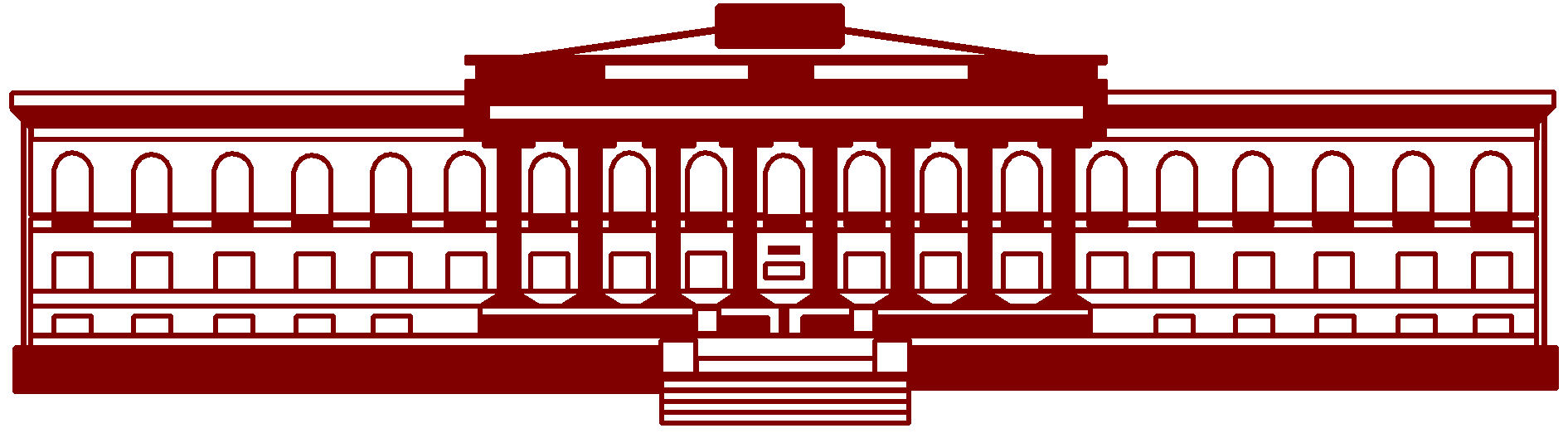
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**імені ТАРАСА ШЕВЧЕНКА**

****

**ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**Кафедра прикладних інформаційних систем**

**Звіт до лабораторної роботи №1**

**З курсу**

**«Безпека мереж і комп’ютерних систем»**

*студента 2 курсу*

*групи ПП-22*

*спеціальності 122 «Комп'ютерні науки»*

*ОП «Прикладне програмування»*

Шевлюк Вікторії Віталіївни

*Перевірив:*

д.т.н, професор

Сайко В. Г.

Київ 2022

**Тема:** Моніторинг поточного функціонування ОС WINDOWS

**Мета:** Дослідити функціональні можливості Диспетчера задач та

ознайомитися із альтернативними йому програмами.

**Завдання:**

**1.** Зареєструйтеся в операційній системі з правами адміністратора.

**2.** Створіть контрольну точку стану ОС на момент початку заняття.

**3**. Запустіть Диспетчер завдань.

**4**. Якщо запуск не заблокований, введіть заборону на нього, а також на

доступ до реєстру Windows за допомогою редактора локальної групової політики

**5.** Переконайтеся в неможливості перегляду процесів в середовищі ОС

Windows.

**6.** Розблокуйте запуск Диспетчера завдань і редактора реєстру.

**7.** Зробіть скріншот вставки "Процеси".

**8.** Зробіть необхідну кількість скріншотів вставки "Процеси" .для того,

щоб отримати повний список всіх процесів.

**9.** Зробіть скріншот вставки "Продуктивність" і проаналізуйте

отримані дані про використовувані ресурси ІС. Результати занесіть в протокол з лабораторної роботи.

**10.** За допомогою довідкових матеріалів проаналізуйте список і опишіть всі процеси (крім тих, що описані в розділі "Теоретичні відомості").

**11.** Дізнайтеся, як можна зіставити кожен процес файлу.

**12.** Зробіть аргументовані висновки для кожного процесу про

можливість його зупинки (завершення).

**13.** Знайдіть (якщо є) підозрілі процеси, що належать вірусам.

**14.** Виконайте відключення підозрілих і другорядних процесів і знову

зробіть скріншот вставки "Процеси".

**15.** Порівняйте дані зі скріншотом з пункту 7 і поясніть отриманий

ефект. Занесіть свої висновки в протокол.

16. По черзі досліджуйте, які додаткові можливості надають програми,

альтернативні Диспетчер завдань:

• TaskManagerEx2;

• Process Explorer

• Process Hacker

• System Explorer

• Daphne v2.04

• Sysinternals Process Explorer v.12.04;

• PROWiSe Manager;

• Anvirrus.exe;

• Task Manager

• KillProcessSetup.exe

• TaskCounterSetup.exe

17. Результати досліджень занесіть в протоколи.

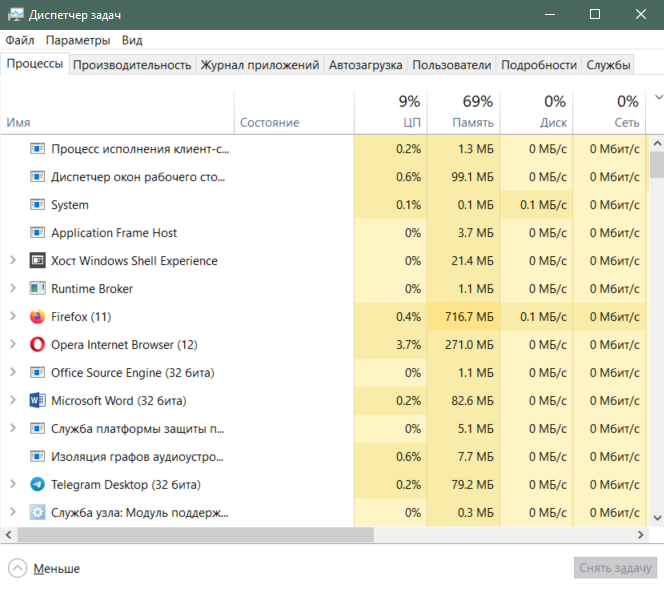
18. За вказівкою викладача проведіть більш детальні дослідження однієї з перших 6 з перерахованих програм зі складанням інструкції по роботі з даною програмою

**Хід роботи:**

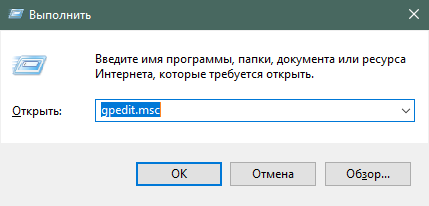
**1)**  Реєструємось в ОС з правами адміністратора – у мене були права адміністратора за замовчуванням:



**2)** Відкриваємо диспетчер задач за допомогою комбінації клавіш Ctrl+Shift+Esc та фіксуємо контрольну точку стану ОС до початку нашої роботи:



**3)** Оскільки доступ до диспетчера не заблокований, я його заблокую (а також доступ до реєстру) за допомогою редактора локальної групової політики:



Заходжу в редактор локальної групової політики та виконую наступні дії:

В розділі "Конфігурація користувача" переходжу в підрозділ

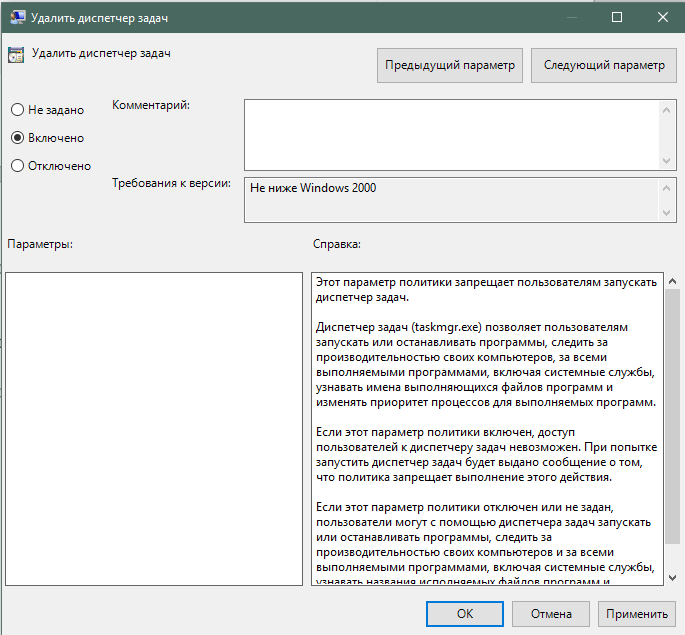
"Адміністративні шаблони";

Далі в пункті "Система" обираю підпункт "Варіанти взаємодій після

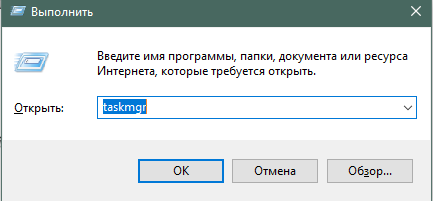
натискання Ctrl+Alt+Del";

Для параметру "Видалити диспетчер задач" встановлюю значення

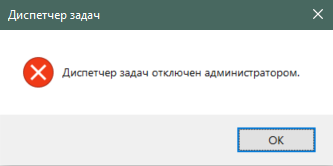
"Включено" – щоб заблокувати та натискаю ОК:



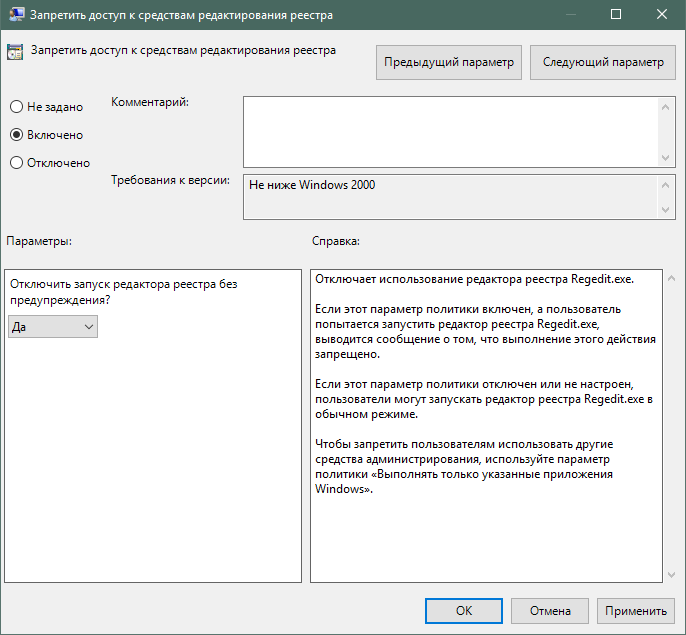
Тепер при спробі зайти в диспетчер натискаючи Ctrl+Shift+Esc нічого не відбувається. Спробуємо зайти в диспетчер іншим способом:



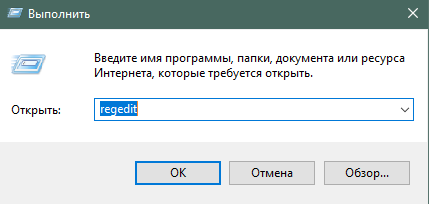
В результаті бачимо таке вікно:

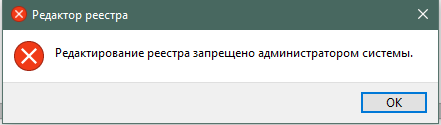


Тепер заблокуємо редагування реєстру:



Перевіримо чи зможемо тепер ми зробити редагування реєстру:



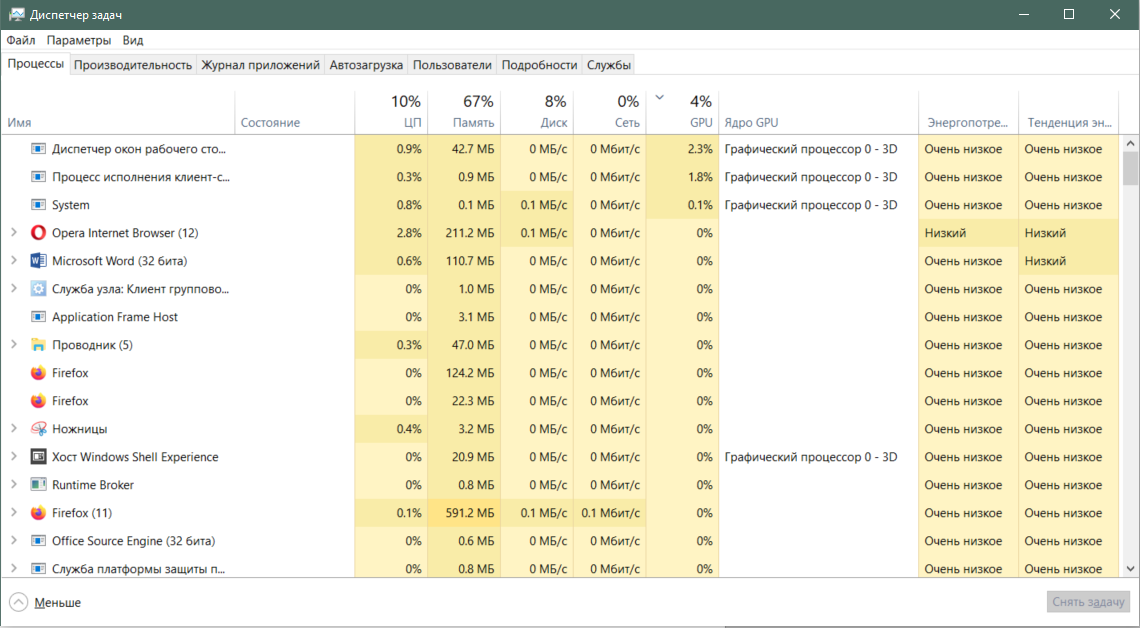


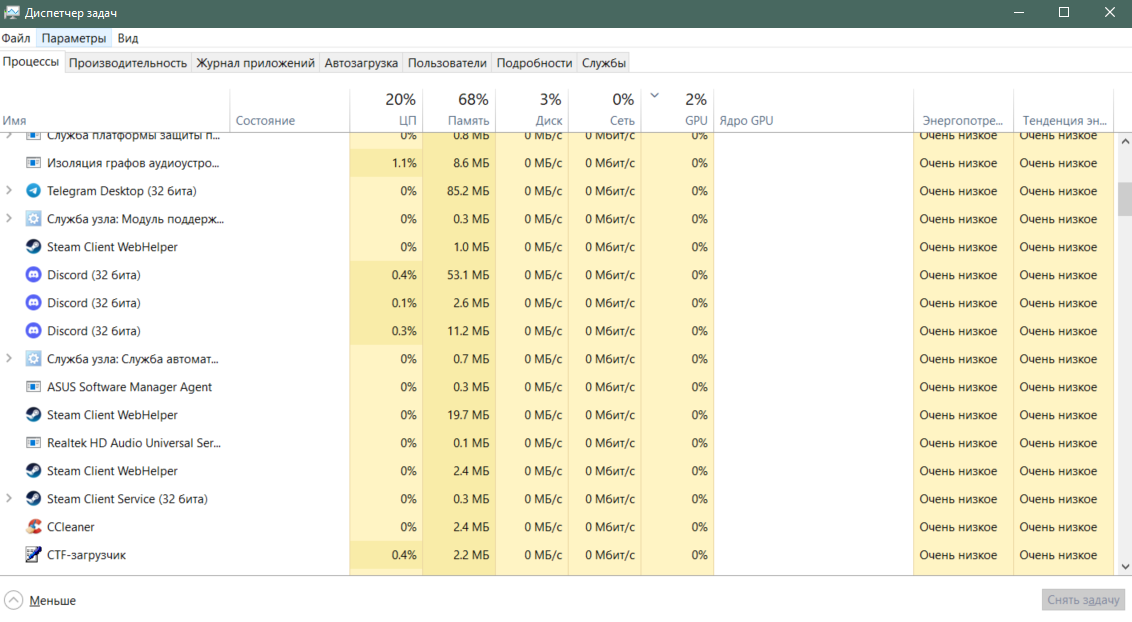
Як бачимо, доступ заблоковано.

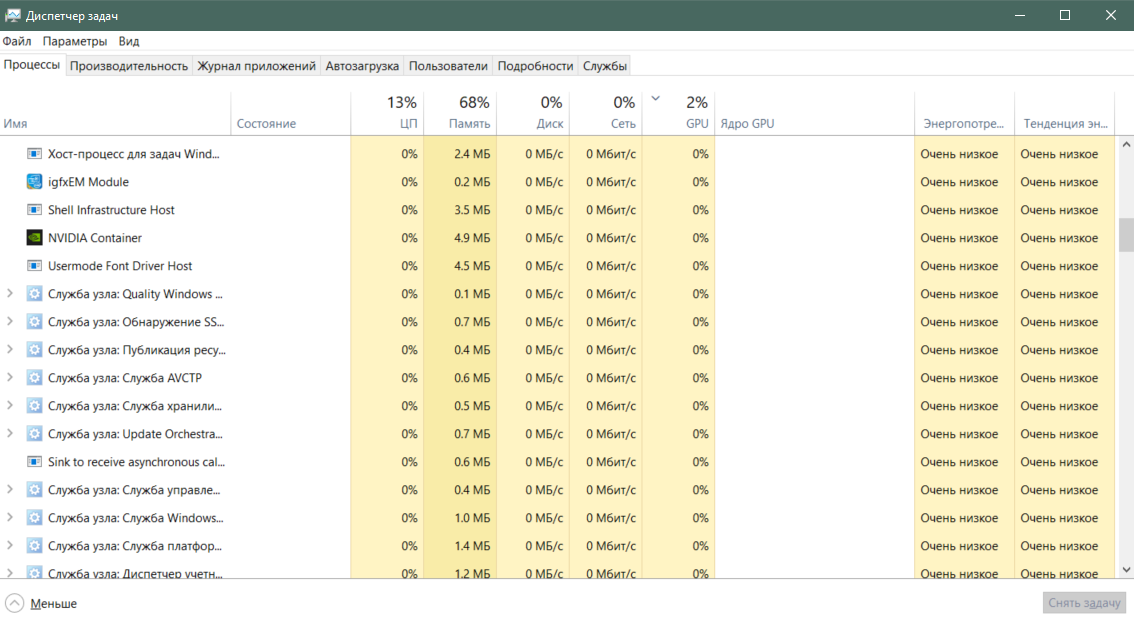
Тепер розблокуємо ці пункти встановивши в редакторі політики для них значення «не задано».

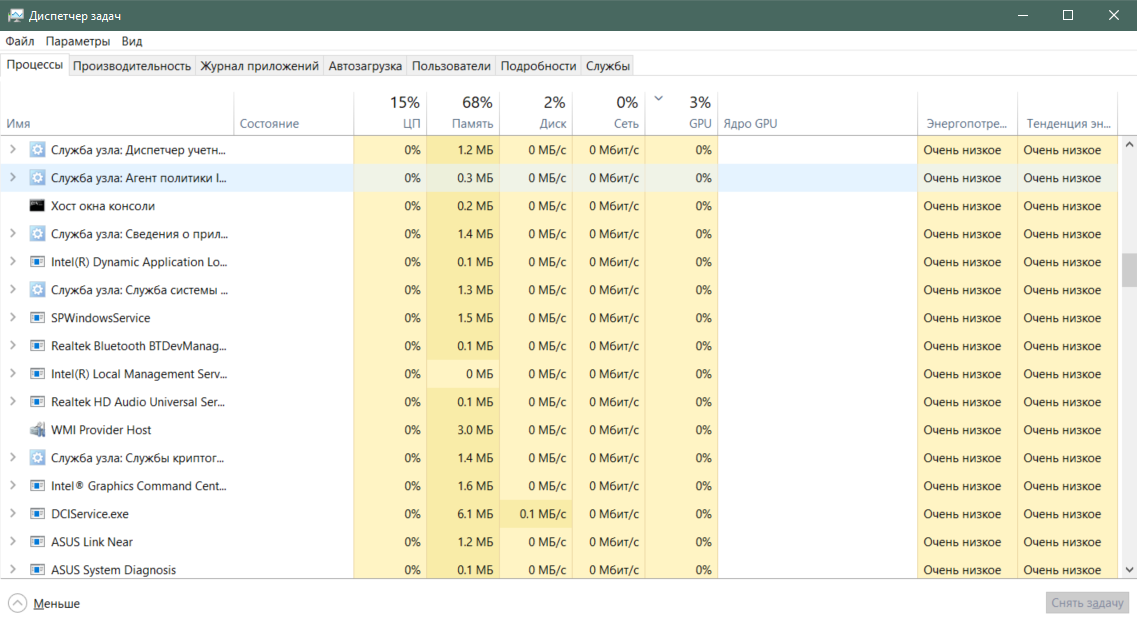
Продовжимо роботу в диспетчері задач.

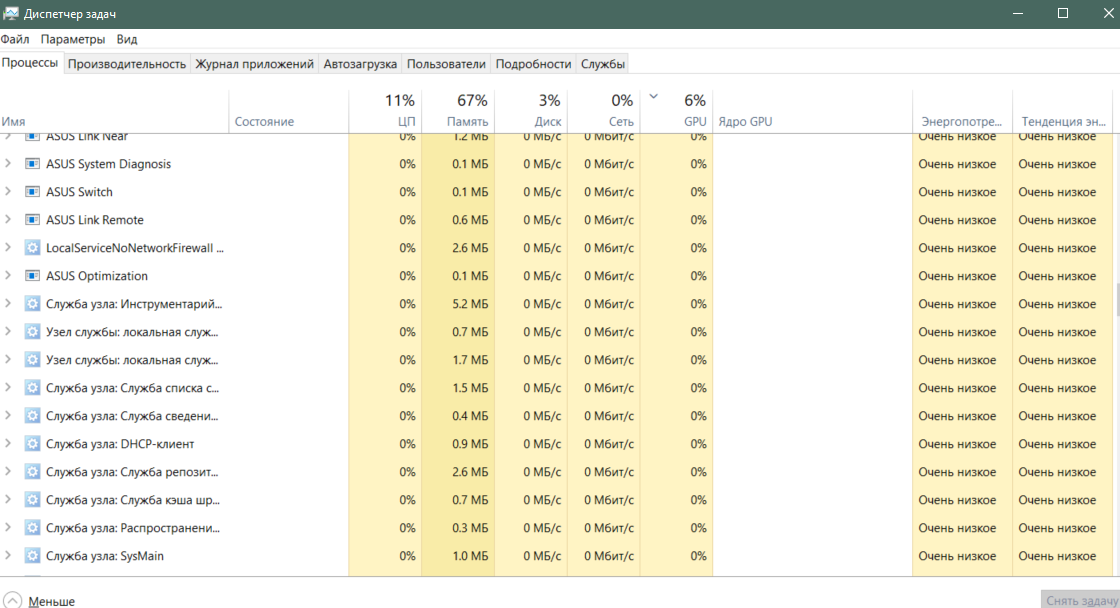
4) Подивимося на повний список процесів:

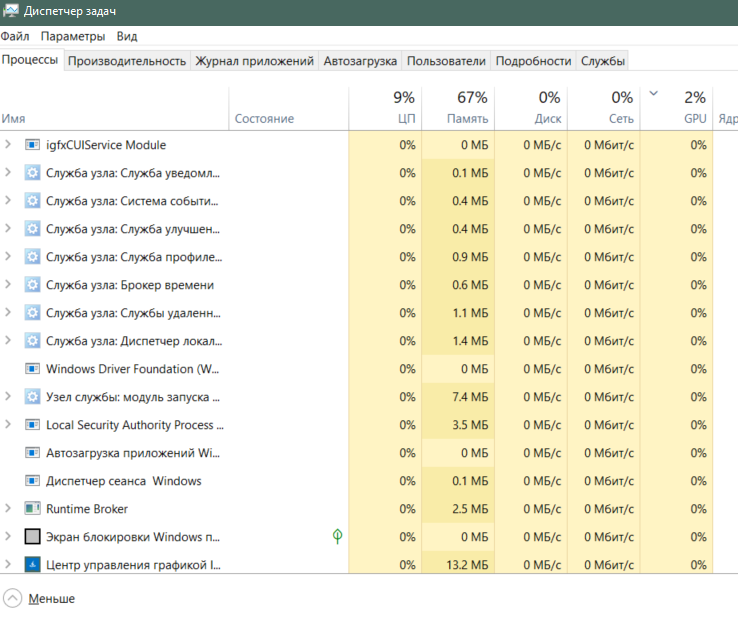


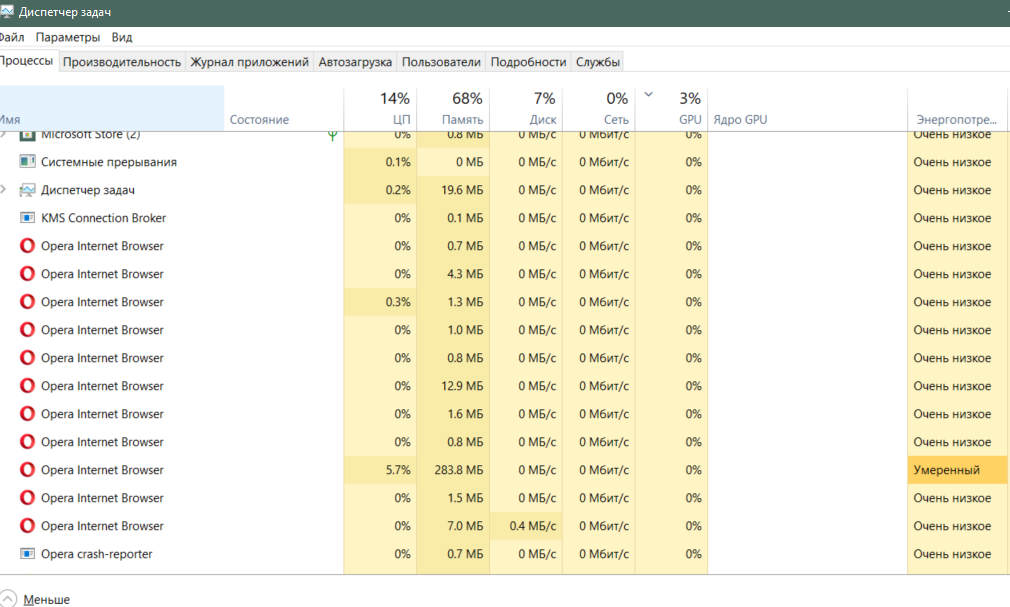


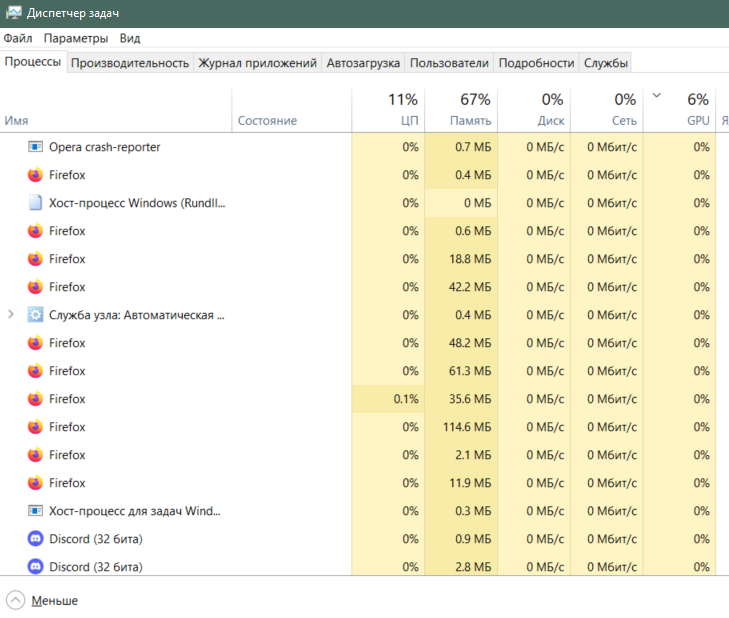


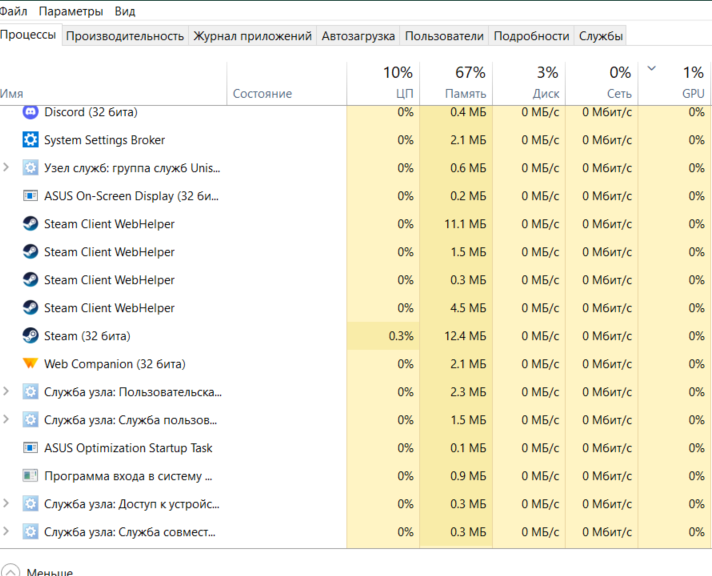


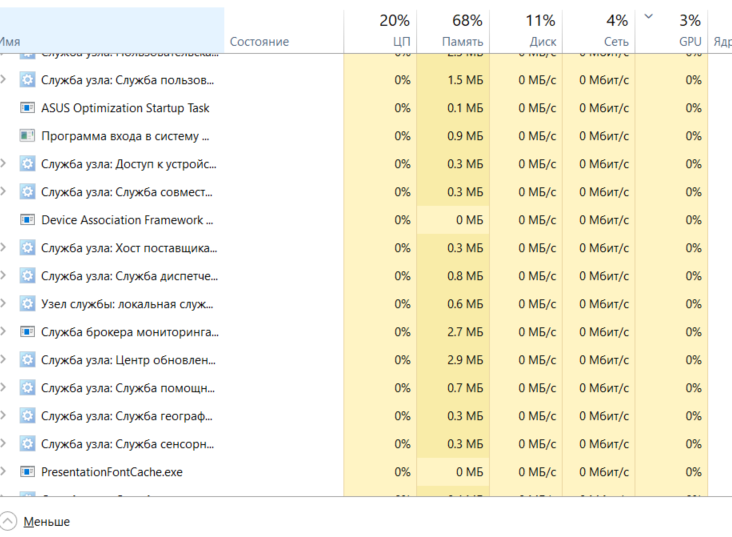


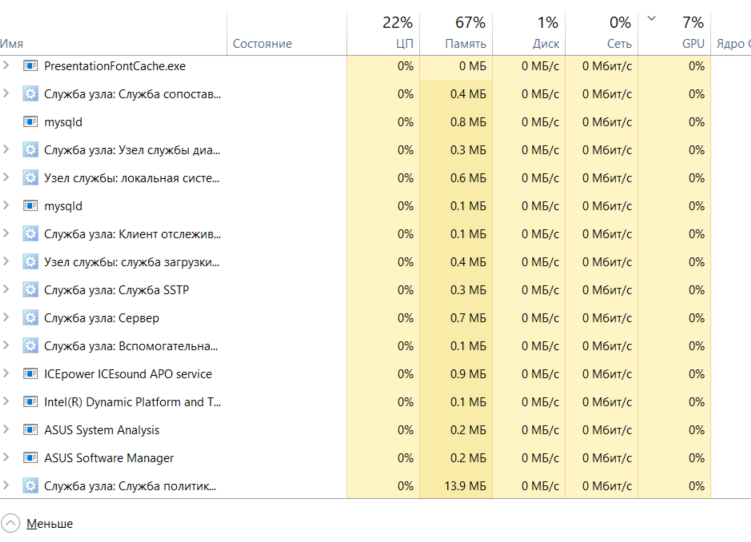


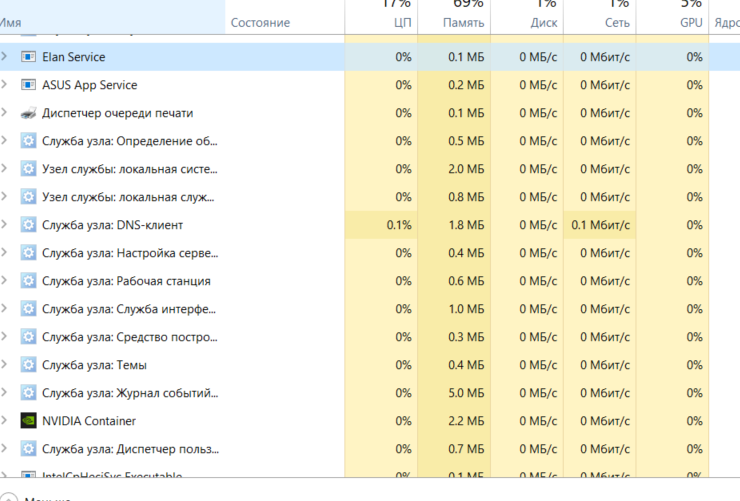


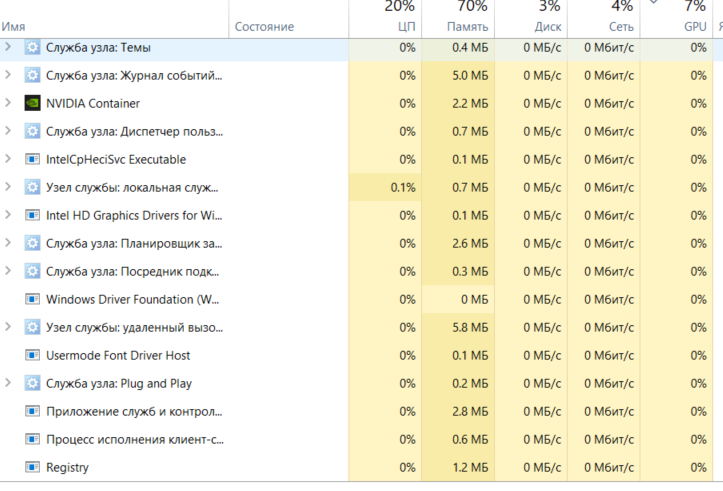




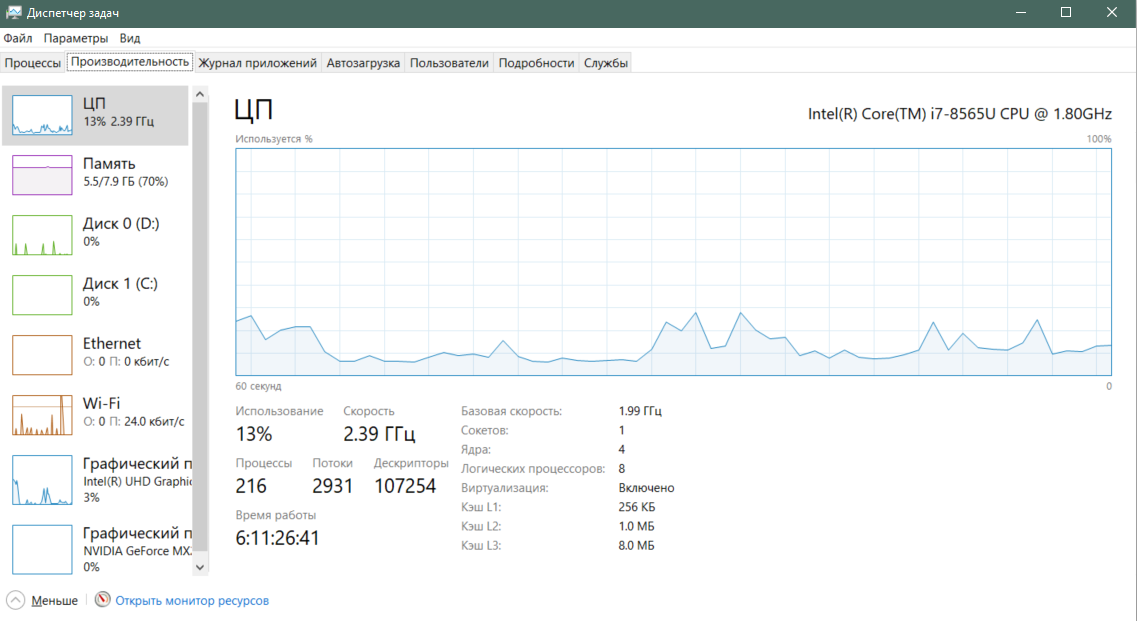








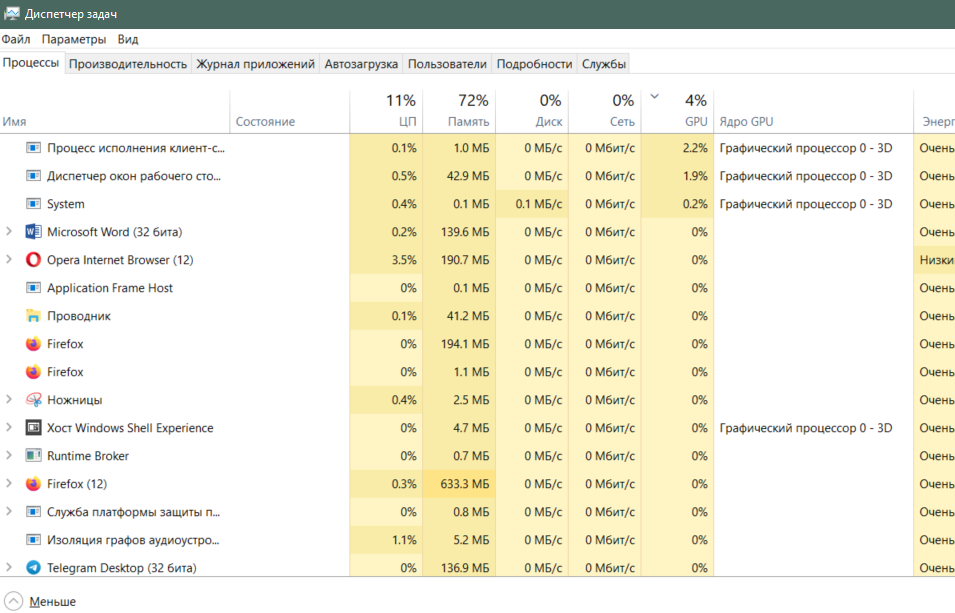
Тепер давайте поглянемо на продуктивність:



Є процеси, які не варто зупиняти, адже це може порушити роботу операційної системи або певних додатків. А є другорядні процеси, зупинення яких може допомогти оптимізувати розподіл ресурсів.

Переглянувши усі запущені процеси, я не знайшла особо підозрілих, і я не впевнена які з процесів – другорядні в даний момент, тому вирішила не зупиняти жоден процес. Проте, при необхідності, це завжди можна зробити (наприклад, якщо не вдається закрити якийсь додаток звичним шляхом – можна зупинити його процес через диспетчер задач).

Отже, стан ОС на кінець мого дослідження не змінився:



**Висновок:**

У ході виконання даної лабораторної роботи ми визначили призначення стандартної системної утиліти «Диспетчера задач». Дана програма використовується для: виводу переліку всіх працюючих додатків і перемикатися між ними, перегляду даних про всі запущені в системі процесах, тимчасової або повної зупинки або запуску процесів, управління роботою стандартних служб ОС Windows, отримання інформації про споживання ресурсів ІС в цілому і кожним процесом, контролю завантаження мережевих підключень, управління активними користувачами ІС та здійснення зупинки роботи операційної системи.

Окрім цього, ми визначили, що «Диспетчер задач» може бути вимкнений у деяких ситуаціях, наприклад адміністратором для попередження несанкціонованого втручання у роботу важливих процесів. Для його розблокування чи заблокування потрібно потрапити до «Редактора локальної групової політики», де у секції «Варіанти взаємодій після натискання Ctrl+Alt+Del» на параметрі «Видалити Диспетчер задач» ставимо потрібний нам статус «Увімкнуто» для заблокування та «Не задано» для розблокування. Аналогічно можливо зробити й для редактору реєстру.

Також ми ознайомились зі структурою «Диспетчера задач» та визначили, що він має 7 вкладок, серед яких: процеси (демонструє різні системі процеси та їх процеси, а також їх навантаження на процесор, ОЗУ, диск і мережу), продуктивність (відображає навантаження на центральний процесор, оперативну пам’ять, жорсткий диск та мережу у вигляді графіків.), журнал додатків (у цій вкладці фіксується активність кожного додатку.), автозавантаження (тут можна налаштувати ті програми, які завантажуються за замовчуванням при увімкнені ПК), користувачі (Відображає список всіх користувачів, котрі працюють на даному ПК, а також переглянути, скільки ресурсів «споживає» кожен із них.), деталі ( у стовпцях таблиці відображаються ідентифікатори процесів, стан, ім’я користувача, який його запустив і т. д.), служби (відображає список служб, їх стан, ID та опис).

**Контрольні питання:**

**1. Поясніть, навіщо необхідно здійснювати контроль та оптимізацію**

**ресурсів ІС.**

Контроль та оптимізація ресурсів ІС необхідні для того, щоб при потребі мати змогу збільшити швидкість та якість роботи системи, а також захистити її від шкідливих процесів

**2. Перелічіть основні функціональні можливості «Диспетчера задач».**

Утиліта Диспетчер завдань (Task Manager) дозволяє нам:

• виводити перелік всіх працюючих додатків і перемикатися між ними;

• переглядати дані про всі запущені в системі процесах;

• тимчасово або повністю зупиняти або запускати процеси, змінювати їх

пріоритет;

• управляти роботою стандартних служб ОС WINDOWS;

• отримувати інформацію про споживання ресурсів ІС в цілому і кожним

процесом;

• контролювати завантаження мережевих підключень;

• управляти активними користувачами ІС;

• здійснювати зупинку роботи операційної системи.

**3. Поясніть, навіщо системні адміністратори блокують «Диспетчер**

**задач» для користувачів.**

Системні адміністратори блокують запуск користувачами Диспетчера завдань для того, щоб вони не могли самостійно переглядати і управляти процесами ОС Windows.

**4. Перелічіть та охарактеризуйте кожну із вкладок «Диспетчера задач».**

►Вкладка Процеси (Processes). На цій вкладкі показує всі запущені додатки

і процеси, а також їх навантаження на процесор, ОЗУ, диск і мережу.

► Продуктивність (Performance). Відображає навантаження на

центральний процесор, оперативну пам’ять, жорсткий диск та мережу у вигляді графіків. На цій же вкладкі можна дізнатися точну модель процесору, диску, мережевого адаптеру, об’єм ОЗУ.

► «Журнал додатків». В цій вкладці фіксується активність кожного

додатку. Тут можна побачити, скільки часу витратив ЦП на виконання

інструкцій окремого додатку та скільки даний додаток «спожив» Інтернету.

► «Автозавантаження». Тут можна налаштувати ті програми, які

завантажуються за замовчуванням при увімкнені ПК і цим сповільнюють його роботу.

► «Користувачі». Відображає список всіх користувачів, котрі

працюють на даному ПК, а також переглянути, скільки ресурсів «споживає»

кожен із них.

► «Деталі». Ця вкладка, як і вкладка «Процеси», показує список

запущених процесів. В стовпцях таблиці відображаються ідентифікатори

процесів, стан, ім’я користувача, який його запустив, навантаження на ЦП, ОЗУ і короткий опис процесу.

► «Служби» відображає список служб, їх стан, ID і опис.

Дозволяє швидко зупинити або запустити необхідну службу.

**5. Для вирішення яких проблем призначена вкладка «Користувачі»?**

Вкладка «Користувачі» дозволяє нам зробити наступні дії:

• Перевірити список зареєстрованих користувачів

• Завершити реєстрацію користувача

• Відключити користувача (сеанси і додатки

залишаються запущеними)

• Перевірити, скільки ресурсів використовує кожен Споживач

Отже, за допомогою цієї вкладки можна вирішити проблеми пов’язані з керуванням користувачів і ресурсів, які вони використовують

**6. Що таке «процес» за стандартом ISO 9000: 2000?**

Стандарт ISO 9000: 2000 Definitions визначає процес як сукупність

взаємозв'язаних і взаємодіючих дій, що перетворюють вхідні дані в вихідні.

**7. Яким чином можуть маскуватися віруси?**

Частина вірусів маскуються під відомі системні процеси, приймаючи

співзвучні назви. Багато віруси приховують свою присутність в диспетчері завдань - вони

невидимі. Вбудований в Windows, власний Диспетчер завдань мало

інформованих і прихованих процесів не показує.