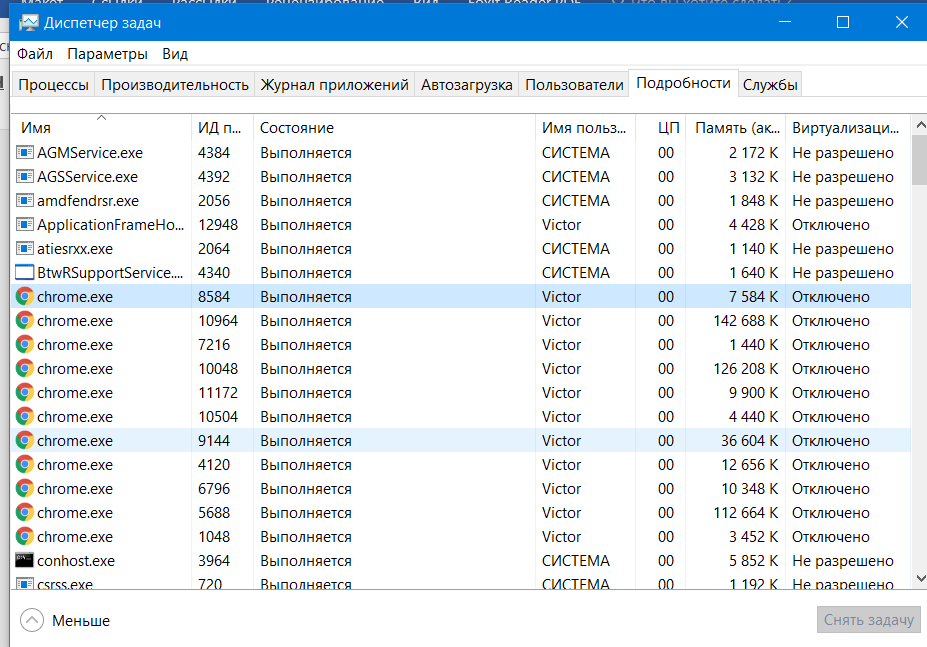
В автозагрузке можно отключить приложения, которые запускаются при запуске системы



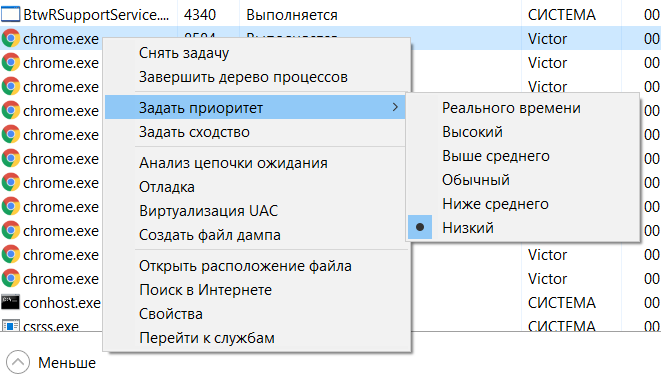
При наличии только одного пользователя раздел пользователи является излишним. Здесь можно развернуть вкладку и увидеть то же самое, что и во вкладке процессы для конкретного пользователя.а



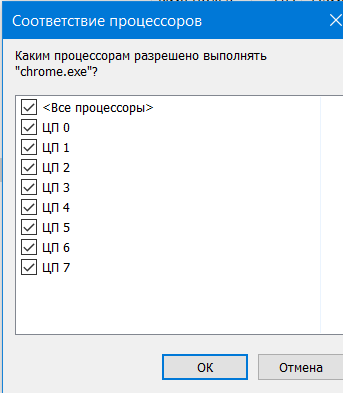
Во вкладке подробности имеется больший функционал для управлением процессов



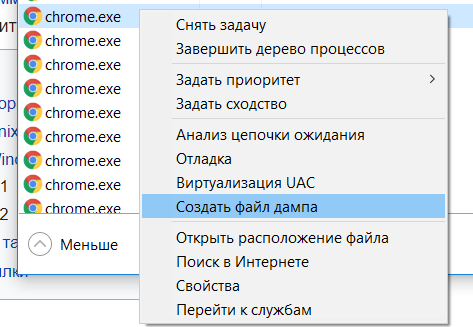
Можно задать приоритет процессу



Можно разрешить процессу выполняться только на определенных виртуальных процессах (потоках)

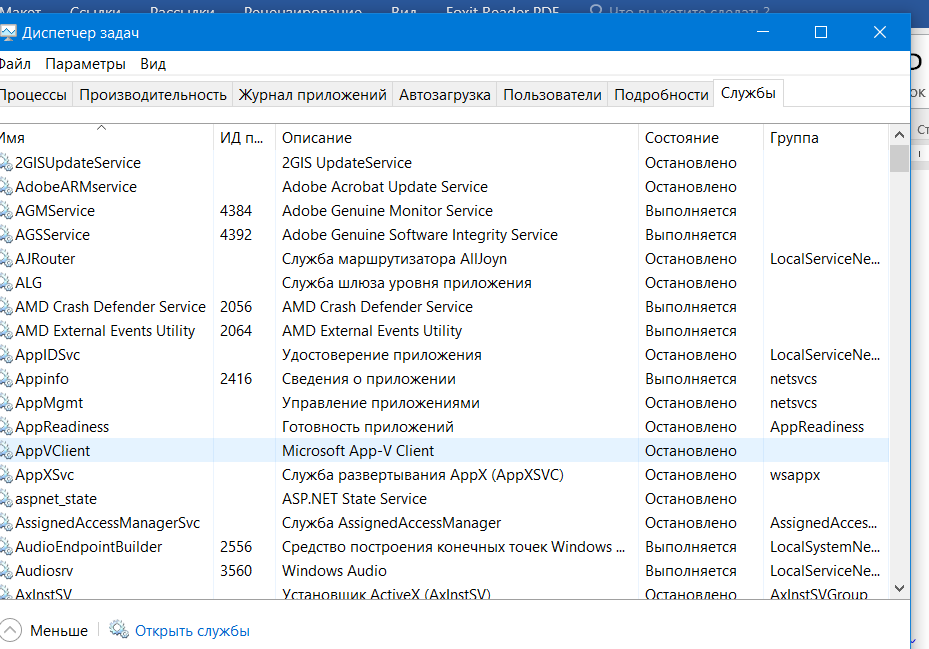


Создать файл дампа



**Дамп памяти** ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *memory dump*; в [Unix](https://ru.wikipedia.org/wiki/Unix" \o "Unix) — *core dump*) — содержимое рабочей памяти одного [процесса](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81_(%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), [ядра](https://ru.wikipedia.org/wiki/%D0%AF%D0%B4%D1%80%D0%BE_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B) или всей [операционной системы](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0). Также может включать дополнительную информацию о состоянии программы или системы, например значения [регистров процессора](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B3%D0%B8%D1%81%D1%82%D1%80_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D1%80%D0%B0) и содержимое [стека](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%BA). Многие операционные системы позволяют сохранять дамп памяти для [отладки программы](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BB%D0%B0%D0%B4%D0%BA%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D1%8B). Как правило, дамп памяти процесса сохраняется автоматически, когда процесс завершается из-за критической ошибки (например, из-за [ошибки сегментации](https://ru.wikipedia.org/wiki/%D0%9E%D1%88%D0%B8%D0%B1%D0%BA%D0%B0_%D1%81%D0%B5%D0%B3%D0%BC%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D0%B8%D0%B8)). Дамп также можно сохранить вручную через [отладчик](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BB%D0%B0%D0%B4%D1%87%D0%B8%D0%BA) или любую другую специальную программу.

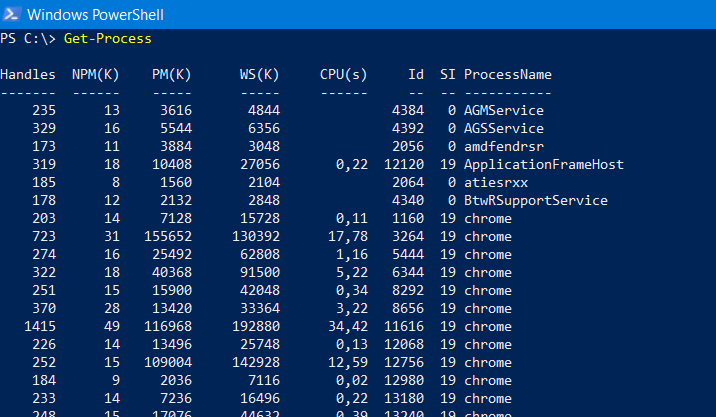
Службы:



На вкладке **Службы (Services)** диспетчера задач перечислены системные службы. Для каждой службы приводится имя, идентификатор процесса (РШ), описание, состояние и группа. Обычно несколько служб работают с одним и тем же идентификатором процесса.

1. **Используя интерфейс командной строки PowerShell;**

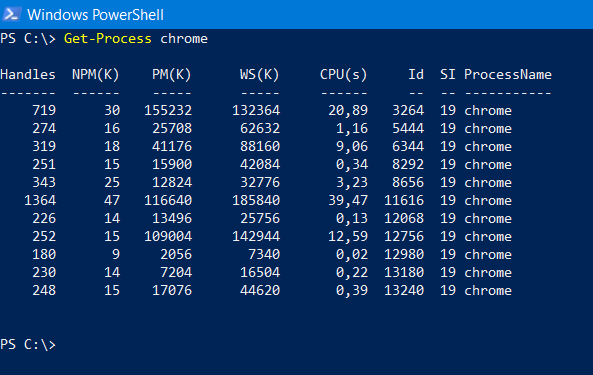
**Управление процессами с помощью PowerShell**

* Get-Process – получить список запущенных **процессов**;

По-умолчанию выводятся следующие свойства запущенных процессов:

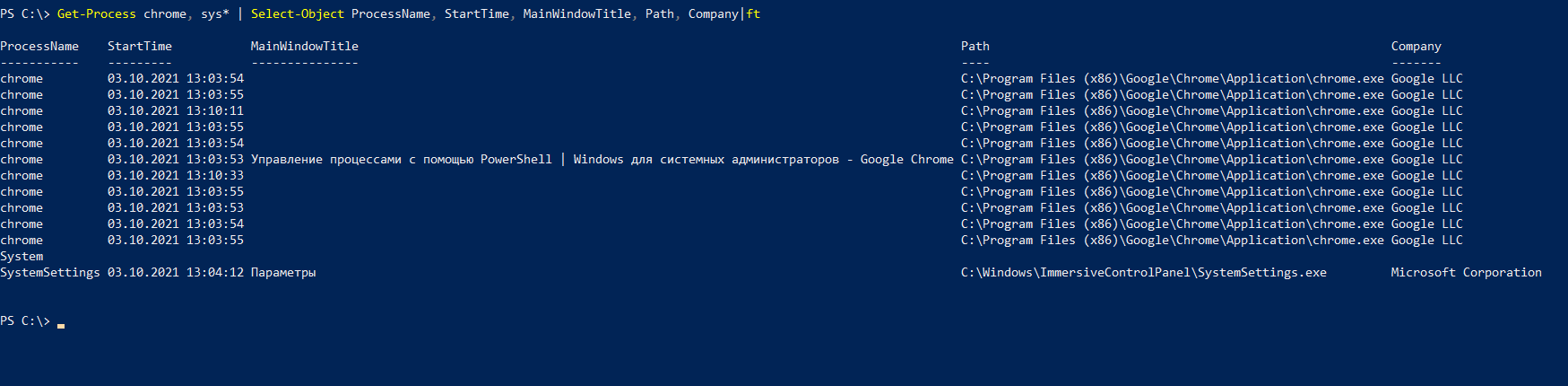
* + **Handles** – количество [дескрипторов](https://winitpro.ru/index.php/2020/08/20/fajl-zablokirovan-processom-windows-snyat-blokirovku/) ввода — вывода, которые отрыл данный процесс;
  + **NPM(K)** — Non-paged memory ([невыгружаемый пул](https://winitpro.ru/index.php/2017/12/06/high-non-paged-pool-windows/)). Размер данных процесса (в Кб.), которые никогда не попадают в файл подкачки на диск;
  + **PM(K)**– размер памяти процесса, которая может быть выгружена на диск;
  + **WS(K)** – размер физической памяти в Кб, используемой процессом (working set).
  + **CPU(s)**– процессорное время, использованное процессом (учитывается время на всех CPU);
  + **ID** — идентификатор процесса;
  + **SI** (Session ID) – идентификатор сеанса процесса (0 — запущен для всех сессий, 1 – для первого залогиненого пользователя, 2 — для второго и т.д.);
  + **ProcessName** – имя процесса.

**Можем получить конкретные процессы по ProcessName**



Можно вывести только определенный свойства процессов. Например, имя (ProcessName) время запуска (StartTime), заголовок окна процесса (MainWindowTitle), имя исполняемого файла (Path) и наименование разработчика (Company):

Get-Process chrome, sys\* | Select-Object ProcessName, StartTime, MainWindowTitle, Path, Company|ft



знак звездочки **\***, означает любое количество символов, а знак вопросительного знака **?**, один любой символ.

**Все параметры процесса winword**



Name : WINWORD

Id : 12648

PriorityClass : Normal

FileVersion : 16.0.4266.1001

HandleCount : 1290

WorkingSet : 173924352

PagedMemorySize : 152334336

PrivateMemorySize : 152334336

VirtualMemorySize : 765857792

TotalProcessorTime : 00:01:16.7343750

SI : 19

Handles : 1290

VM : 765857792

WS : 173924352

PM : 152334336

NPM : 75880

Path : C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Company : Microsoft Corporation

CPU : 76,734375

ProductVersion : 16.0.4266.1001

Description : Microsoft Word

Product : Microsoft Office 2016

\_\_NounName : Process

BasePriority : 8

ExitCode :

HasExited : False

ExitTime :

Handle : 2496

SafeHandle : Microsoft.Win32.SafeHandles.SafeProcessHandle

MachineName : .

MainWindowHandle : 66146

MainWindowTitle : OS\_lab3.docx - Word

MainModule : System.Diagnostics.ProcessModule (WINWORD.EXE)

MaxWorkingSet : 1413120

MinWorkingSet : 204800

Modules : {System.Diagnostics.ProcessModule (WINWORD.EXE), System.Diagnostics.ProcessModule (ntdll.dll), System.Diagnostics.ProcessModule (wow64.dll), System.Diagnostics.ProcessModule (wow64win.dll)...}

NonpagedSystemMemorySize : 75880

NonpagedSystemMemorySize64 : 75880

PagedMemorySize64 : 152334336

PagedSystemMemorySize : 1095248

PagedSystemMemorySize64 : 1095248

PeakPagedMemorySize : 160047104

PeakPagedMemorySize64 : 160047104

PeakWorkingSet : 199688192

PeakWorkingSet64 : 199688192

PeakVirtualMemorySize : 783884288

PeakVirtualMemorySize64 : 783884288

PriorityBoostEnabled : True

PrivateMemorySize64 : 152334336

PrivilegedProcessorTime : 00:00:17.8750000

ProcessName : WINWORD

ProcessorAffinity : 255

Responding : True

SessionId : 19

StartInfo : System.Diagnostics.ProcessStartInfo

StartTime : 03.10.2021 13:03:49

SynchronizingObject :

Threads : {1168, 1572, 9784, 4896...}

UserProcessorTime : 00:00:58.8593750

VirtualMemorySize64 : 765857792

EnableRaisingEvents : False

StandardInput :

StandardOutput :

StandardError :

WorkingSet64 : 173924352

Site :

Container :

**Описание основных:**

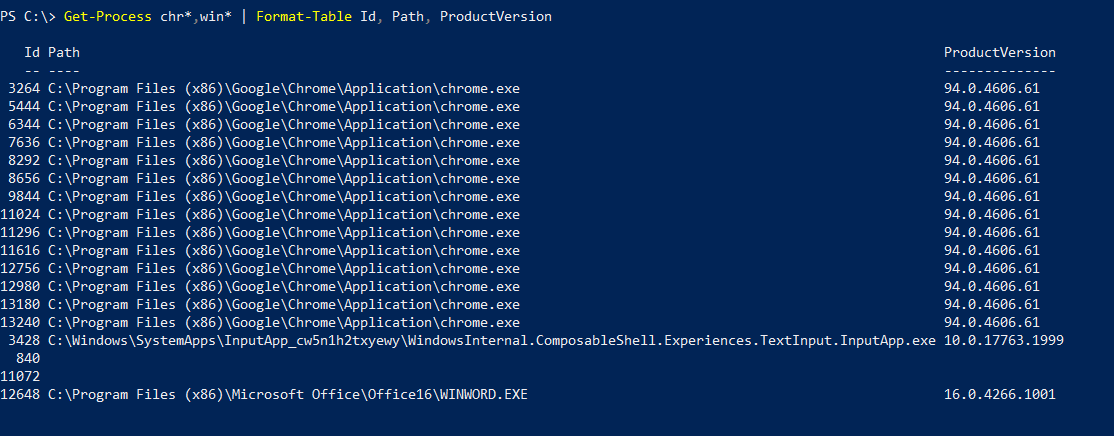
Количество дескрипторов процесса (**Handles**), Объем невыгружаемой памяти процесса (**NPM** - ***N****on****p****aged System****M****emory*), Объем памяти процесса возможный для записи в файл подкачки (**PM** - ***P****aged System****M****emory*), Объем памяти процесса выделенный в оперативной памяти (**WS** - ***W****orking****S****et*), Использованное процессорное время (**CPU**), Имя процесса (**ProcessName**).

**Path** - Путь до исполняемого файла процесса.  
**Description** - Описание исполняемого файла.  
**MainWindowTitle** - Заголовок главного окна процесса, если окно конечно есть.  
**Modules** - Модули используемые процессом.  
**MainModule** - Главный модуль процесса.  
**StartTime** - Время запуска процесса.  
**Priority** - Приоритет процесса.  
**Company** - Компания создавшая исполняемый файл процесса.  
**ProductVersion** - Версия исполняемого файла процесса.  
**UserProcessorTime** - То же что и **CPU** (использованное процессорное время), но только в более удобном формате.

# **Вывод указанных полей в виде таблицы**

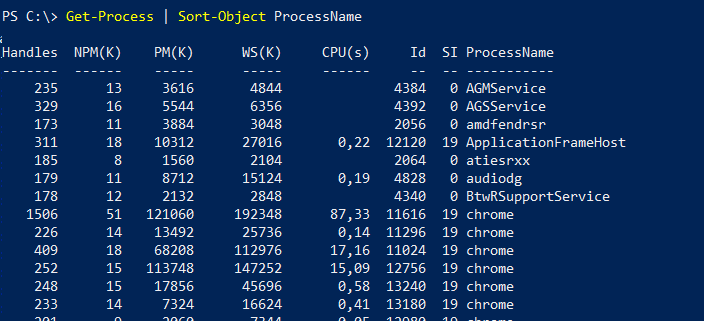
Get-Process chr\*,win\* | Format-Table Id, Path, ProductVersion

(результат как у select-object <выбранные параметры>)



Выполнить сортировку вывода командлета **Get-Process** можно передав его вывод по конвейеру командлету **Sort-Object**. К примеру, сортировка по имени процесса, в алфавитном порядке.

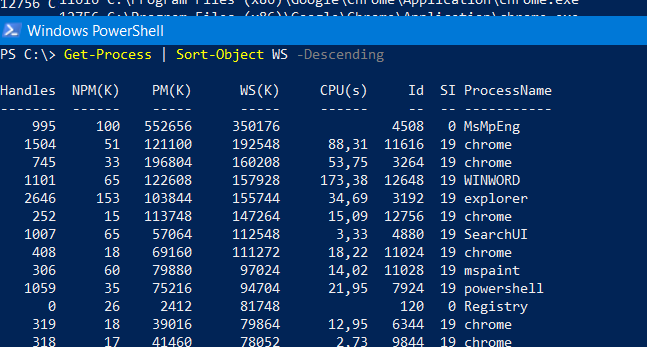
Get-Process | Sort-Object ProcessName



**Выполнение сортировки по используемой оперативной памяти**

Get-Process | Sort-Object WS –Descending

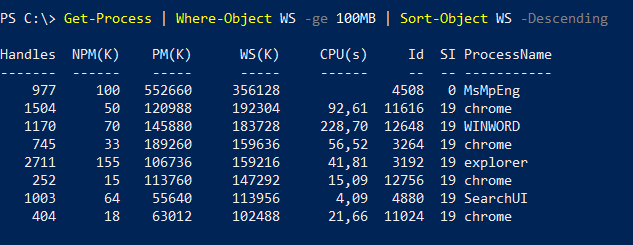
(флаг «-Descending» – в обратном порядке)



**Вывод процессов, объем выделенной памяти для которых больше или равен 100 МБ**

Get-Process | Where-Object WS -ge 100MB

Существуют и другие параметры сравнения: **-gt** больше, **-lt** меньше, **-eq** равно, **-ge** больше/равно, **-le** меньше/равно. Подробнее все параметры сравнения, можно посмотреть в справке по командлету **Where-Object**.

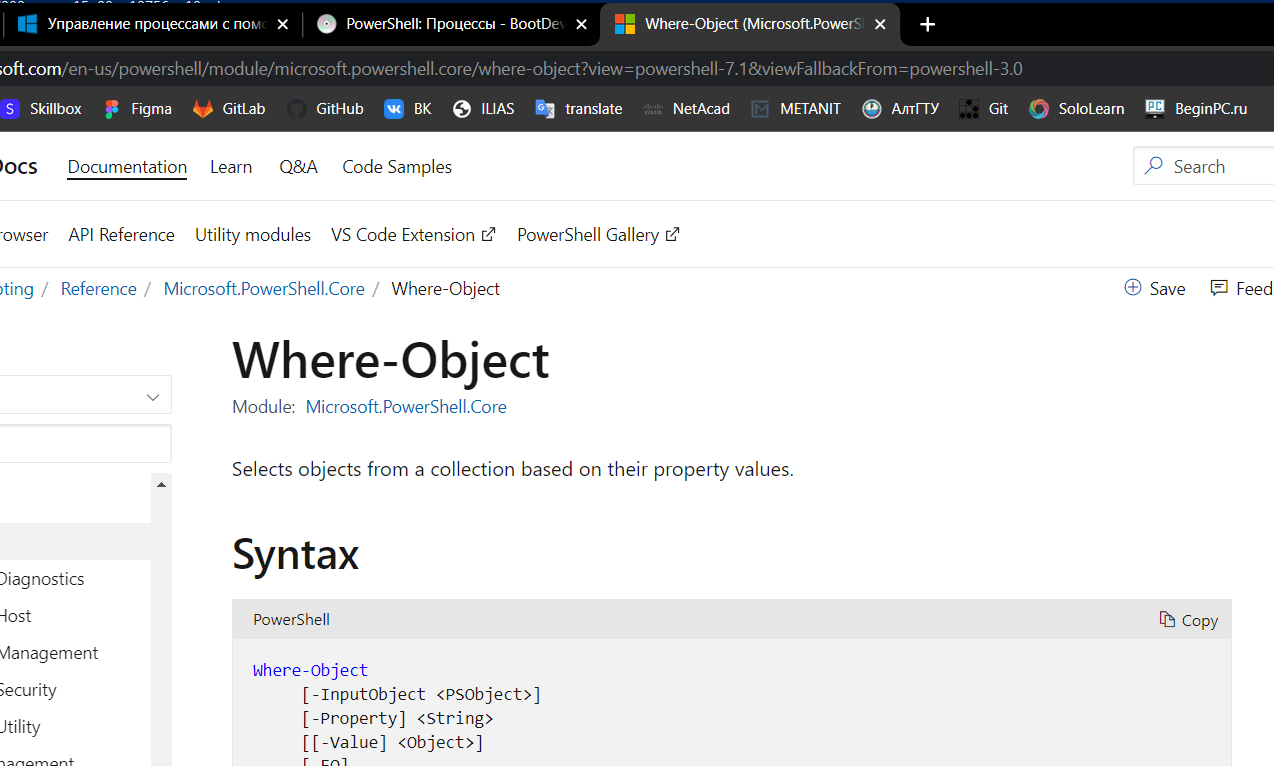


(условия, сортировки, выборки и т.д. можно объединять!)

**Вызов онлайн-справки по командлету Where-Object**

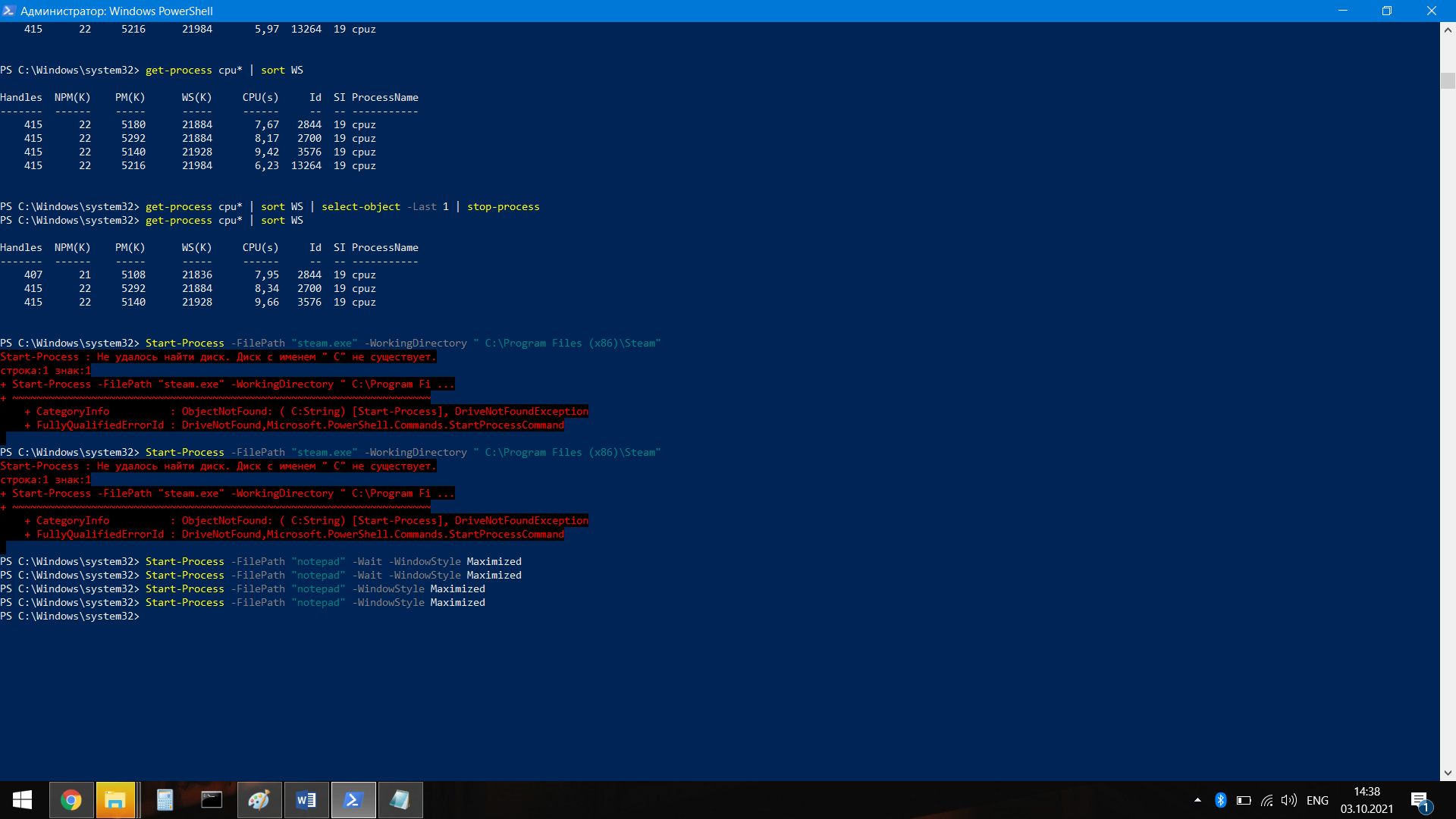
Get-Help Where-Object –online

(можно вызывать справку по любому командлету)



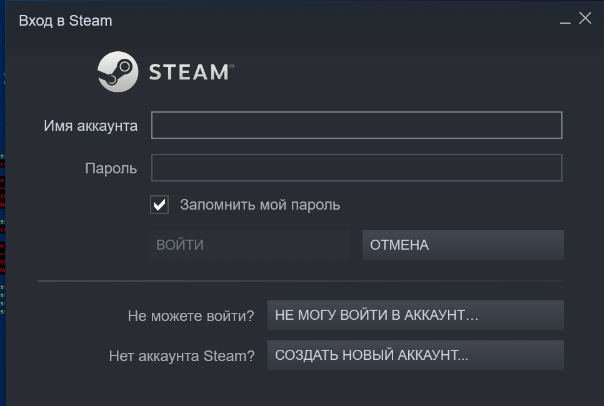
* **Start-Process – запустить процесс/программу;**

Start-Process -FilePath "notepad" -WindowStyle Maximized – открыть блокнот



Запустить процесс .exe из определенной папки

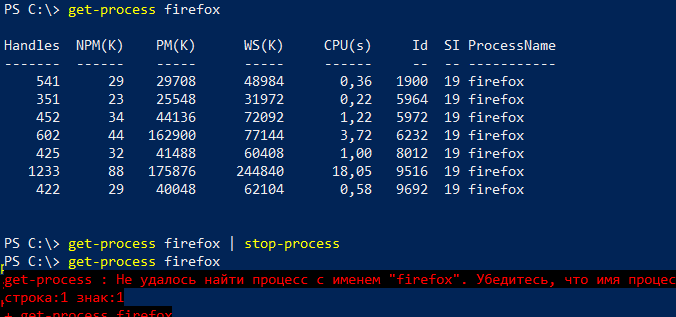




* **Stop-Process – принудительно остановить процесс;**

**# Закрыть все процессы "firefox"**

Get-Process firefox | Stop-Process



**Флаги для выборки:**

Select-Object

[-InputObject <PSObject>]

[-Property] <Object[]>]

[-ExcludeProperty <String[]>]

[-ExpandProperty <String>]

[-Unique]

[-Last <Int32>] – ВЫБОР НЕСКОЛЬКИХ ПЕРВЫХ ИЗ СПИСКА

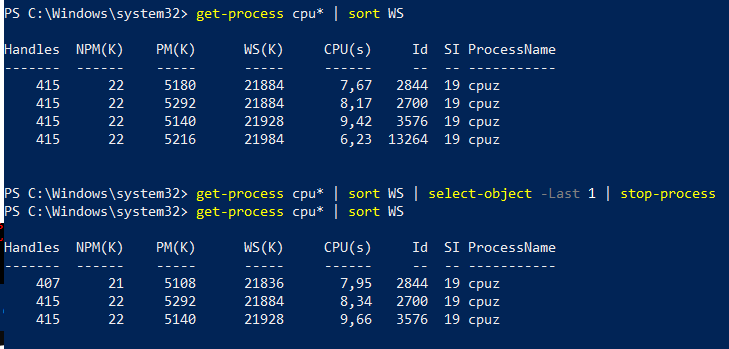
[-First <Int32>] – ВЫБОР НЕСКОЛЬКИХ ПОСЛЕДНИХ ИЗ СПИСКА

[-Skip <Int32>]

[-Wait]

[<CommonParameters>]

**# Закрыть самый большой по потреблению ОП процесс"cpuid"**

get-process cpu\* | sort WS | select-object -Last 1 | stop-process

* **Debug-Process – используется для отладки процессов;**

Отлаживает один или несколько процессов, выполняющихся на локальном компьютере.

**Синтаксис**

Debug-Process [-Name] <string[]> [-Confirm] [-WhatIf] [<CommonParameters>]

Debug-Process [-Id] <Int32[]> [-Confirm] [-WhatIf] [<CommonParameters>]

Debug-Process -InputObject <Process[]> [-Confirm] [-WhatIf] [<CommonParameters>]

**Описание**

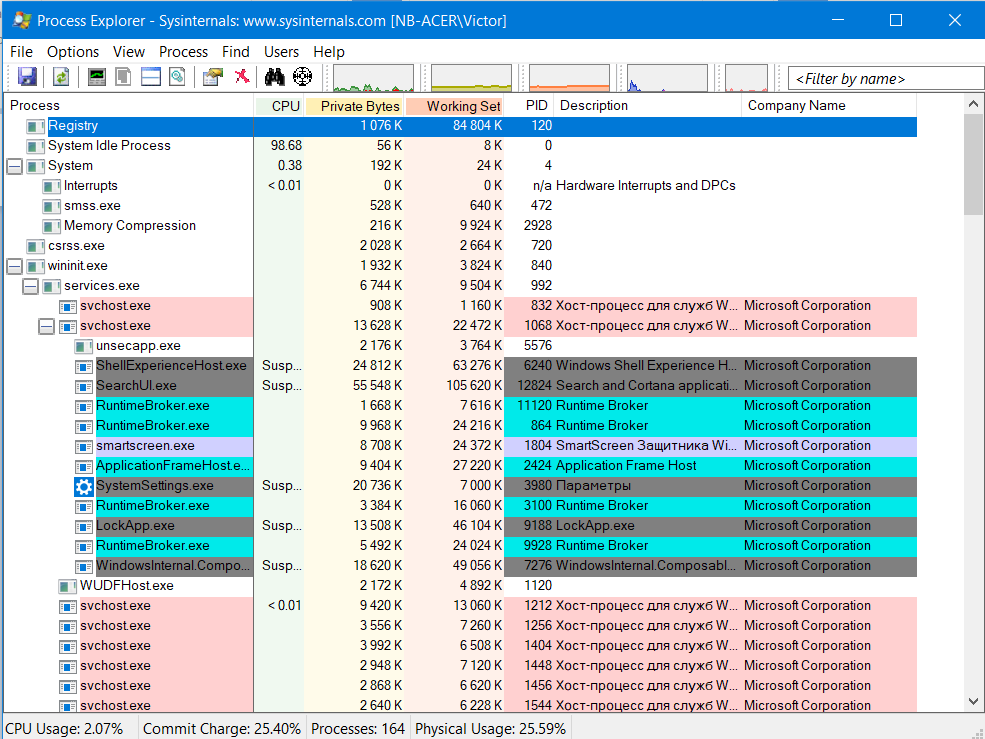
Командлет Debug-Process присоединяет отладчик к одному или нескольким процессам, выполняющимся на локальном компьютере. Процессы можно задать, указав их имена или идентификаторы (PID) либо передав объекты процессов по конвейеру командлету Debug-Process.

Командлет Debug-Process присоединяет отладчик, который в данный момент зарегистрирован для процесса. Перед использованием этого командлета проверьте, что отладчик загружен и правильно настроен.

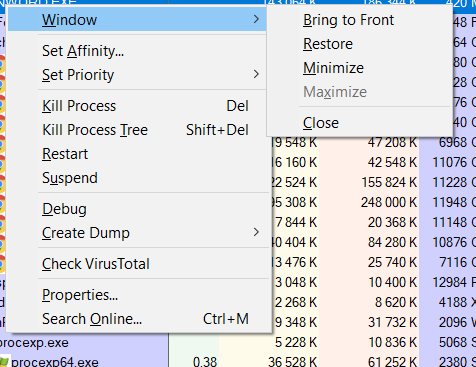
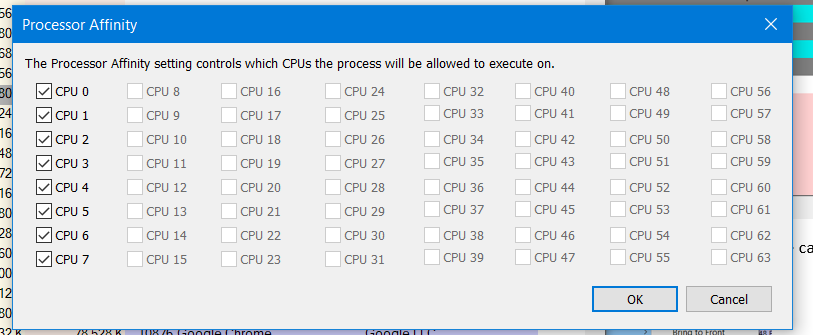
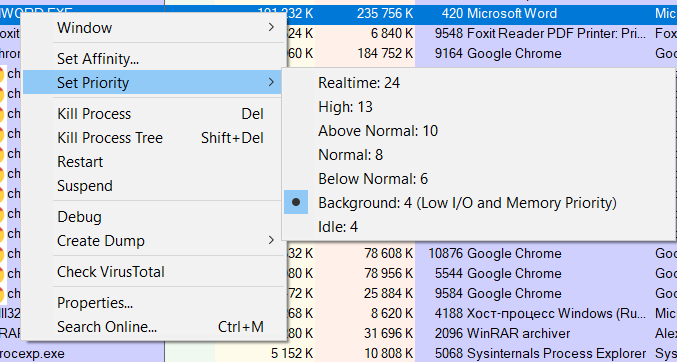
* **Wait-Process – используется для ожидания окончания процесса.**
* Ожидает остановки процессов, прежде чем принимать следующий ввод.
* **Синтаксис**
* Wait-Process [-Id] <Int32[]> [[-Timeout] <int>] [<CommonParameters>]
* Wait-Process -InputObject <Process[]> [[-Timeout] <int>] [<CommonParameters>]
* Wait-Process [-Name] <string[]> [[-Timeout] <int>] [<CommonParameters>]
* **Описание**
* Командлет Wait-Process ожидает остановки одного или нескольких выполняющихся процессов, прежде чем принимать следующий ввод. Этот командлет отключает командную строку консоли Windows PowerShell до тех пор, пока процессы не будут остановлены. Процесс можно задать с помощью его имени или идентификатора (PID). Также можно передать объект процесса командлету Wait-Process по конвейеру.
* Командлет Wait-Process работает только с процессами, выполняющимися на локальном компьютере.

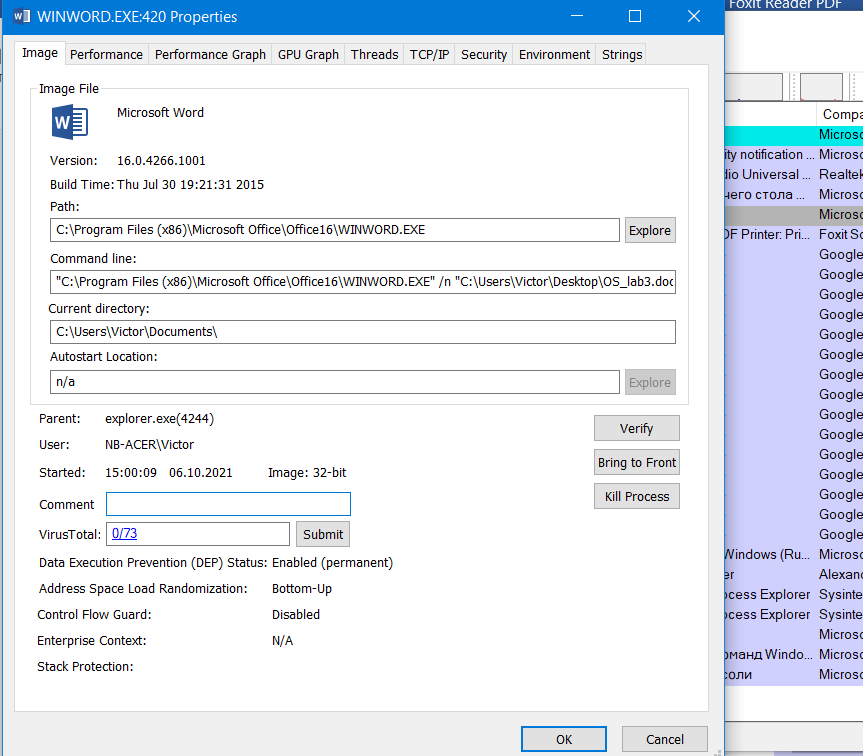
****

1. **Используя дополнительные инструменты с sysinternals (**[**https://docs.microsoft.com/en-us/sysinternals/**](https://docs.microsoft.com/en-us/sysinternals/)**).**

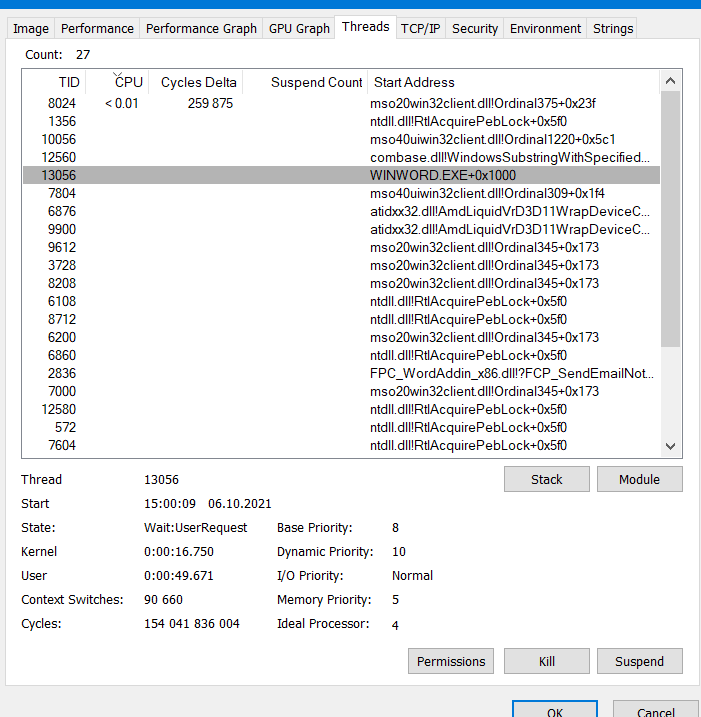


Я скачал утилиту process explorer. Это аналог диспетчера задач. В нём можно посмотреть всё то же самое, что и в диспетчере, но более подробно.

* Видно иерархию процессов (кто кого породил)
* Можно программно изменять размер окна процесса 
* Выбирать используемые ядра 
* Выбирать приоритет процесса 
* Завершать (убивать) процесс или дерево процессов
* Перезапуска процесс
* Временно приостанавливать
* Отлаживать
* Создавать файл dump для сохранения параметров процесса (стека и др)
* Посмотреть свойства процесса очень подробно



Там же увидеть информацию о потоках процесса



В process explorer можно так же и фильтровать процессы, сортировать, убивать, создавать. Некоторые действия можно делать только при запуске от имени администратора. Есть дублирующие иконки над таблицей процессов. Поле ввода для поиска по имени и другое. Proccess explorer предоставляет больше возможностей, чем диспетчер задач.

**Вывод:** Диспетчер задач (особенно в новых версиях Windows) очень часто оказывается незаменимым, поскольку позволяет, как минимум, быстро закрывать зависшие программы, перезапускать и настроить автозапуск нужых программ. Более опытным пользователям порой может потребоваться проанализировать нагрузку на компьютер от той или иной программы или же в целом. Поэтому всегда нужно уметь пользоваться диспетчером задач.  
Всё, что можно сделать с помощью GUI интерфейса диспетчера задача, реализуется и в консольном интерфейсе powerShell. В нём больше возможностей, так как не всё можно уместить в GUI интерфейсе.  
Также пользователю предоставляется возможность скачать утилиты для удобства управления процессами и потоками, если предыдущих двух вариантов недостаточно. Например, можно скачать ProcessExplorer.