Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Институт Информационных Технологий и Анализа Данных

Кафедра вычислительной техники

**Название работы** – “Управление процессами в ОС Windows”

Отчет по лабораторной работе “Лабораторная работа №1”

по дисциплине Информационная безопасность и защита информации

Вариант 3

Выполнил

Студент, номер группы ИСМб-19-1 \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.Д.Солопов

Дата: \_\_\_\_\_\_\_\_\_\_

Принял

Должность \_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В.Чумилин

Дата: \_\_\_\_\_\_\_\_\_\_

Иркутск 2021 г.

Содержание

[Цель работы 3](#_Toc64402118)

[Постановка задач 4](#_Toc64402119)

[Решение задач 5](#_Toc64402120)

[Вывод 29](#_Toc64402121)

Цель работы

Изучение возможностей контроля и управления процессами в операционных системах Windows, научиться работать с Диспетчером задач, ознакомиться с управлением процессами в ОС Windows с помощью утилит Process Explorer, Process Hacker.

Постановка задач

Копии экрана с выполненным заданием и описание выполненных действий

привести в отчете.

**Задание 1.** На вкладке Процессы Диспетчера задач измените количество столбцов, запишите выполненные для этого операции. Какие из процессов запущены Пользователем?

**Задание 2.** Сколько процессов активно на момент выполнения практической работы, на сколько загружен центральный процессор, какой объем памяти выделен на текущие процессы?

**Задание 3.** Просмотреть справочную систему Диспетчера задач. Найти информацию о запуске новых программ, завершении текущих программ с использованием Диспетчера и выписать в тетрадь.

**Задание 4.** Выполните следующие действия с помощью утилит Process Explorer и Process Hacker. Выполняемые действия иллюстрируйте копиями экранов.

• Отсортируйте процессы по заданному критерию.

• Опишите один из системных процессов.

• Запустите указанное приложение.

• Опишите возникший процесс по заданным характеристикам.

• Принудительно завершите указанный процесс.

• Опишите различия в работе 3 утилит.

Решение задач

**Задание 1:**

На вкладке Процессы Диспетчера задач измените количество столбцов, запишите выполненные для этого операции. Какие из процессов запущены Пользователем?

Для выполнения данного задания в ОС Windows 10 необходимо открыть диспетчер задач нажав комбинацию клавиш Esc + Shift + Ctrl.

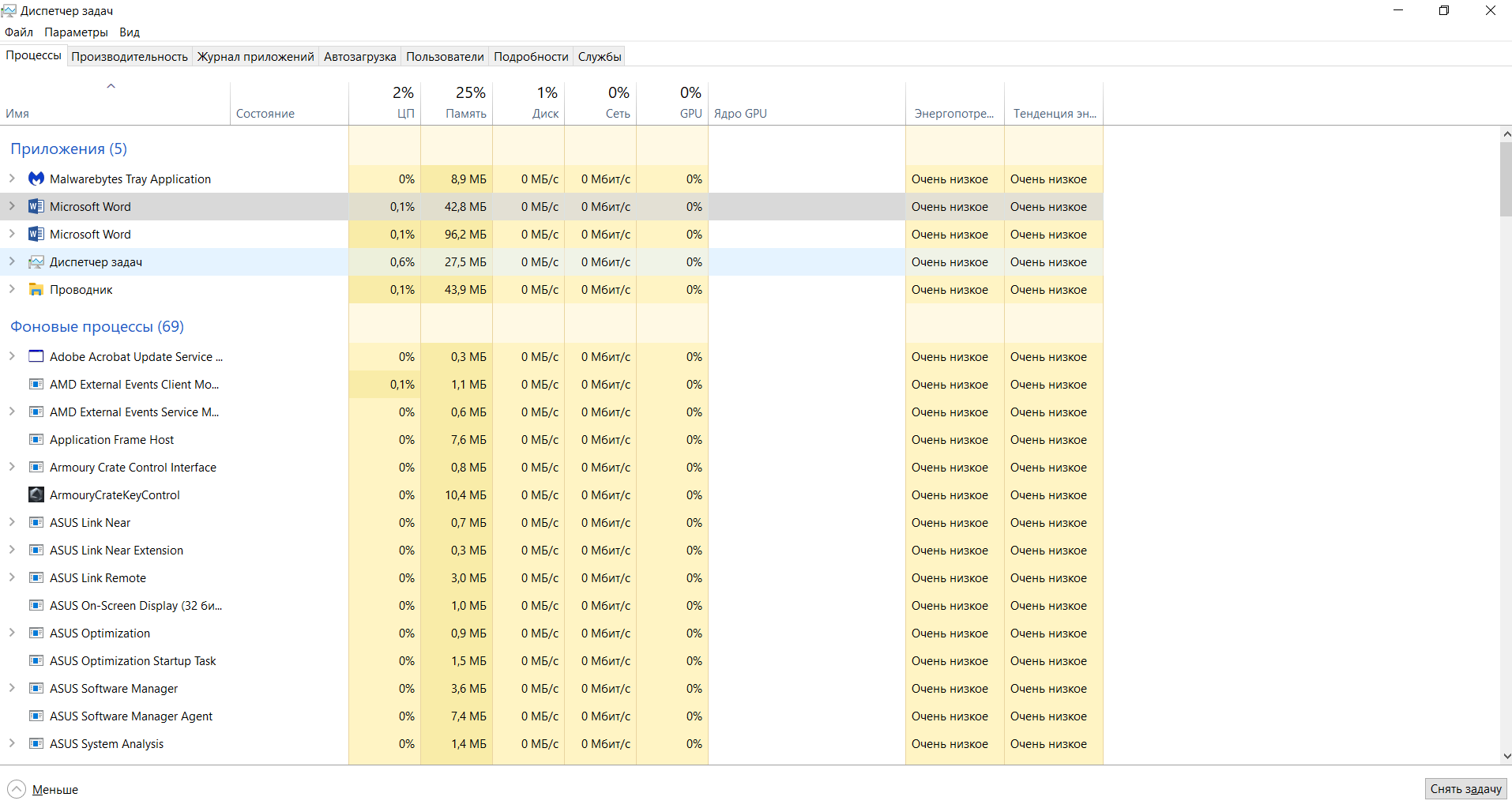


Рисунок 1 – Результат вызова диспетчера задач с помощью комбинации клавиш

Для уменьшения или увеличения количество столбцов в диспетчере задач достаточно нажать правую кнопку мыши в любом месте множества атрибутов таблицы, диспетчера задач, а затем убрать или выбрать те столбцы и строки, которые есть необходимость просматривать.

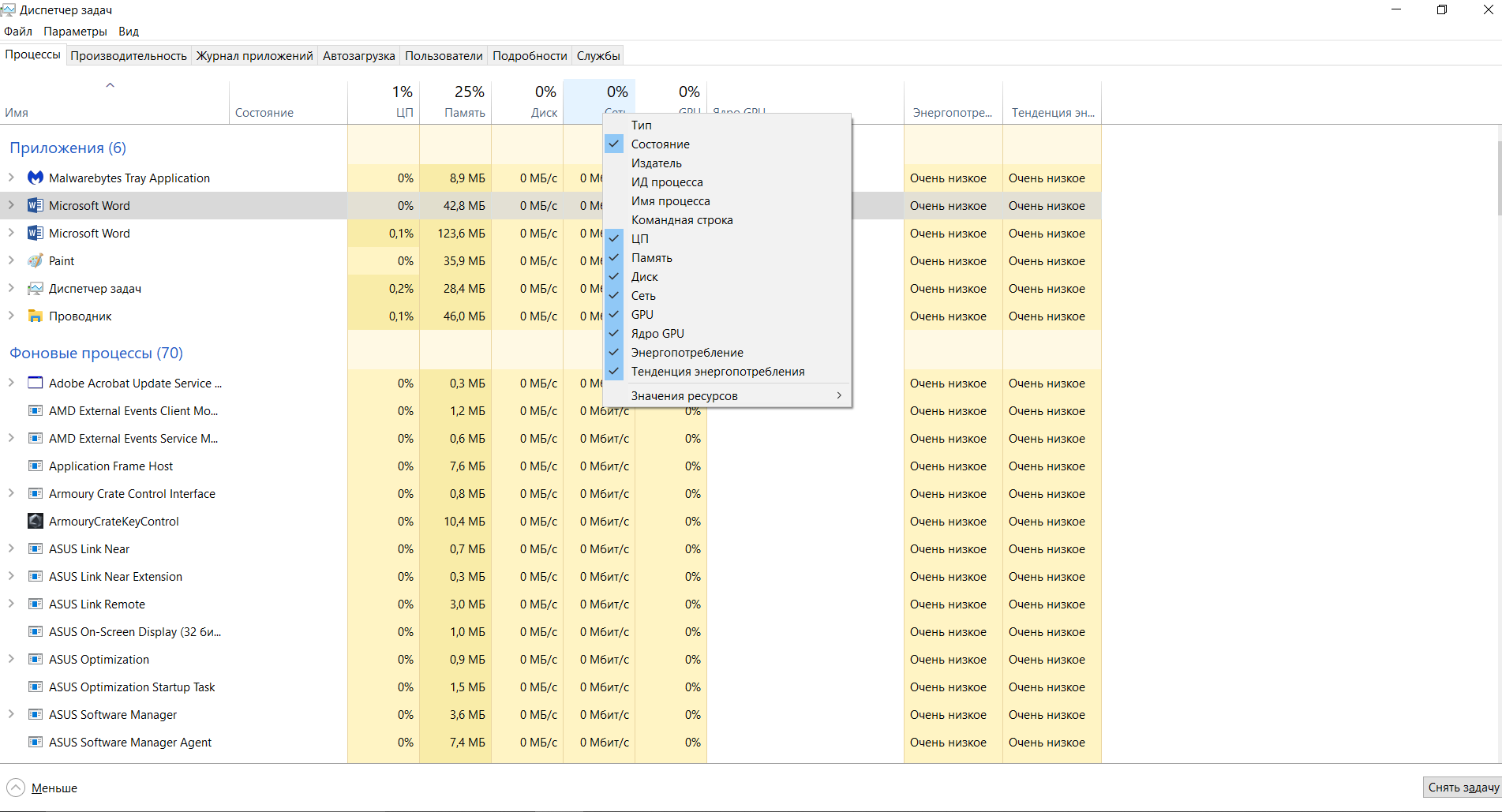


Рисунок 2 – Результат нажатия правой кнопки мыши в область атрибутов таблицы диспетчера задач

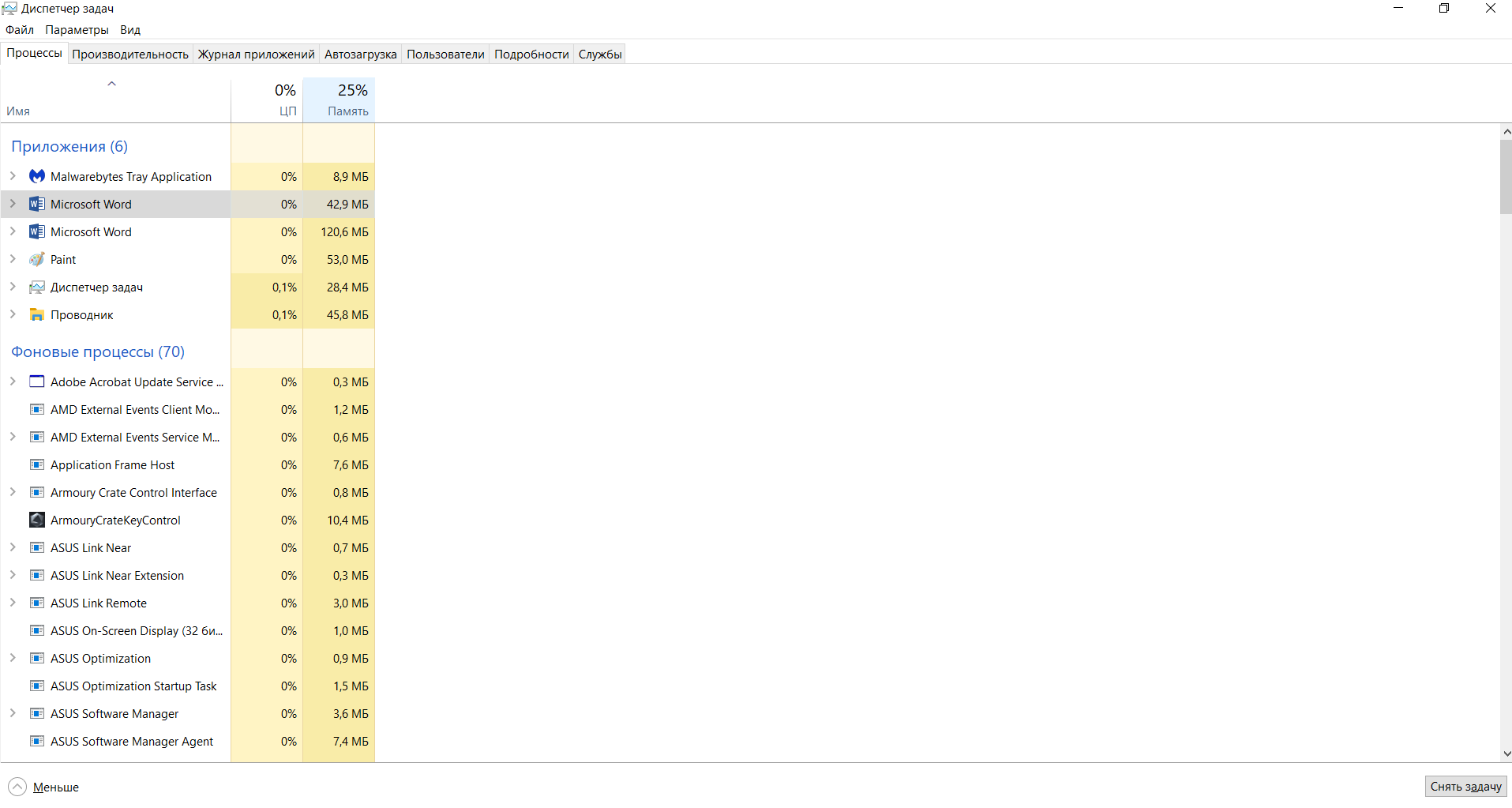


Рисунок 3 – Уменьшение числа столбцов в таблице диспетчера задач

На рисунке 3 продемонстрирован результат изменения числа столбцов в диспетчере задач, с помощью интерфейса описанный рисунком 2.

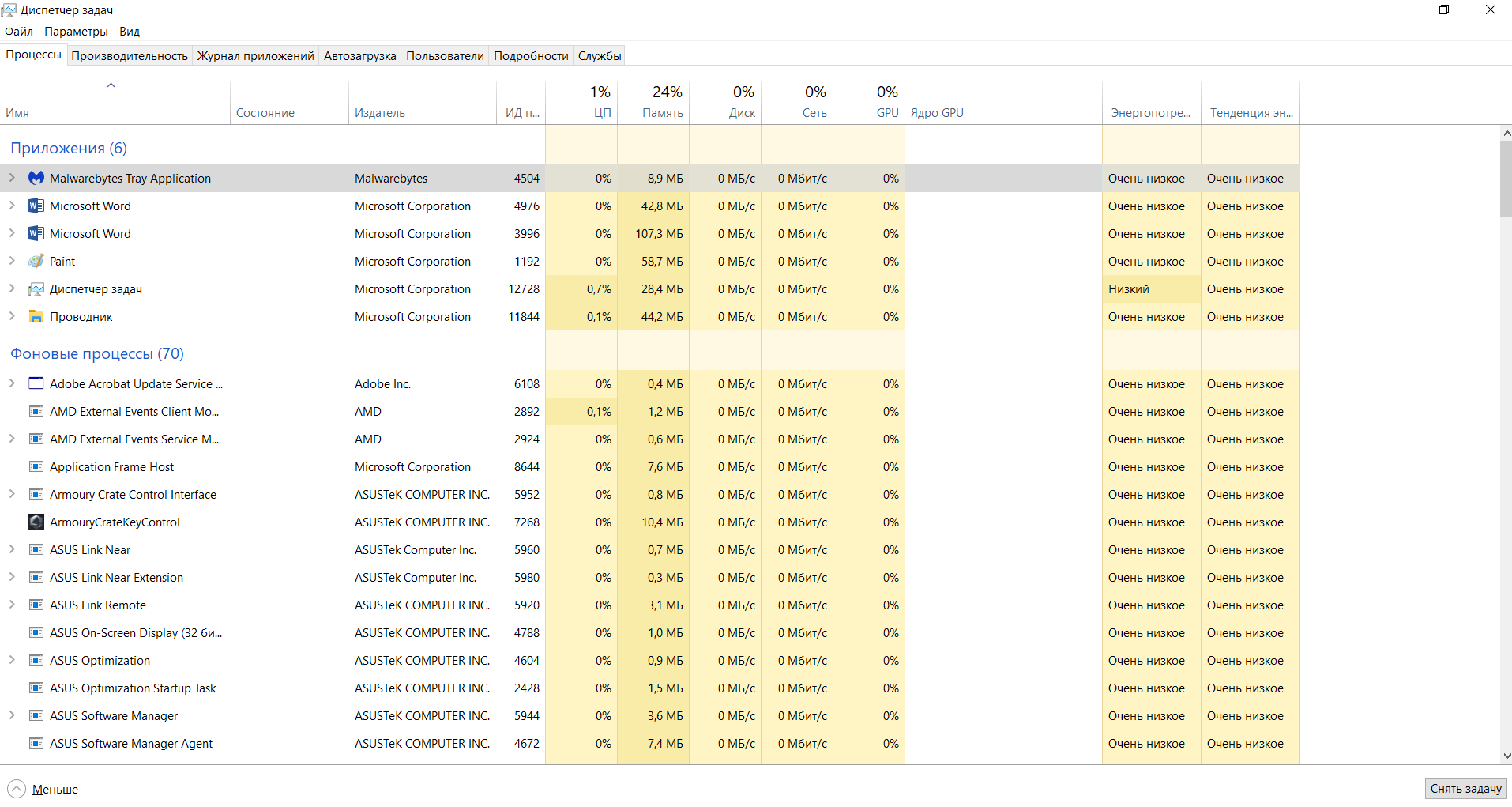


Рисунок 4 – Увеличение числа столбцов в диспетчере задач относительно результата, представленного на рисунке 2

Поиск процессов, которые запустил пользователь, будем рассматривать относительно рисунка 4.

Процессы, запущенные пользователем: Malwarebytes Tray Application, Microsoft Word (2 процесса), Paint, Диспетчер задач и Проводник.

**Задание 2.** Сколько процессов активно на момент выполнения практической работы, на сколько загружен центральный процессор, какой объем памяти выделен на текущие процессы?

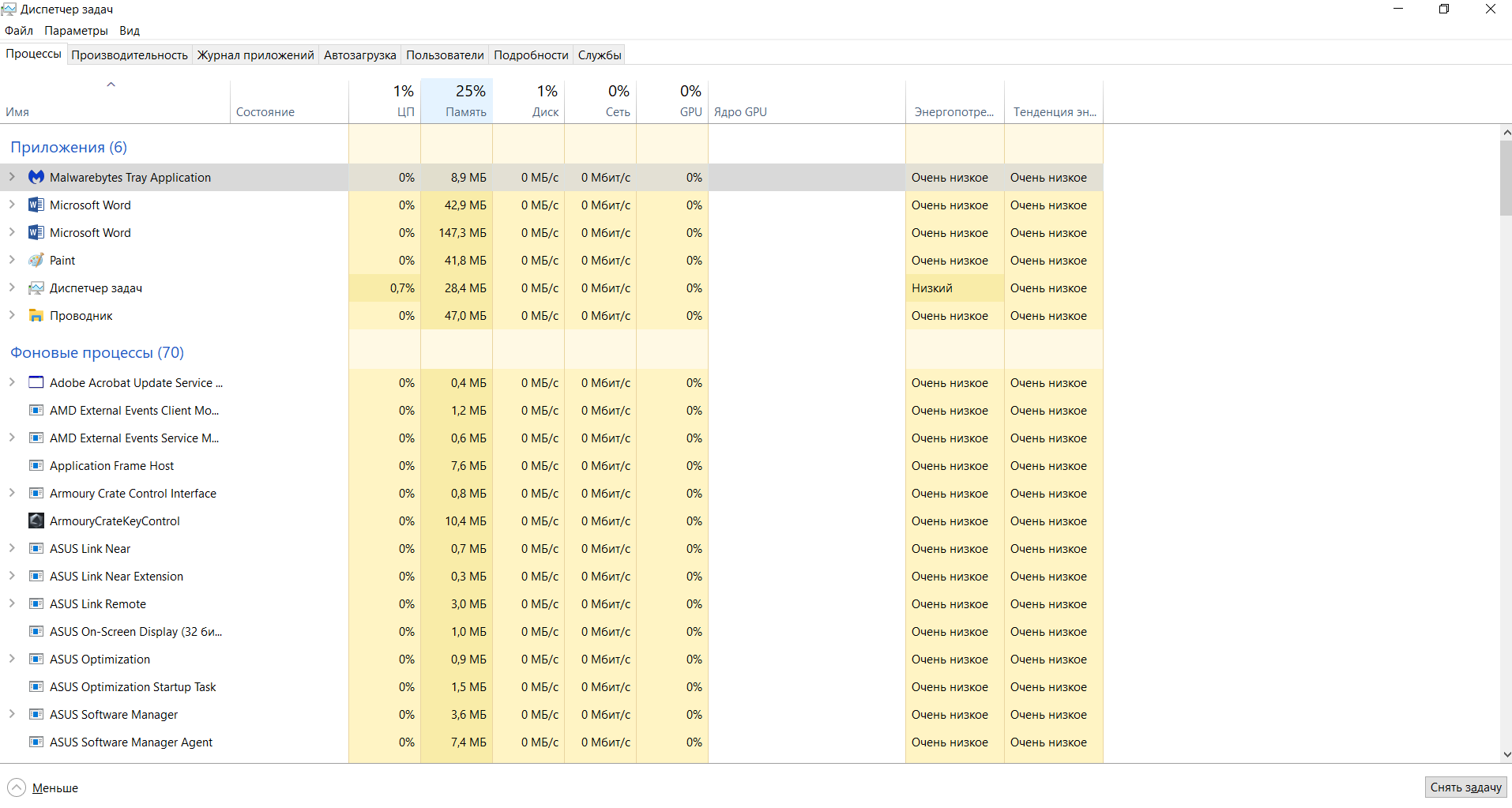


Рисунок 5 – Данные диспетчера задач на момент выполнения лабораторной работы

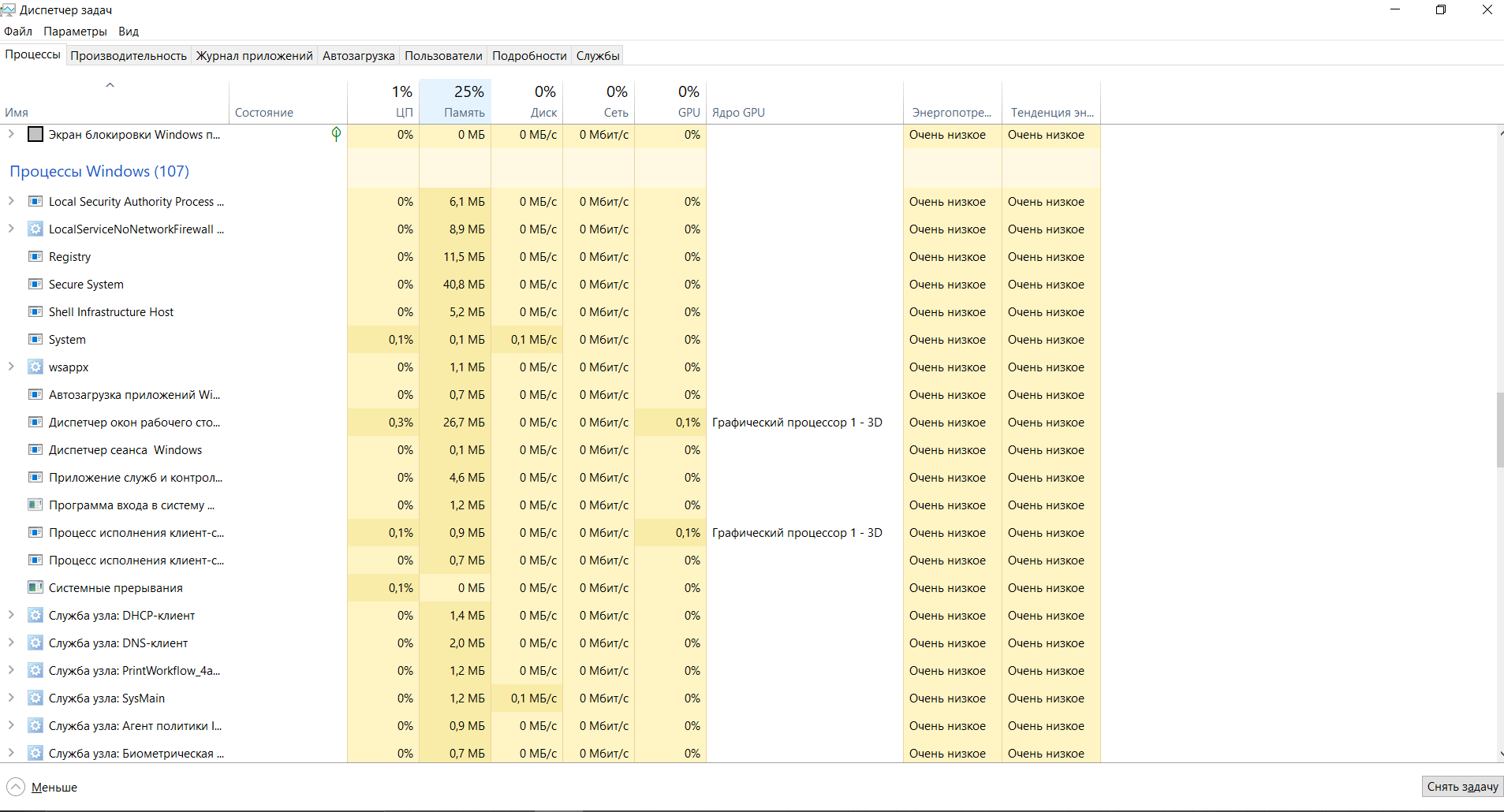


Рисунок 6 - Данные диспетчера задач на момент выполнения лабораторной работы

Общее число активных процессов на момент выполнения работы (включая фоновые, пользовательские и процессы Windows): 6 + 70 + 107 = 183 процесса.

Следует отметить, что фоновые и Windows процессы изменяются достаточно быстро и динамично. Процессы могут как зависеть от пользовательских действий (пользовательские процессы), так и не зависеть от пользовательских действий (фоновые и Windows процессы, однако в Windows процессах оцениваются действия пользователя для включения или отключения тех или иных процессов).

Для оценки состояния процессора и объёма памяти стоит зайти во вкладку “Производительность” диспетчера задач и оценить каждый отдельный пункт производительности.

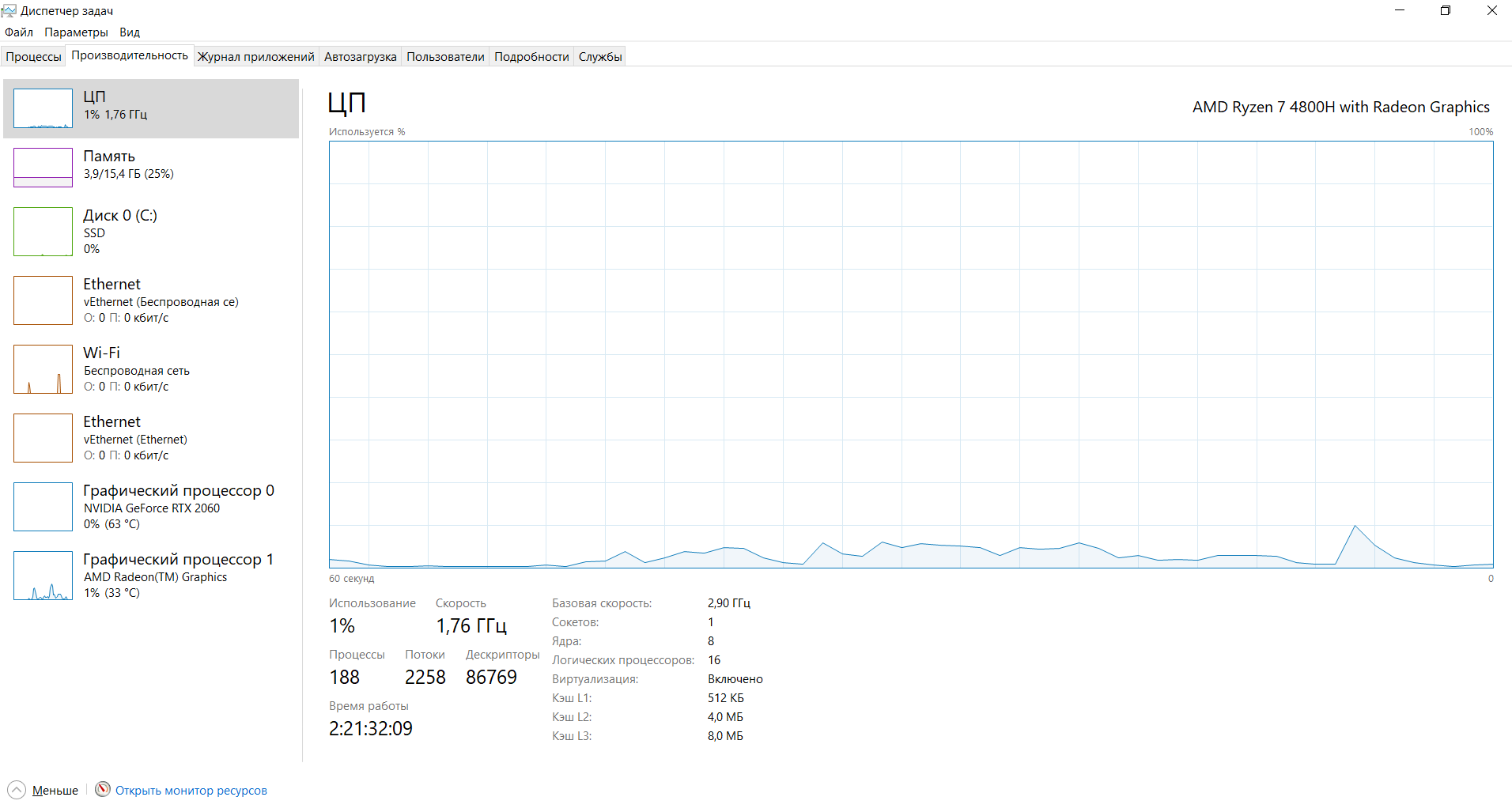


Рисунок 7 – Показатели производительности процессора (ЦП)

Рассматривая актуальные показатели производительности ЦП на момент выполнения лабораторной работы (см. рис. 7) можно сделать вывод о том, что процессор загружен на 1%, его частота обработки данных 1, 76 ГГц, количество процессов, которые он обрабатывает 188, потоков 2258, дескрипторов 86769 и многие другие данные о производительности.

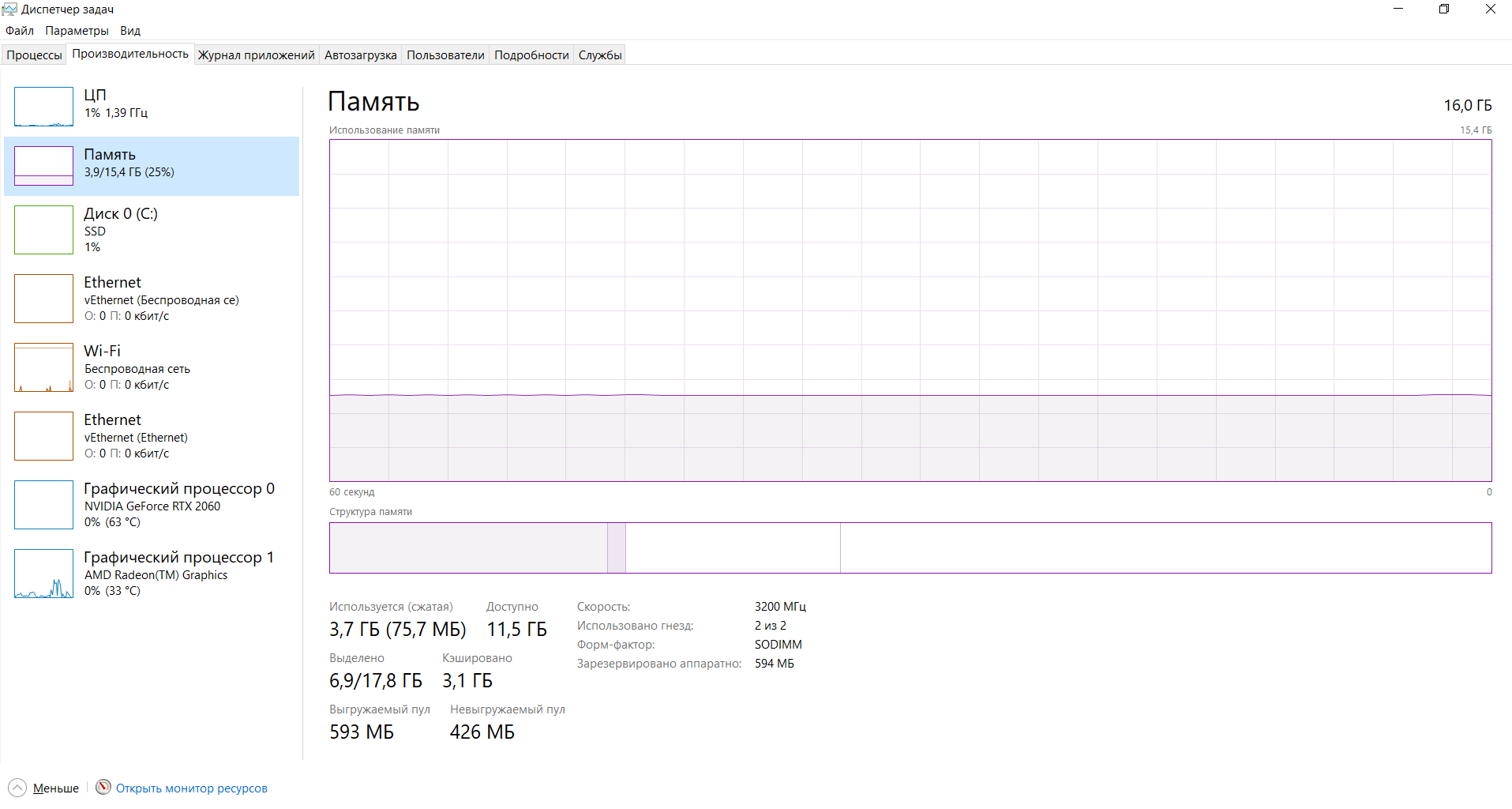


Рисунок 8 - Показатели производительности памяти (ОЗУ)

Рассматривая актуальные показатели производительности памяти на момент выполнения лабораторной работы (см. рис. 8) можно сделать вывод о том, что память, используемая процессами количественно равна 3,7 ГБ, доступно 11,5 ГБ, выделено 6,9/17,8 ГБ, кэшировано 3,1 ГБ, выгружаемый пул 593 МБ, невыгружаемый пул 426 МБ и многие другие данные о производительности.

**Задание 3.** Просмотреть справочную систему Диспетчера задач. Найти информацию о запуске новых программ, завершении текущих программ с использованием Диспетчера и выписать в тетрадь.

Интерфейс диспетчера задач в ОС Windows 10 не предоставляет вкладку “Справка”, как её предоставляет диспетчер задач более ранних версий ОС Windows.

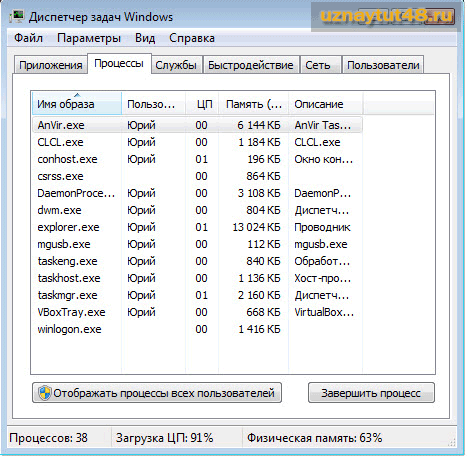


Рисунок 9 – Диспетчер задач в Windows 7

Ссылка на источник (дата обращения 16.02.2021): <http://uznaytut48.ru/windows/dispetcher-zadach-windows.html>

Однако, если перейти в монитор ресурсов, выбрав в диспетчере задач вкладку “Производительность”, будет доступна вкладка “Справка” (см. рис. 10).

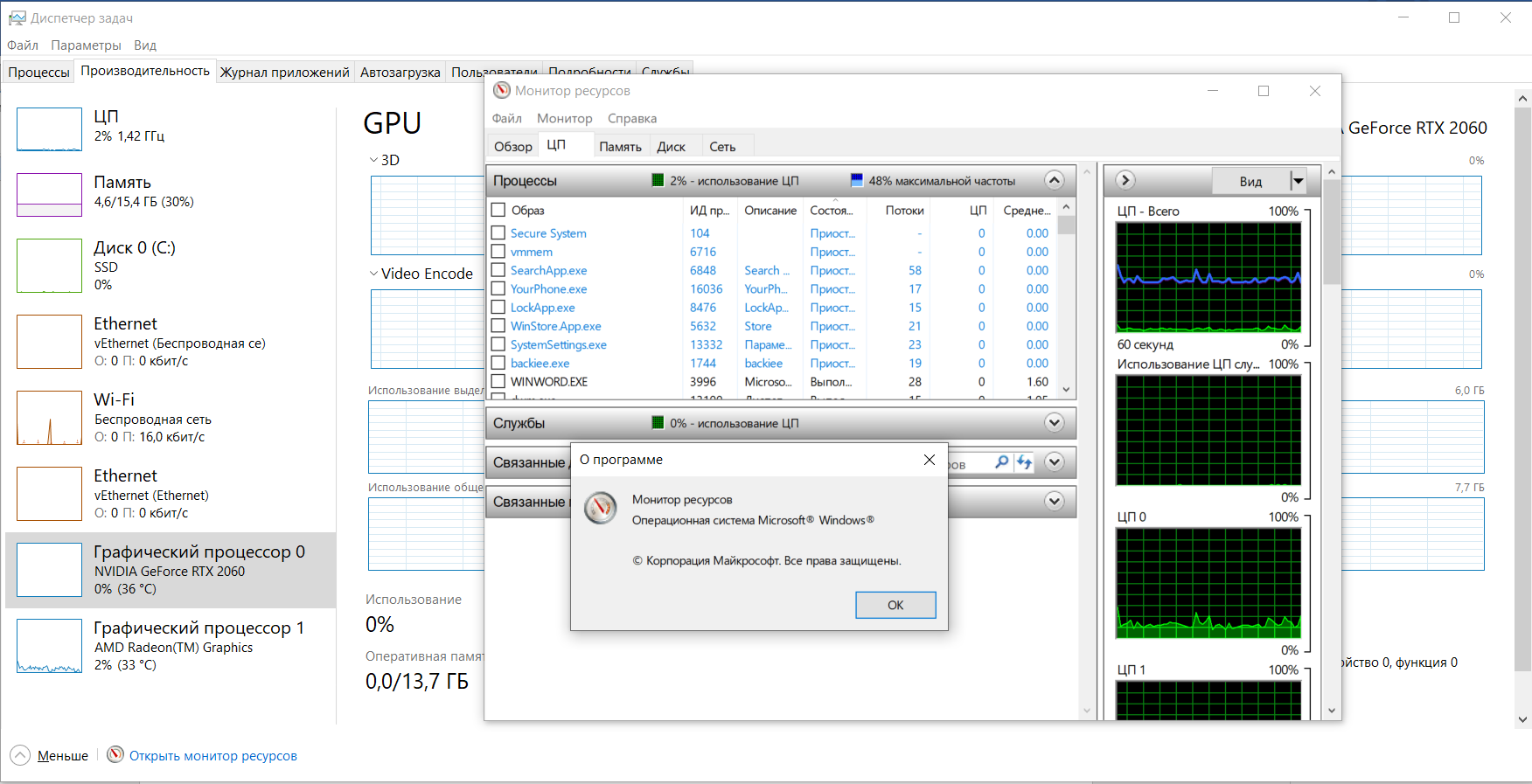


Рисунок 10 – Справка из монитора ресурсов

Справку об использовании диспетчера задач можно найти в интернете, информация доступна и находится в свободном доступе.

Ссылка на статью (дата обращения 16.02.2021): <https://ip-calculator.ru/blog/ask/kak-polzovatsya-dispetcherom-zadach-v-windows-10/>

Ссылка на статью (дата обращения 16.02. 2021): <https://www.bestfree.ru/article/computer/task-manager.php>

В ОС Windows 7 справка в диспетчере задач присутствует, на рисунках 11-13 представлена справочная информация.

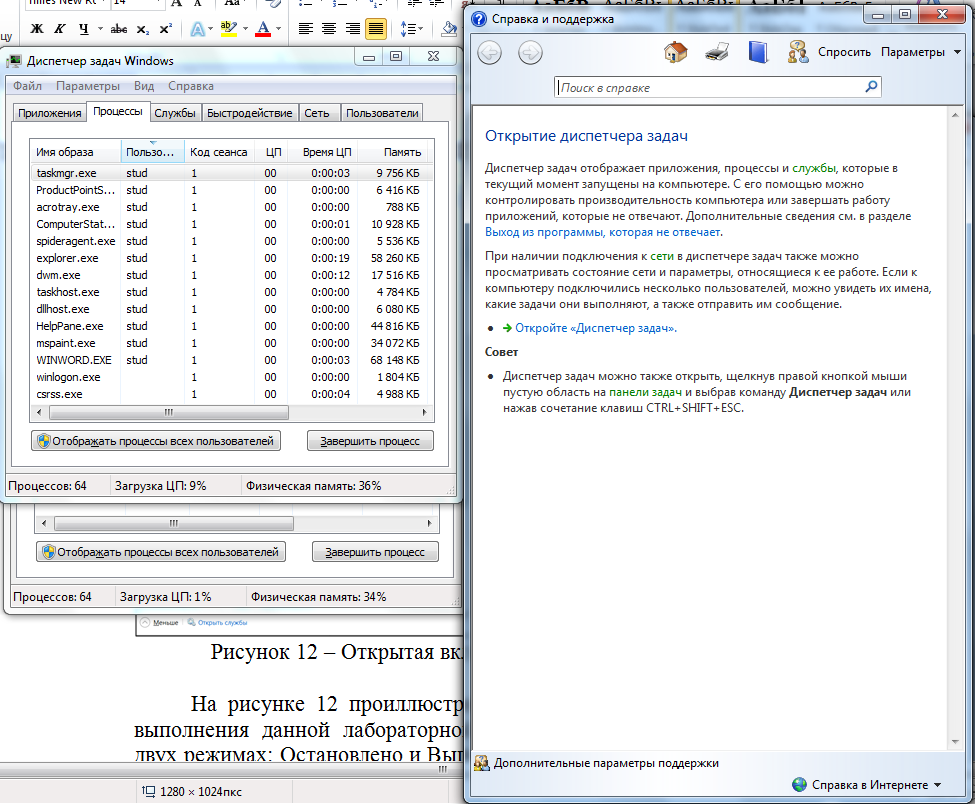


Рисунок 11 – Справочная информация о диспетчере задач

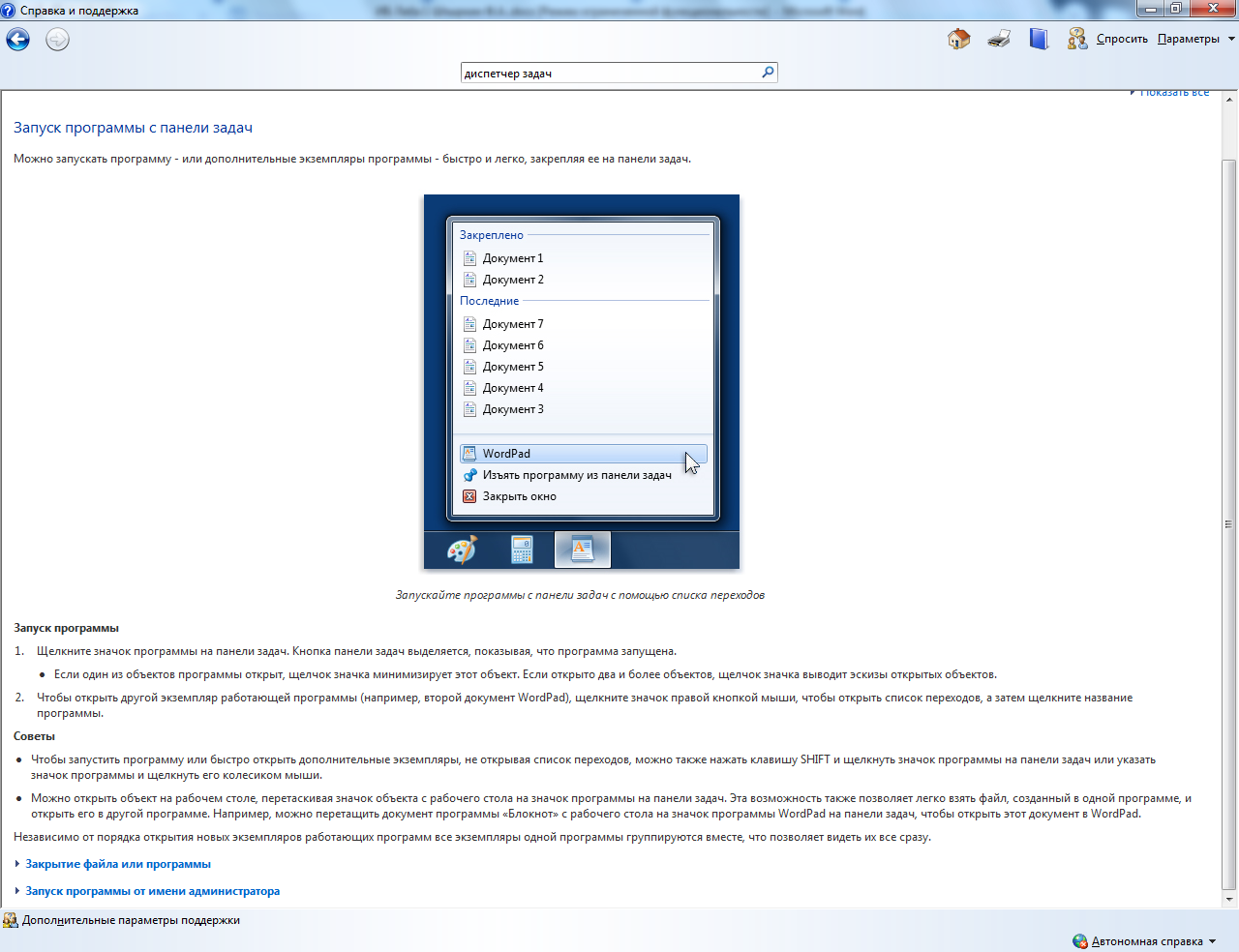


Рисунок 12 – Справочная информация о диспетчере задач

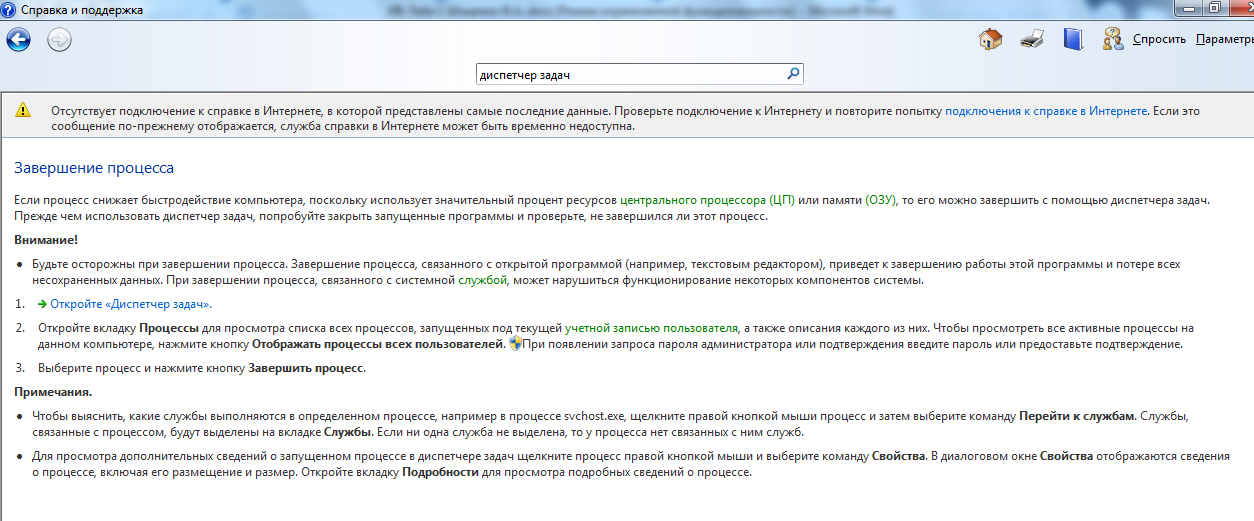
****

Рисунок 13 - Справочная информация о диспетчере задач

Для получения информации о времени пользования процессами необходимо открыть вкладку “Журнал приложений” и обратить внимание на такой показатель как “Время ЦП” характеризующее всё время, потраченное ЦП на обработку инструкций процесса.

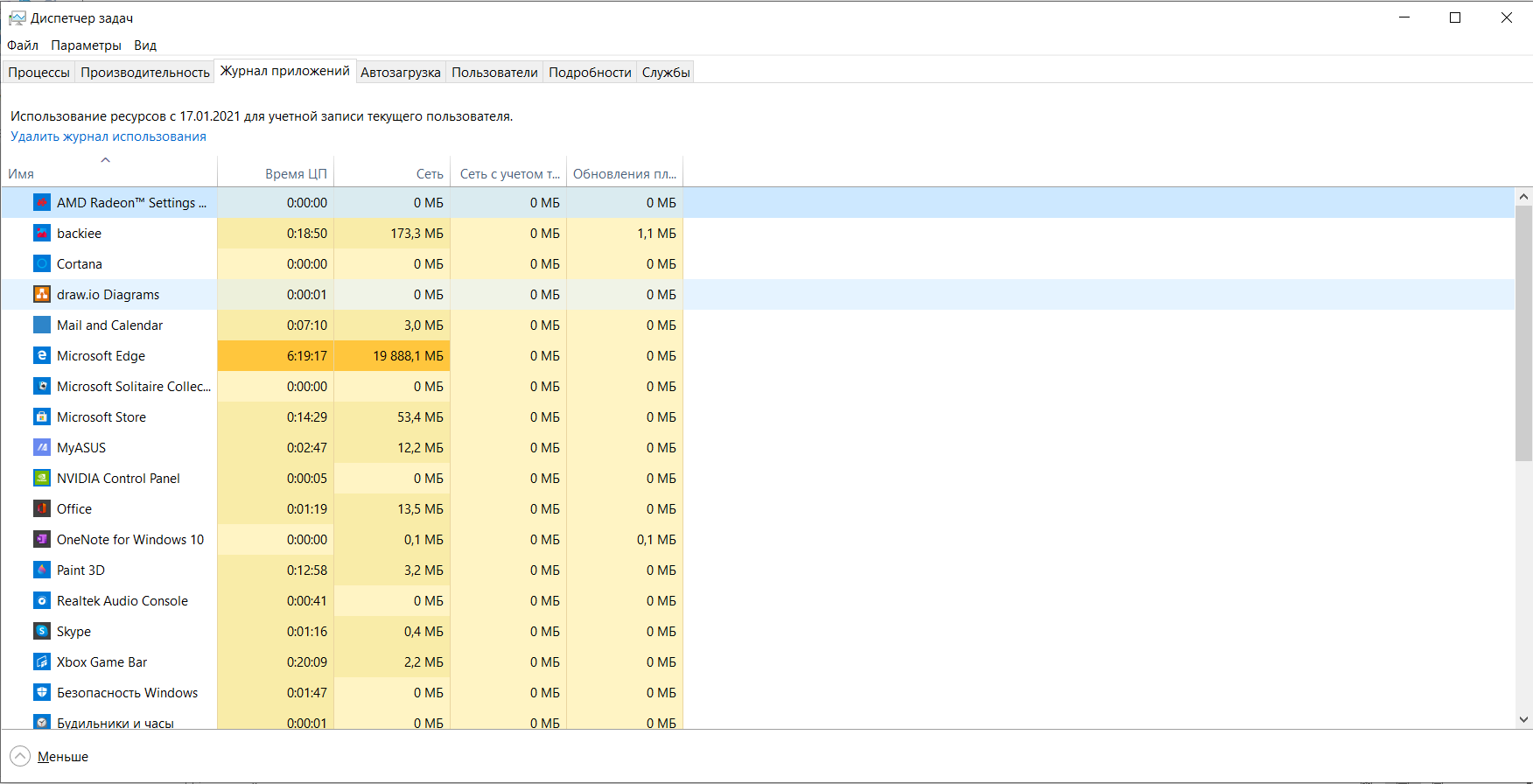


Рисунок 14 – Журнал приложений в диспетчере задач

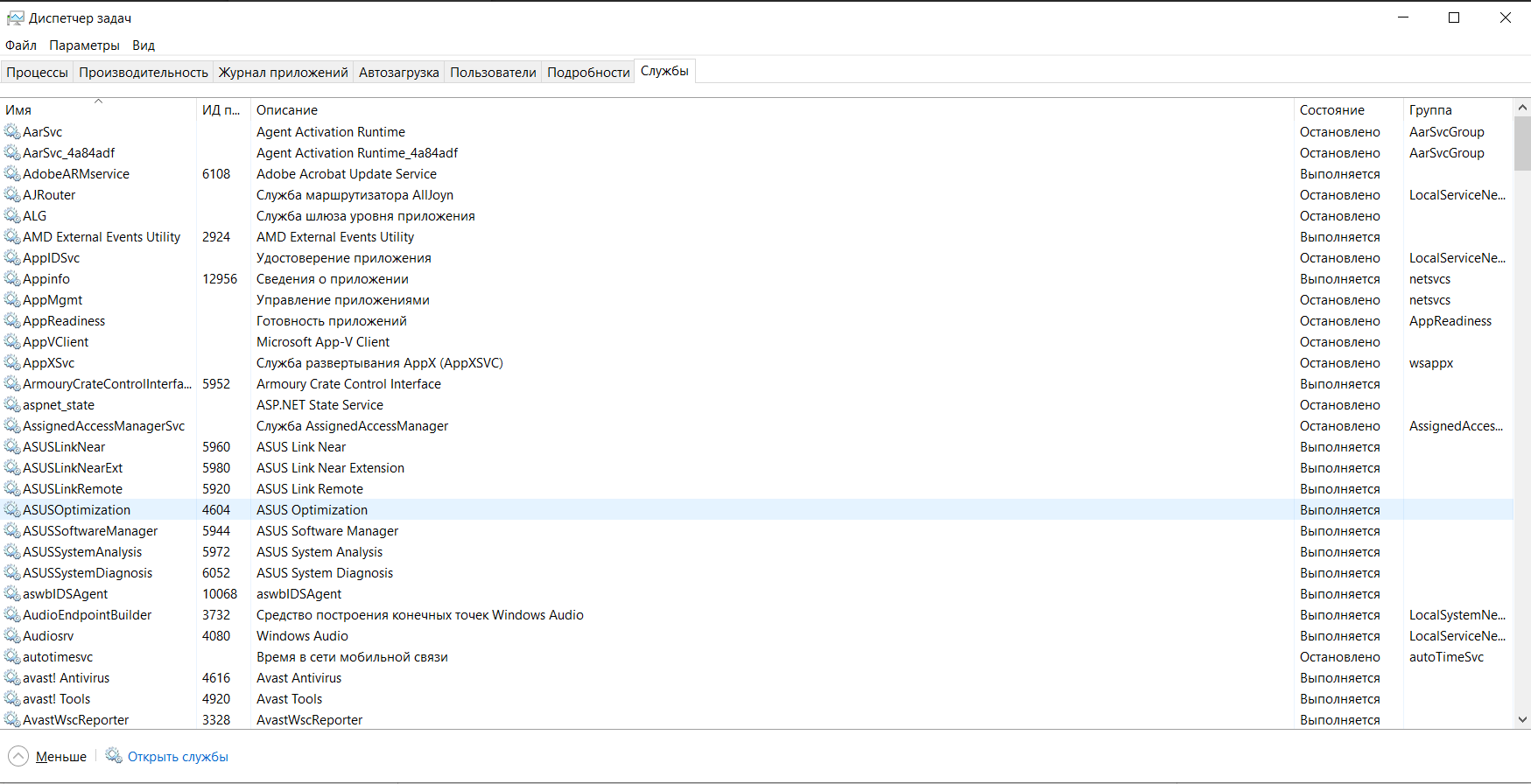


Рисунок 15 – Открытая вкладка “Службы” в диспетчере задач

На рисунке 12 проиллюстрировано состояние всех служб на момент выполнения данной лабораторной работы. Состояние может находится в двух режимах: Остановлено и Выполняется.

Чтобы открыть справку в Process Explorer нужно нажать на вкладку Help в программе (см. рис. 14).

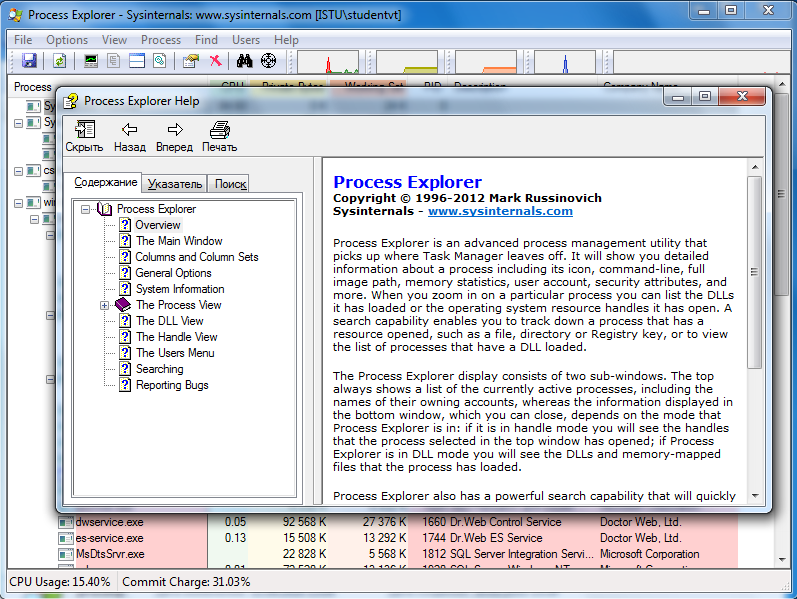


Рисунок 16 – Открытая вкладка “Help” в Process Explorer

**Задание 4.** Выполните следующие действия с помощью утилит Process Explorer и Process Hacker. Выполняемые действия иллюстрируйте копиями экранов.

• Отсортируйте процессы по заданному критерию.

• Опишите один из системных процессов.

• Запустите указанное приложение.

• Опишите возникший процесс по заданным характеристикам.

• Принудительно завершите указанный процесс.

• Опишите различия в работе 3 утилит.

**Сортировка по загрузке процесса:**

Чтобы сортировать таблицу по загрузке процесса, нужно в Process Explorer или Process Hacker нажать на атрибут CPU, и над самим названием столбца должна появиться направляющая метка (как сортируется по возрастанию или по убыванию значения полей)

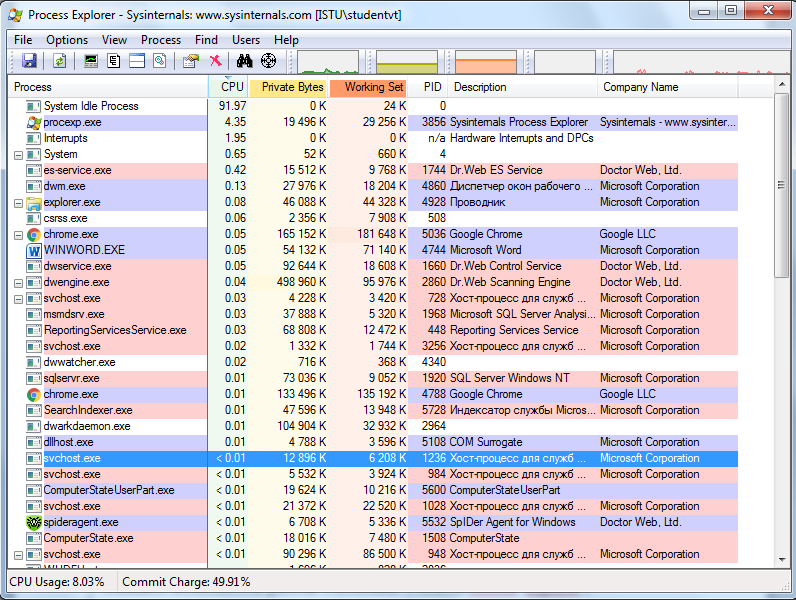


Рисунок 17 – Сортировка по загрузке процесса в Process Explorer (по убыванию)

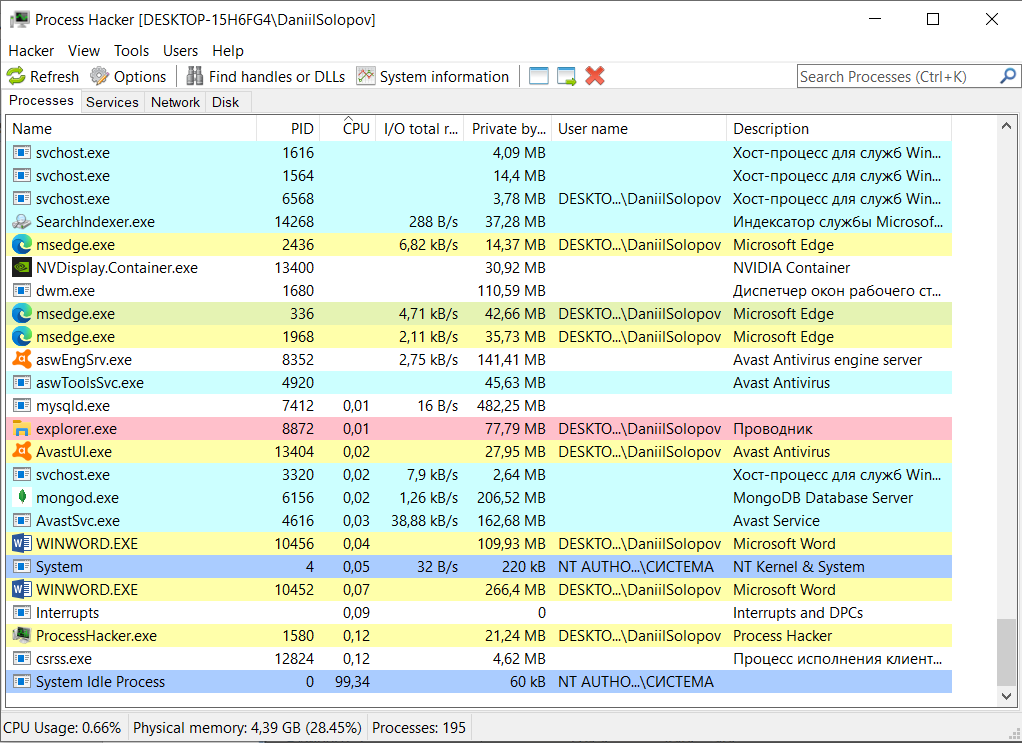


Рисунок 18 – Сортировка по загрузке процесса в Process Hacker (по возрастанию)

**Описание системного процесса:**

Подсистема клиент/сервер времени выполнения (англ. Client/Server Runtime Subsystem, CSRSS) или csrss.exe, входит в состав операционной системы Microsoft Windows NT, и представляет собой часть пользовательского режима подсистемы Win32.

Завершение csrss.exe ведёт к BSOD (синему экрану смерти) и аварийной перезагрузке Windows. Исполняемый файл csrss.exe хранится в папке %SYSTEMROOT%\system32.

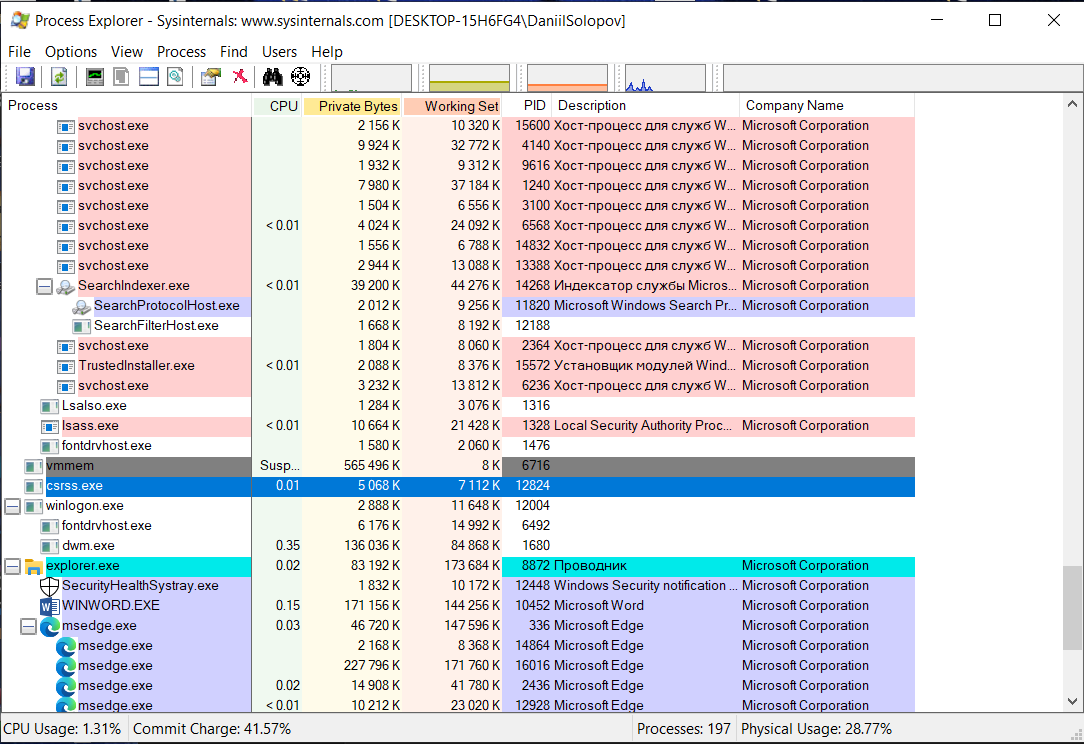
PID (идентификатор процесса): 4774

CPU < 0.01 (степень использования процессора меньше 1%)

Description: Процесс исполнения клиент-сервер

Private Bytes (объем оперативной памяти, выделенной данному процессу и не разделяемой с другими процессами): 5068 К

Working Set (рабочий набор процесса, представляющий собой суммарный объем всех страниц используемой им памяти, в данный момент времени): 7112 К

Рисунок 19 – Системный процесс csrss.exe в Process Explorer

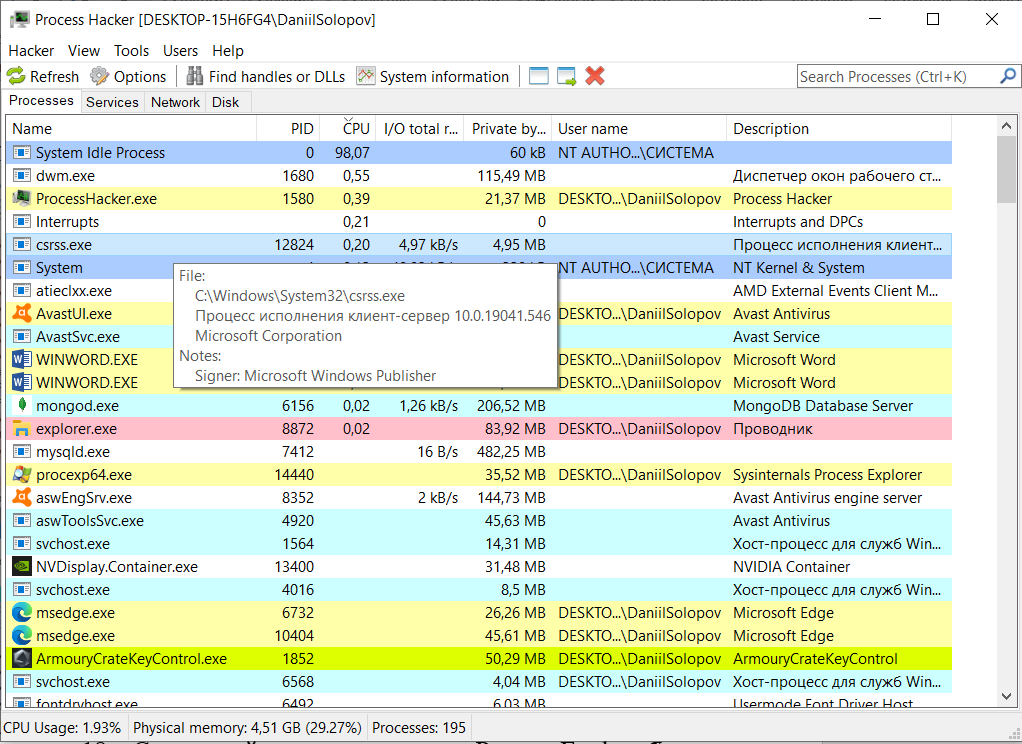


Рисунок 20 - Системный процесс csrss.exe в Process Hacker

**Запуск приложения WordPad:**

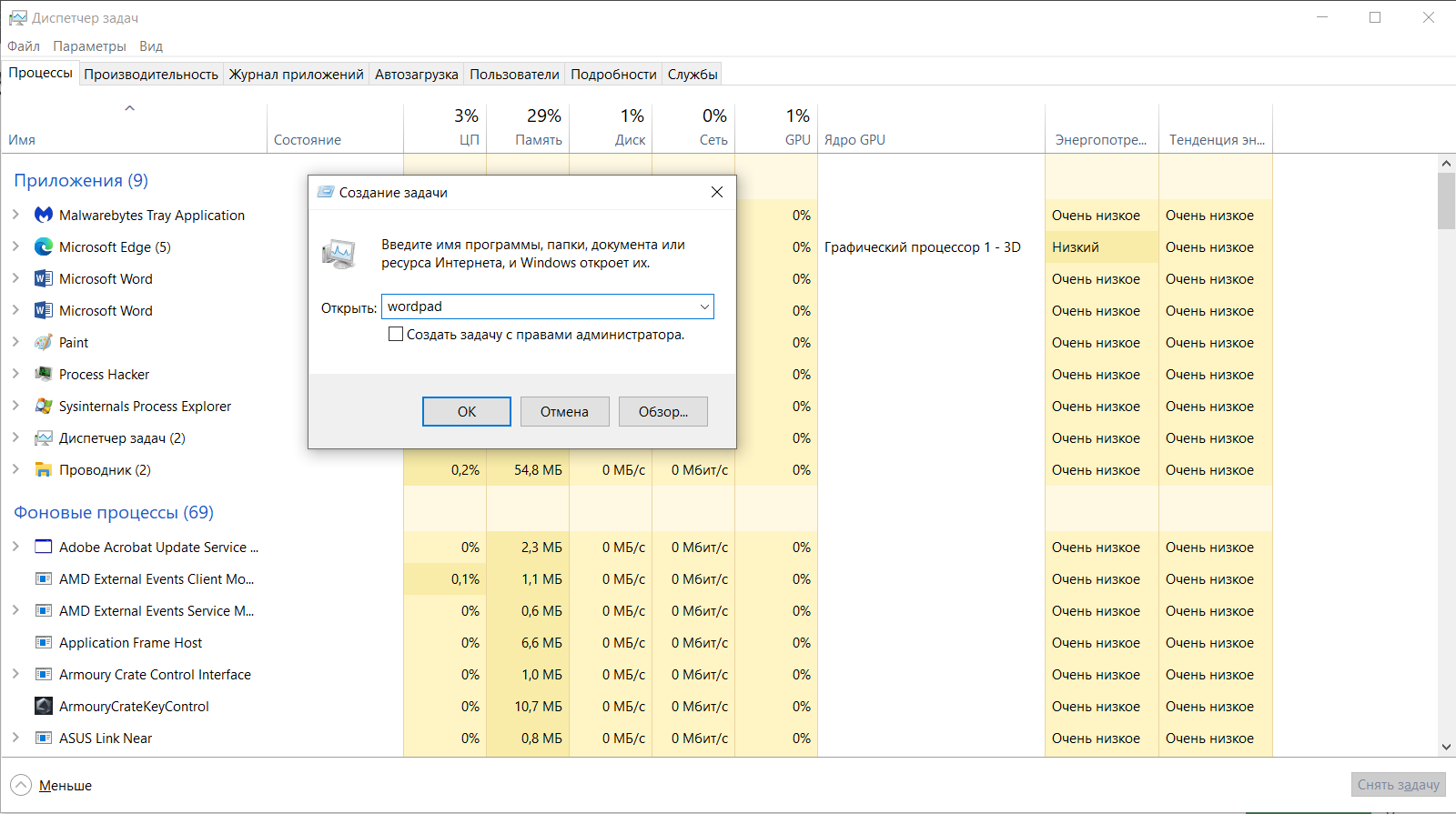


Рисунок 21 – Запуск приложения WordPad через диспетчера задач

Чтобы запустить приложение WordPad через диспетчер задач, нужно нажать на вкладку “Файл”, а далее нажать на вкладку “Запустить новую задачу”. На рисунке 20 представлен результат нажатия на вкладки, а на рисунке 21 представлен результат.

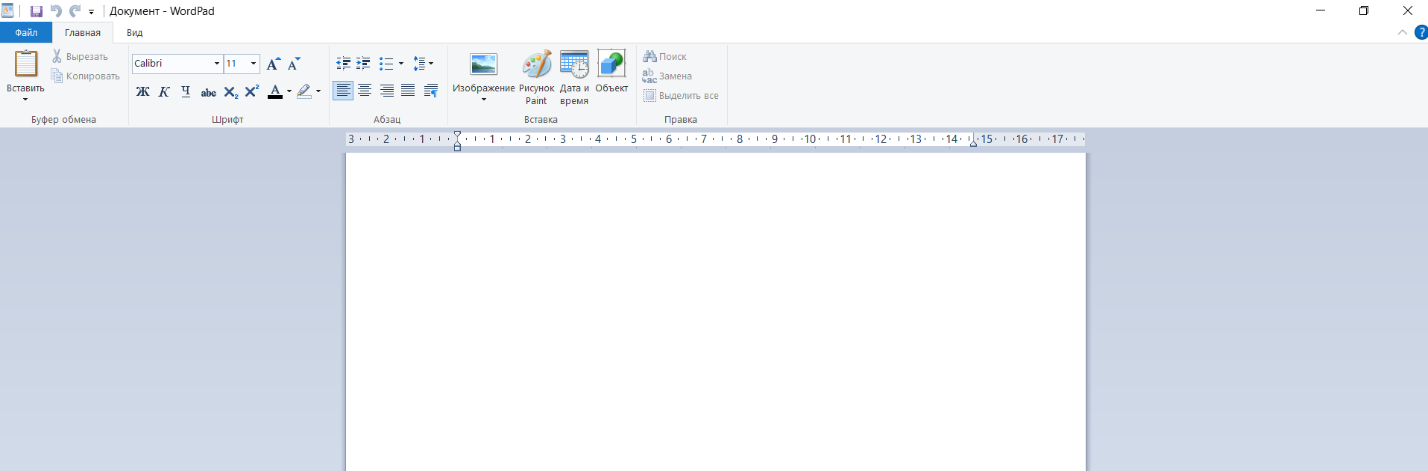


Рисунок 22 – Результат запуска приложения

Для запуска приложения в Process Explorer необходимо нажать на кнопку File, а затем на кнопку Run и в текстовом поле ввести wordpad.

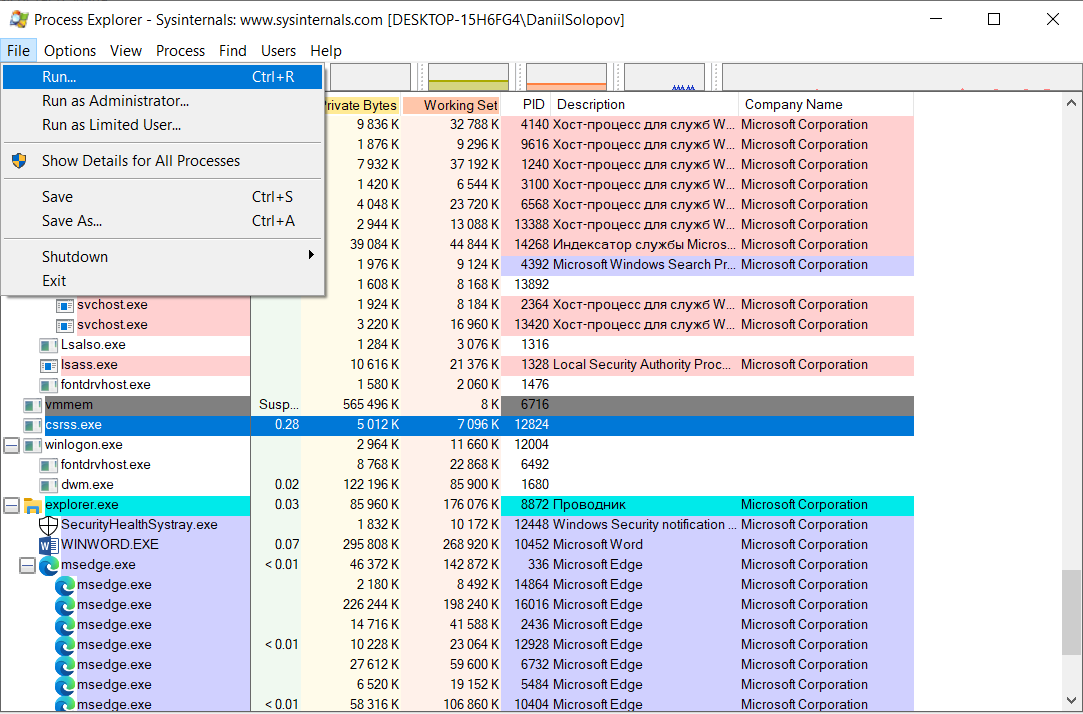


Рисунок 23 – Нажатие вкладок в Process Explorer

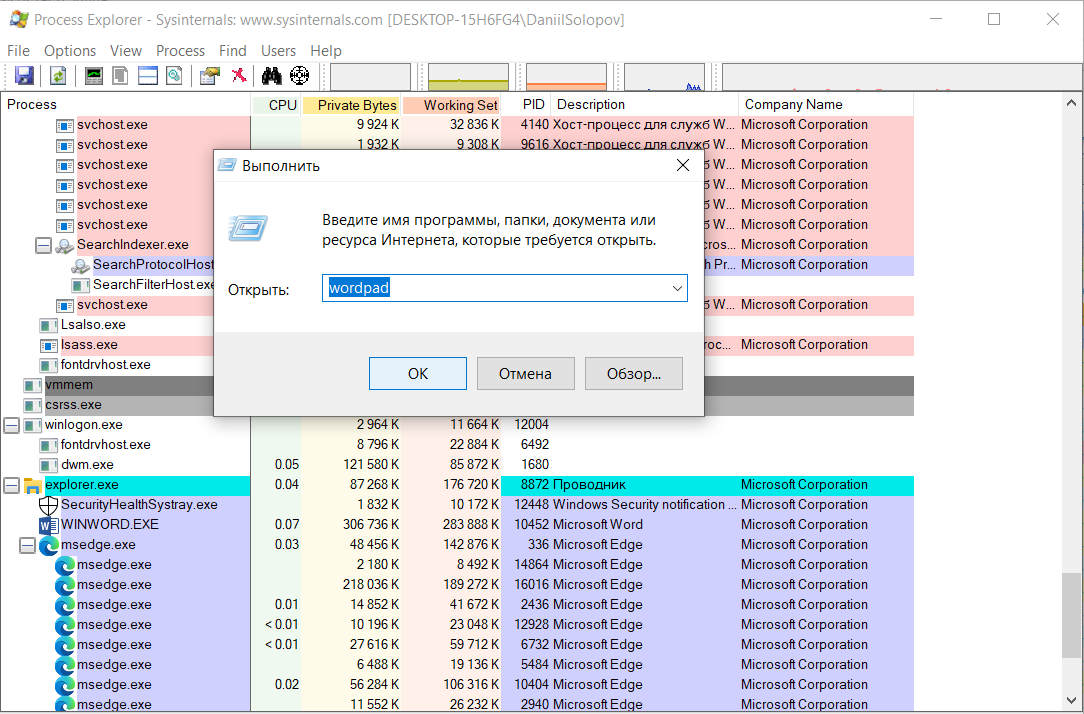


Рисунок 24 – Запуск приложения в Process Explorer

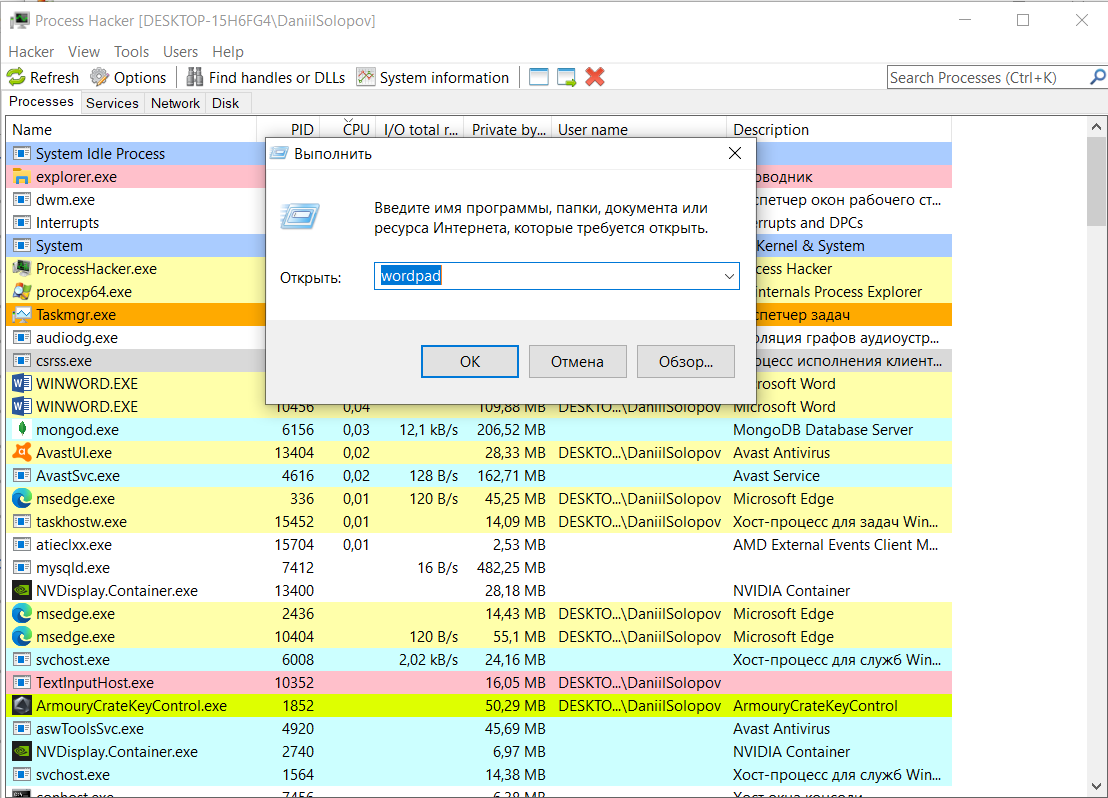


Рисунок 25 – Запуск приложения в Process Hacker

**Описание возникшего процесса по характеристике “определить используемые handles”:**

Для определения используемых handles нужно в Process Hacker выбрать пункт пользовательского меню Find handles or DLLs (Бинокль) и ввести в текстовое поле строку “wordpad”, в выведенном списке будет находится информация о всех используемых handles (см. рис. 26).

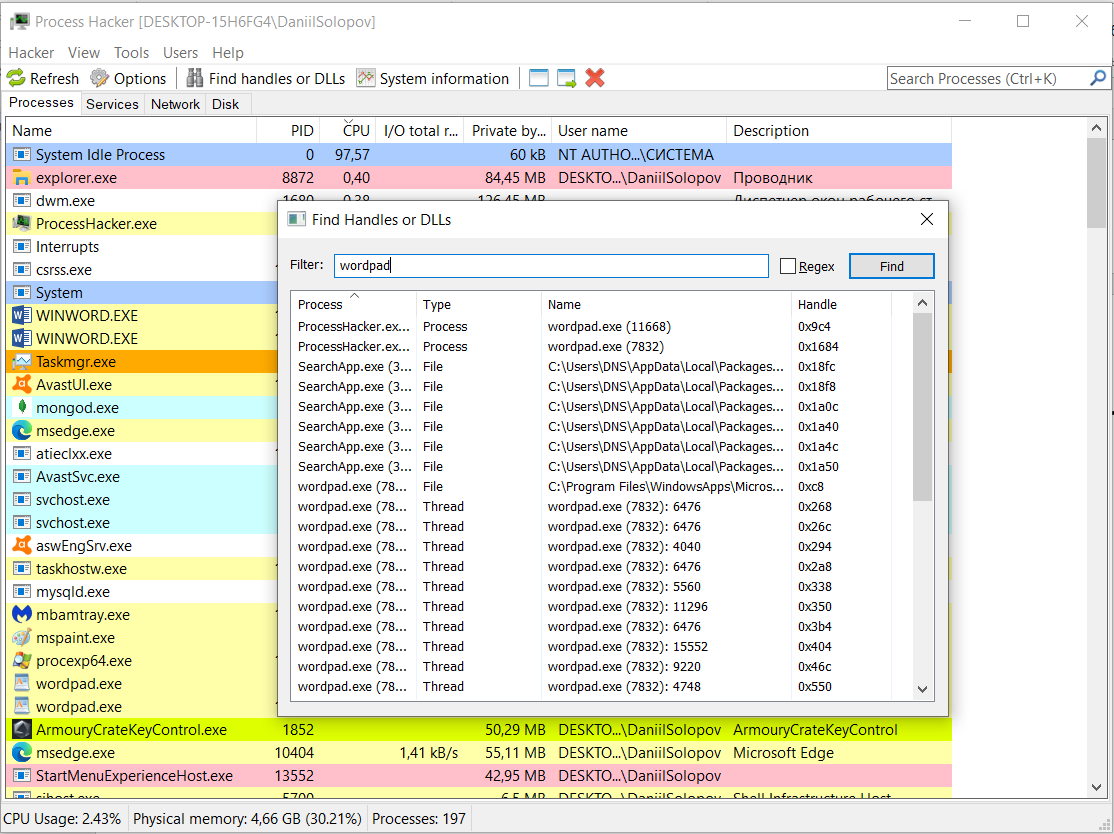


Рисунок 26 – Определение используемых handles

Для определения используемых handles приложения WordPad в Process Explorer необходимо нажать на кнопку пользовательского интерфейса Find Handle or DLL (Бинокль) или нажать на комбинацию клавиш CTRL + F и в текстовое поле написать строку “wordpad” (см. рис. 27).

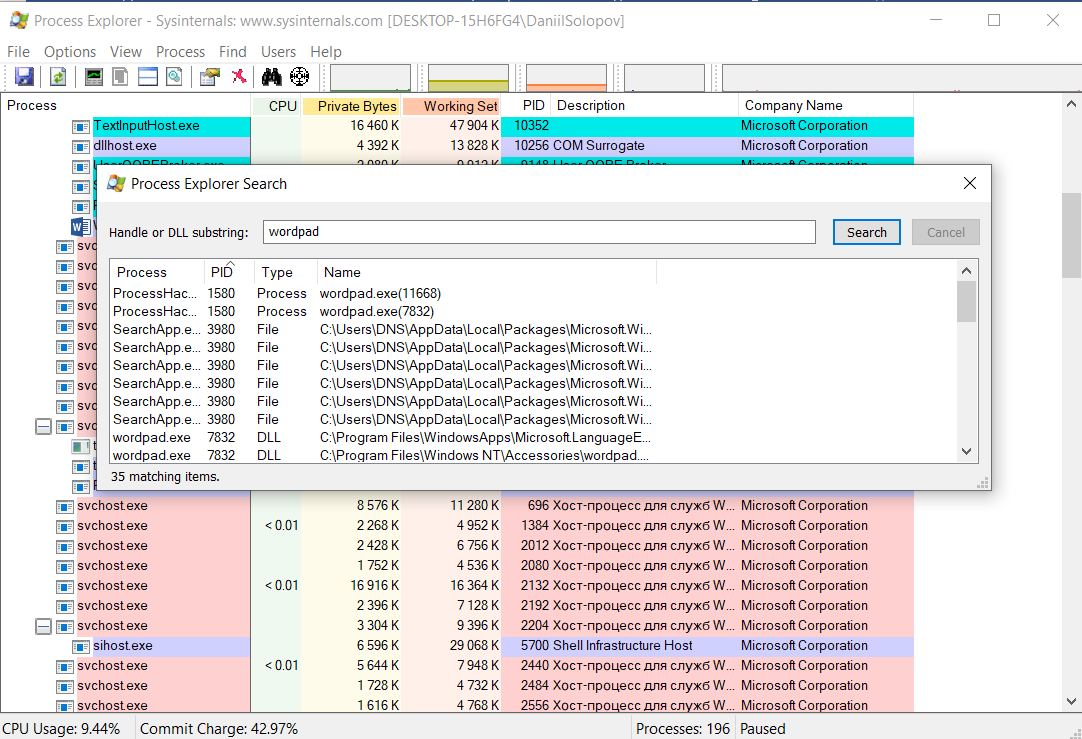


Рисунок 27 – Определение используемых handles

**Принудительно завершить указанный процесс:**

Для принудительного завершения процесса достаточно нажать на него в Process Hacker и нажать в выпадающем меню на кнопку Terminate (см. рис. 28).

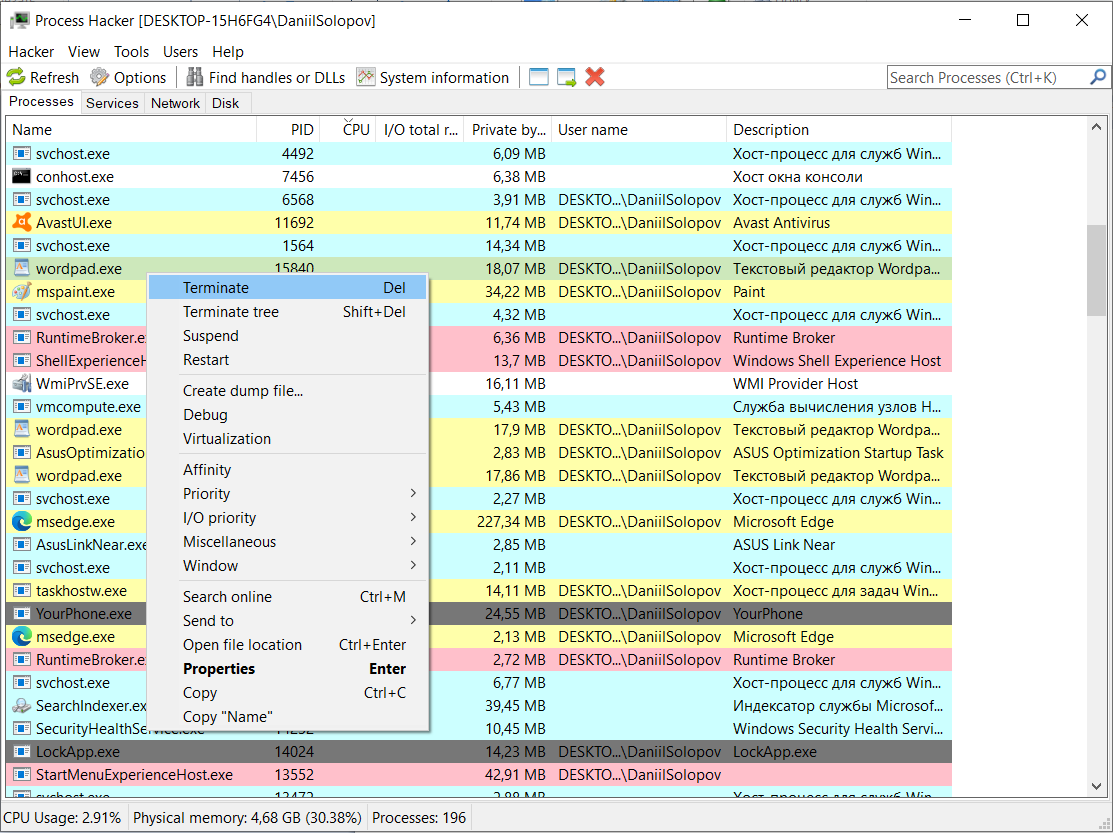


Рисунок 28 – Принудительное завершение процесса

В Process Explorer выполняются действия, аналогичные действиям в Process Hacker в данной ситуации, за исключением одного – нажимается кнопка Kill Process, а не Terminate.

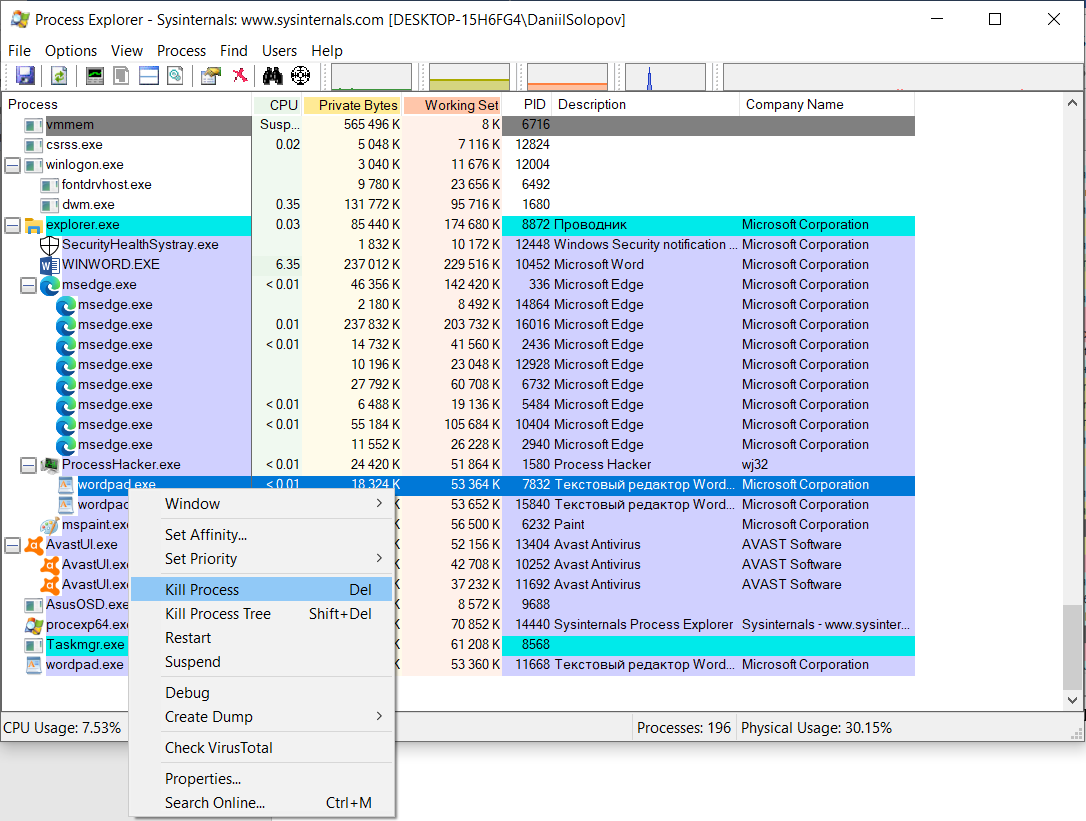


Рисунок 29 – Принудительное завершение процесса

**Описание различий в работе 3-х утилит (Диспетчер задач, Process Explorer, Process Hacker):**

Основное различие утилит состоит в интерфейсе – у Process Explorer и Process Hacker практически одинаковые интерфейсы, за исключением расположения тех или иных клавиш, вкладок и синонимичных названий (например, Kill Process и Terminate, при удалении процесса (см. рис. 28-29)), однако Диспетчер задач интерфейсом достаточно сильно отличается от Process Explorer и Process Hacker (см. рис. 30-32).

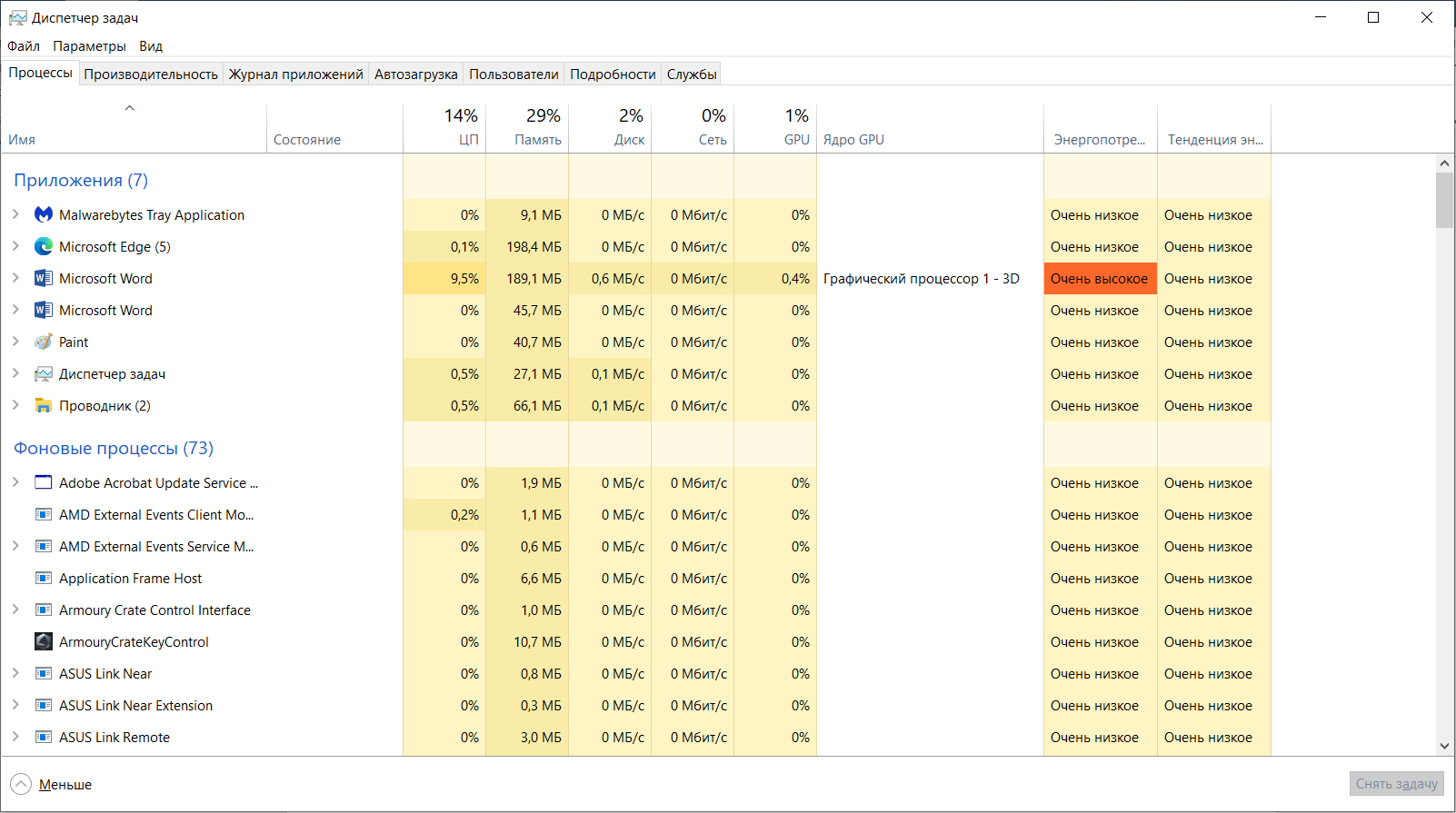


Рисунок 30 – Интерфейс утилиты Диспетчер задач

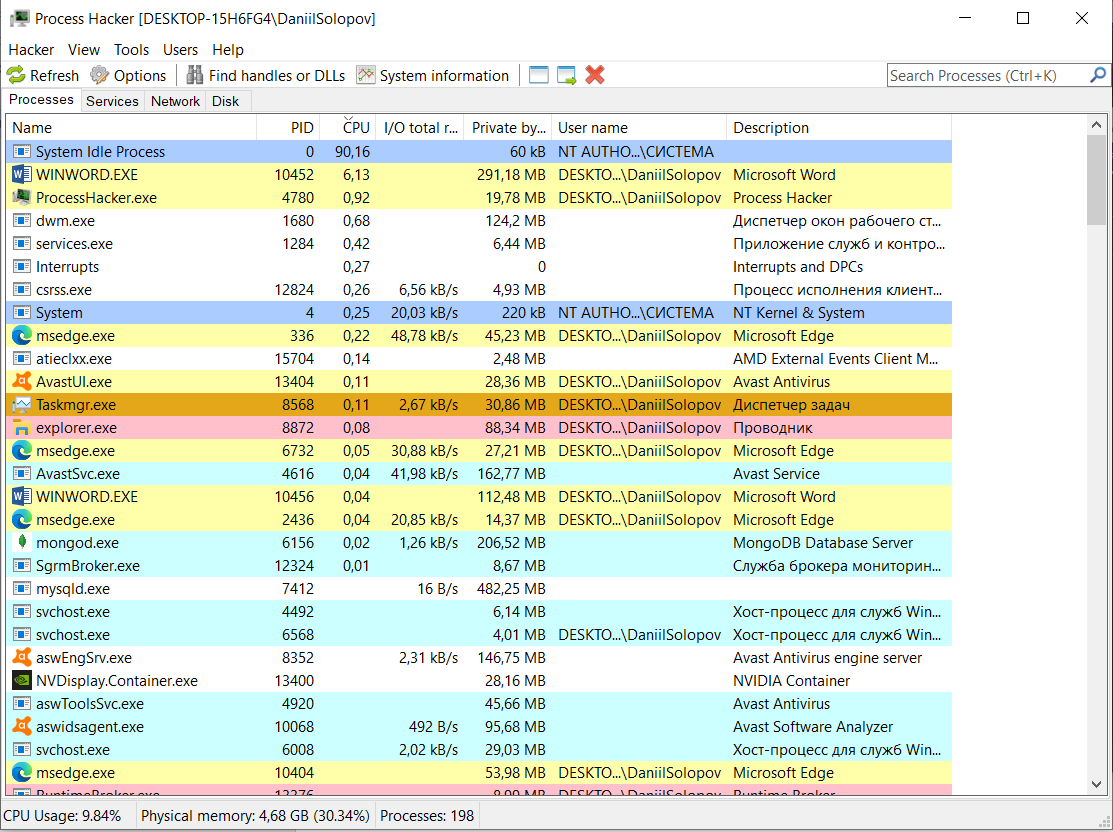


Рисунок 31 – Интерфейс утилиты Process Hacker

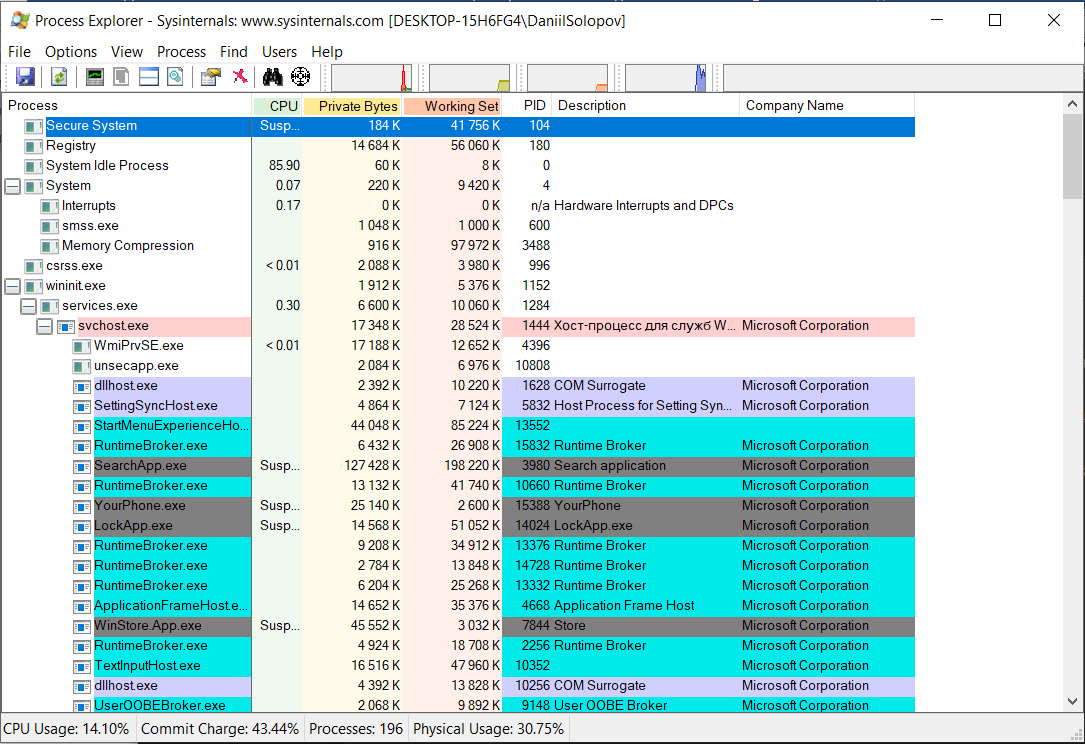


Рисунок 32 – Интерфейс утилиты Process Explorer

В Process Hacker при изменении состояний процессов меняется их положение в таблице, по этой причине возникает неудобство принудительного завершения процесса – для этого нужно сначала нажать клавишу Pause / Break, найти процесс и осуществить завершение процесса.

По функциональной составляющей утилиты сильно схожи, в особенности Process Hacker и Process Explorer, однако утилиты Process Hacker и Process Explorer предоставляют удобный интерфейс для решения задачи “определить используемые handles”, чем Диспетчер задач.

Вывод

Были изучены возможности контроля и управления процессами в операционных системах Windows, был получен опыт работы с Диспетчером задач, Process Explorer и Process Hacker.

Были решены поставленные задачи с помощью утилит, а также, основываясь на практике работы с утилитами, были указаны найденные различия между утилитами – в основном, различия касаются интерфейса самих утилит.