**ПРАКТИЧНА РОБОТА №3 Тема: Захист комп’ютера від вірусів**

Мета: Практично закріпити знання та вміння виконання антивірусної

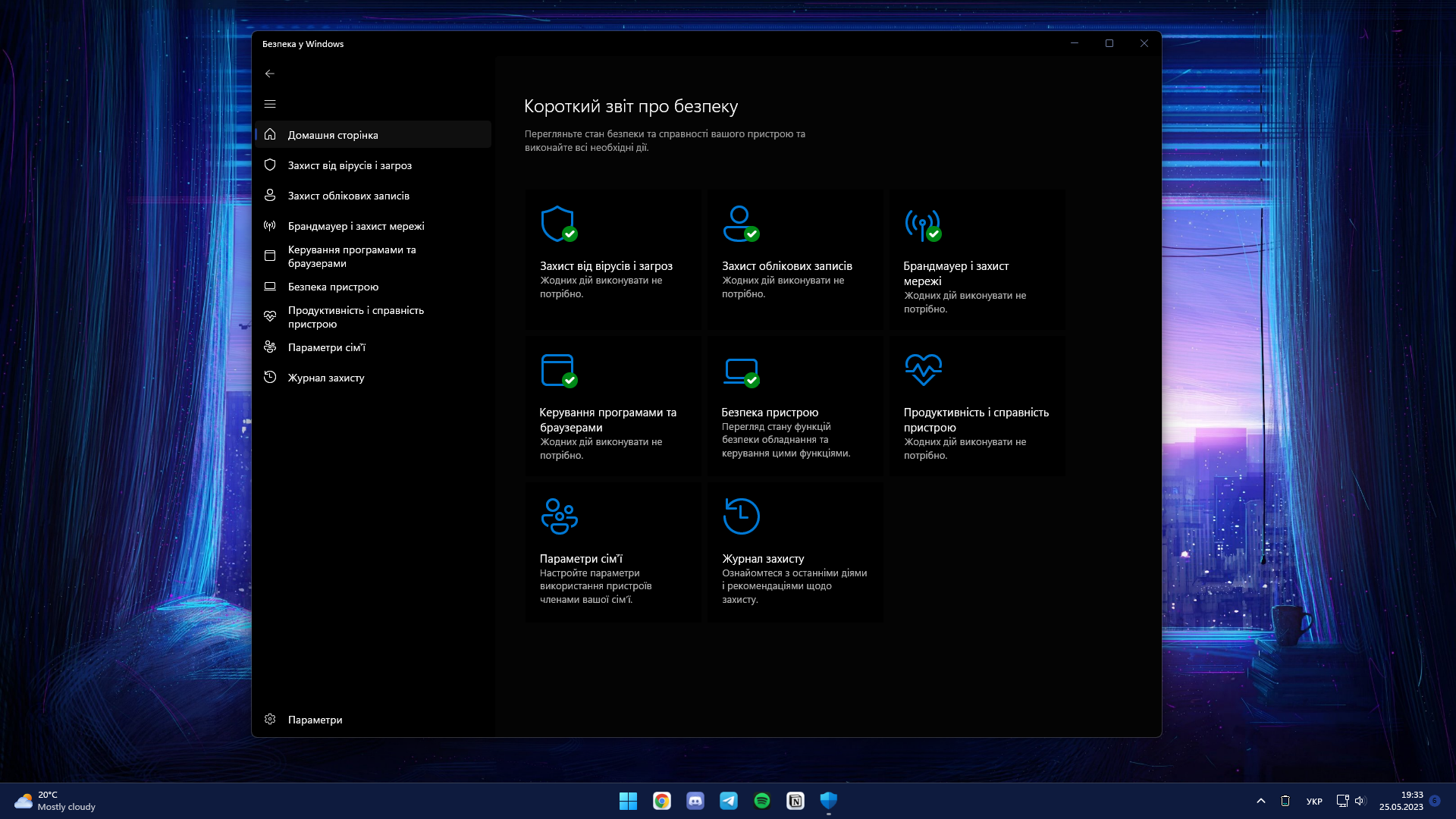
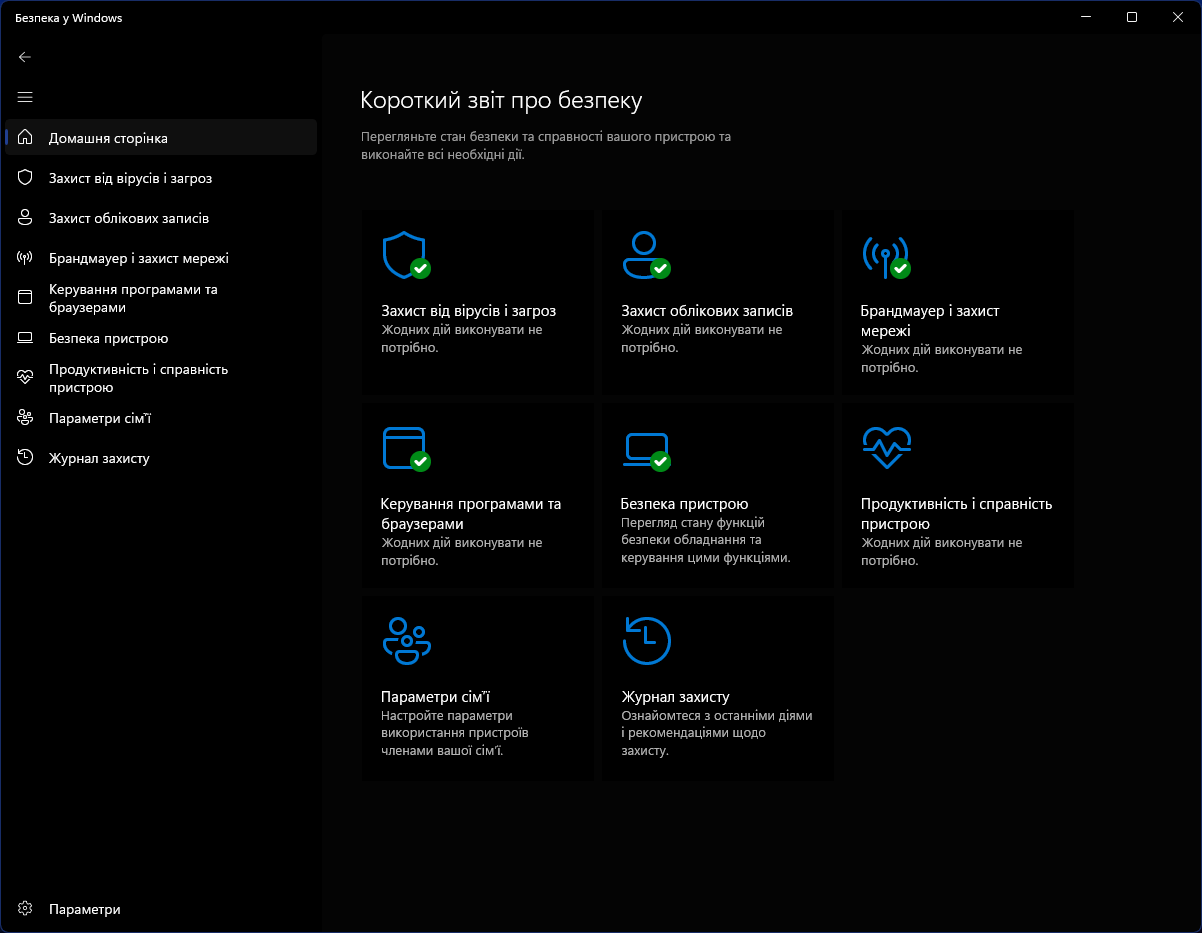
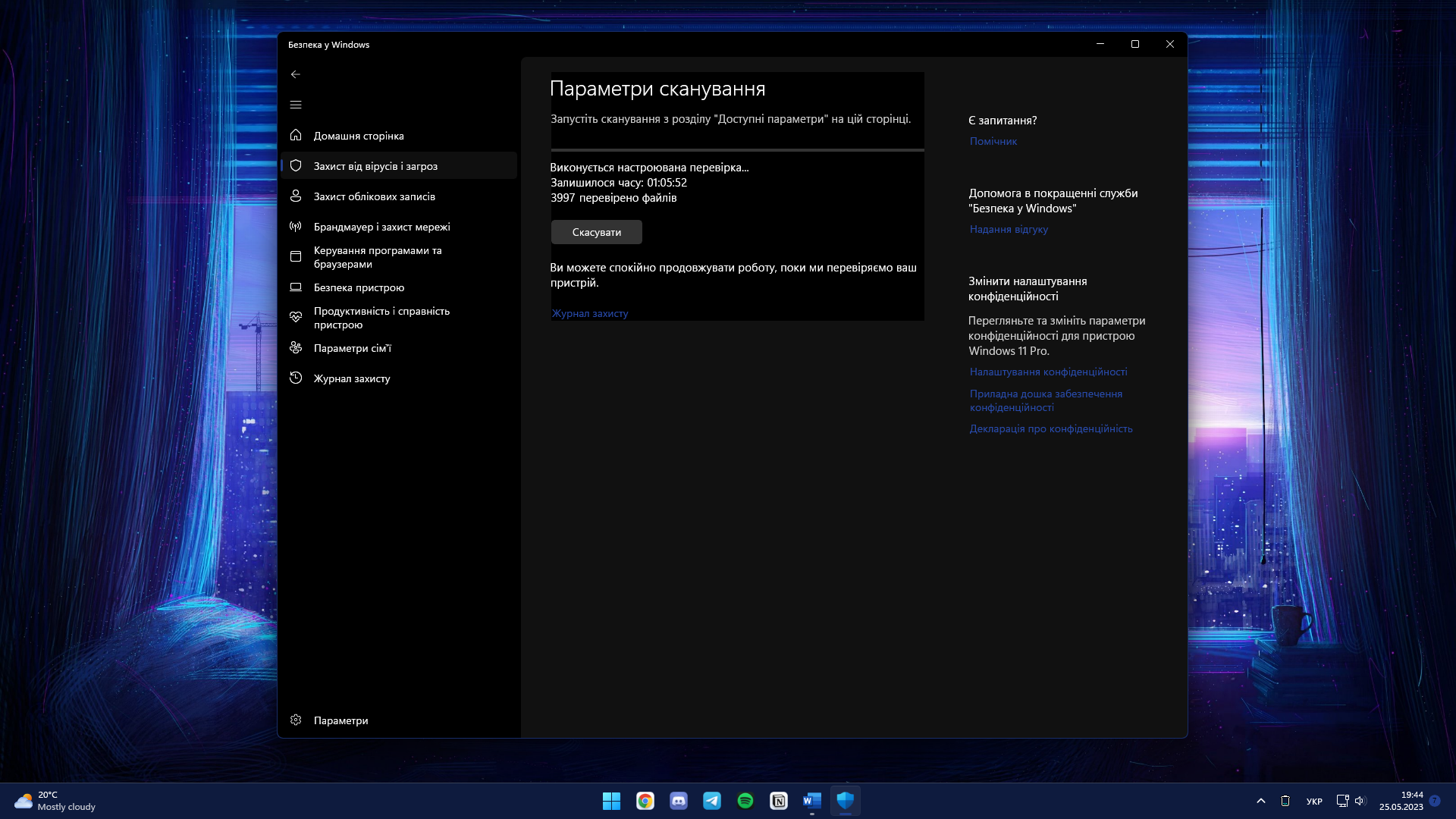
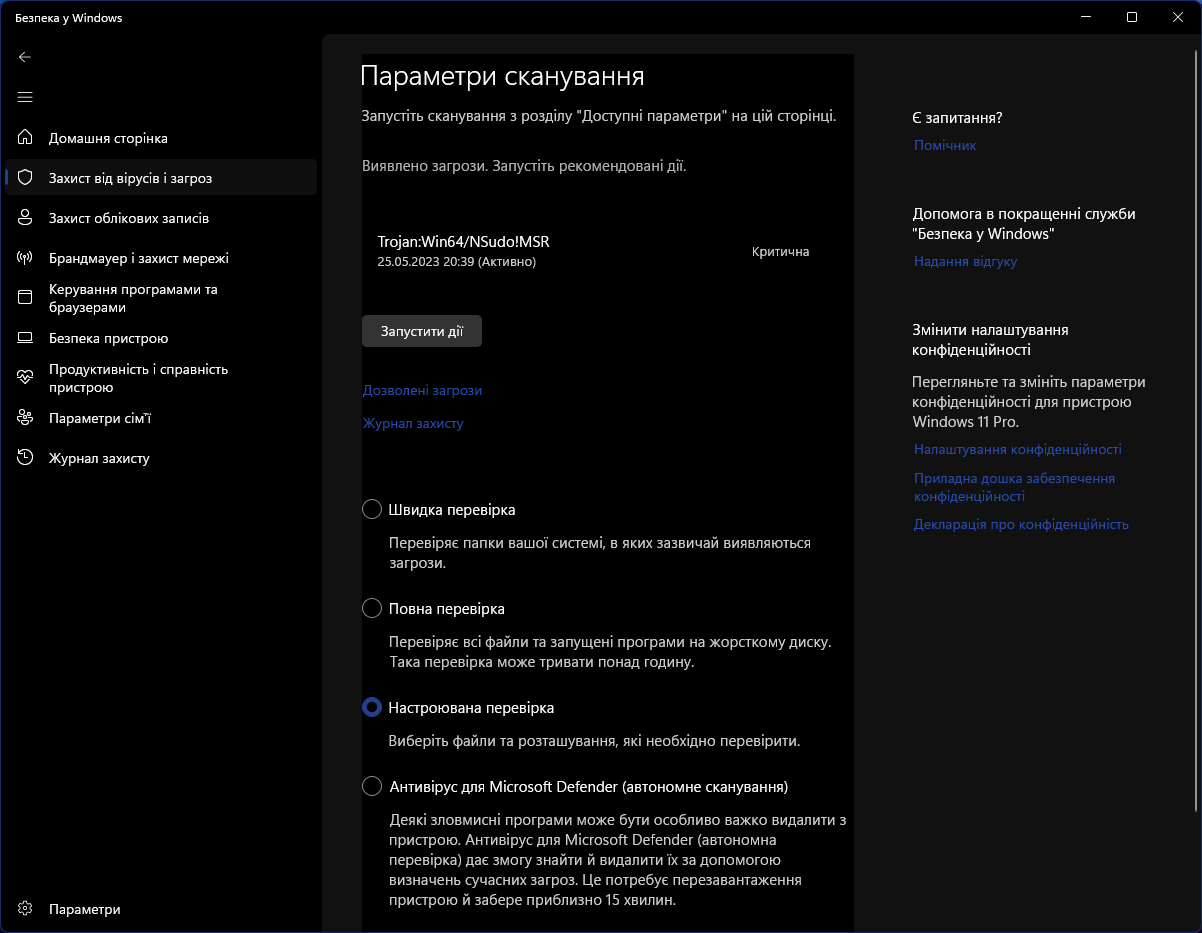
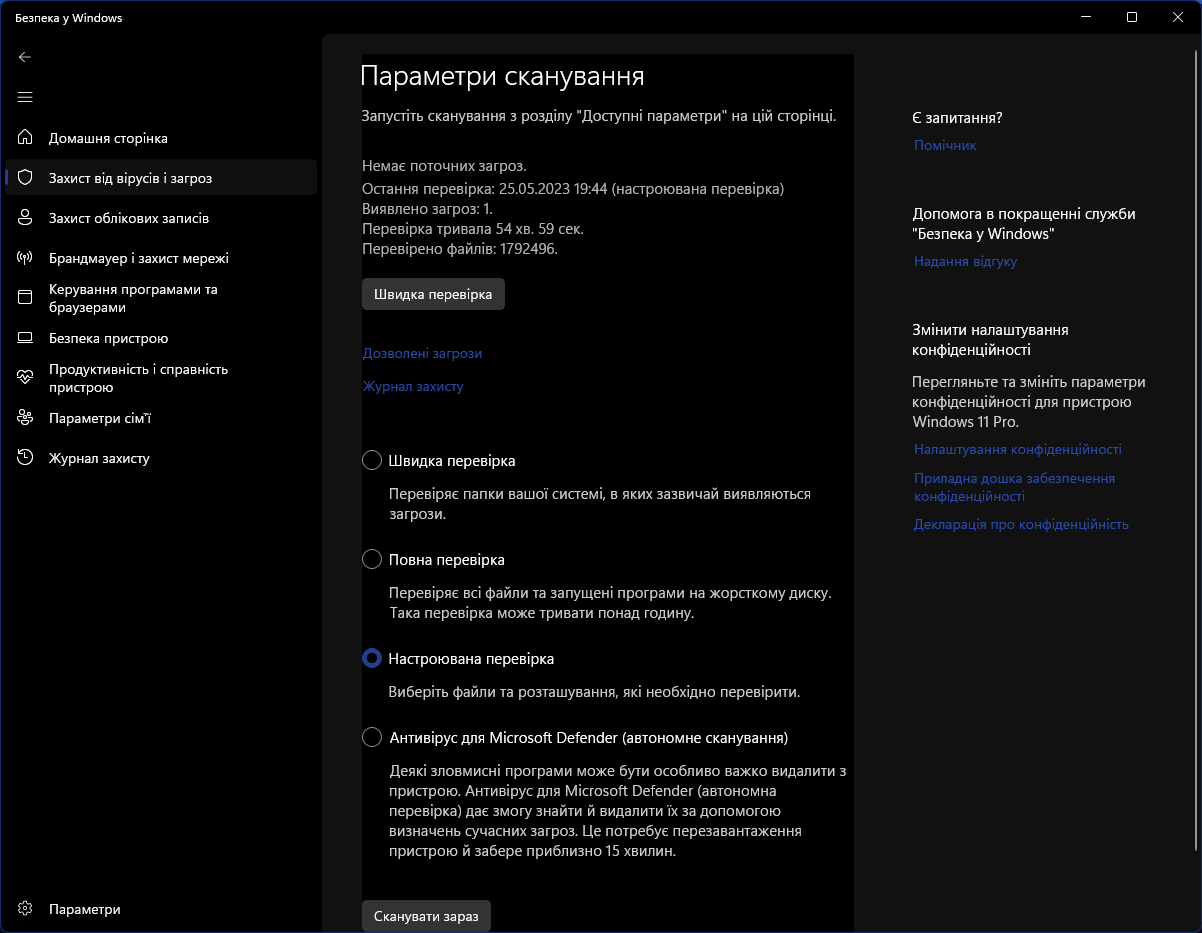
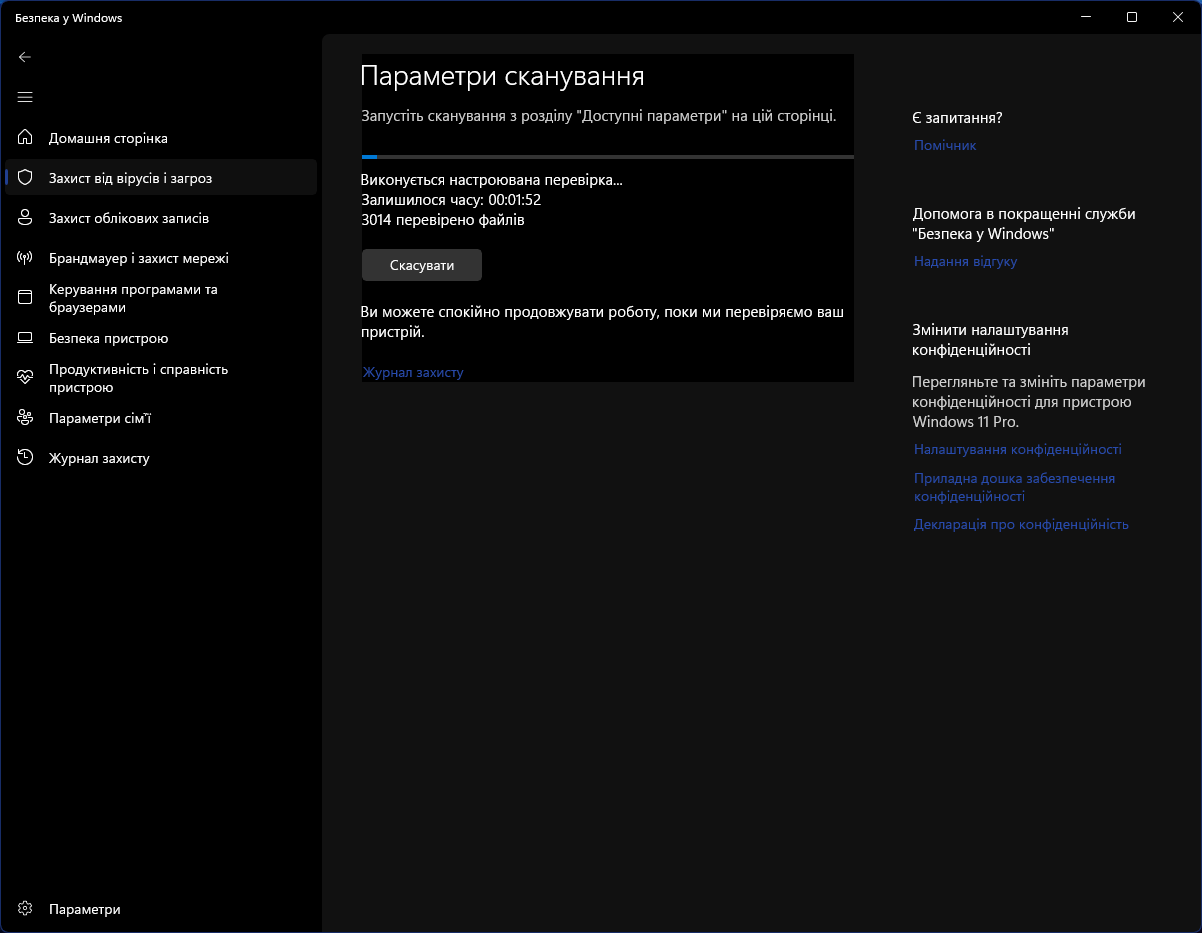
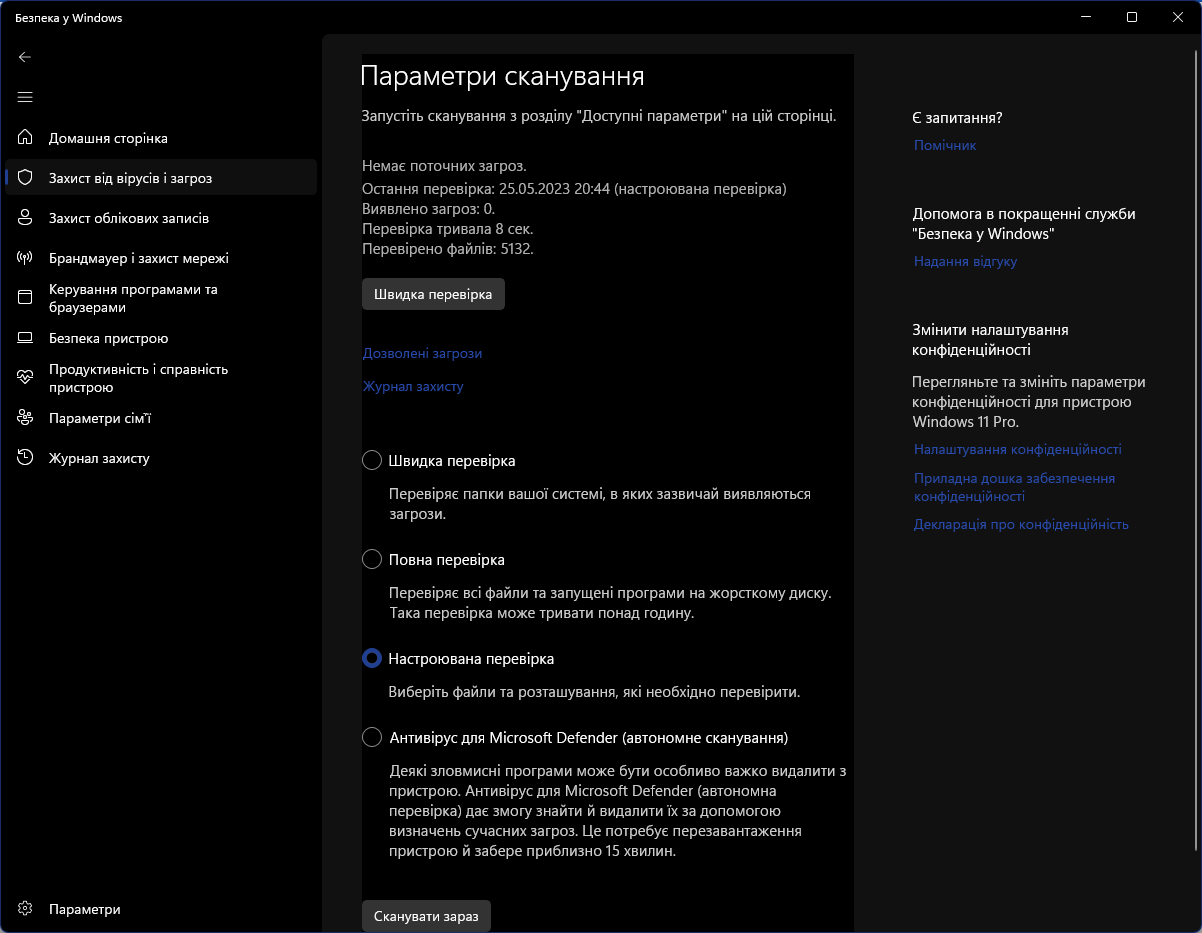
профілактики дисків та пам’яті ПК.

Обладнання: ПК.

ПЗ: Ос Windows, антивірусна програма.

Виконавець: Любченко Олег

Хід роботи

1. Запускаю антивірусну програму
2. Інтерфейс простий, функціонал розбитий на декілька вкладок, що дає змогу швидко віднайти те, що потрібно
3. Інформація, яку надає про себе програма:  
   Версія програми «Безпека у Windows»: 1000.25305.0.9000  
   Версія служби «Безпека у Windows»: 1.0.2303.28002-0  
   Версія клієнтської програми захисту від зловмисного ПЗ: 4.18.2304.8  
   Версія системи: 1.1.20300.3  
   Версія антивірусного ПЗ: 1.389.2374.0  
   Версія антишпигунського ПЗ: 1.389.2374.0  
     
   Додаткова інформація:  
   Строк завершення дії ліцензійного ключа: відсутній.  
   Дата виходу: 23 жовтня 2006  
   Стан захисту: активний.  
   Статус антивірусної бази: оновлюється.
4. Виконую сканування диску C  
   Результат:   
     
   Виконую сканування папки «Мої документи»  
     
   Результат: 
5. Під час сканування диску C було перевірено 1792496 файлів та виявлено одну потенційну загрозу у вигляді додатку для гри (подібні файли часто відзначають як віруси, адже вони проникають до процесів гри). Програма антивірус запропонувала три варіанти дій:  
   1. Видалити файл;  
   2. Перемістити його до карантину;  
   3. Дозволити на пристрої.  
   Під час сканування папки «Мої файли» було перевірено 5123 файли та не зафіксовано жодних загроз.
6. Питання:
7. Комп'ютерний вірус - це шкідлива програма, яка може самовідтворюватися та поширюватися, шкодити комп'ютерній системі, викрадати, пошкоджувати або знищувати дані.
8. Програми для боротьби з комп'ютерними вірусами називаються антивірусними програмами або антивірусами.
9. Віруси поділяються за рівнем небезпеки на низькоризикові, середньоризикові та високоризикові, в залежності від потенційних шкідливих наслідків.
10. Віруси поділяються за способом розповсюдження на віруси-приклади, що прикріплюються до виконуваних файлів, віруси-макроси, що використовують макроси в документах, та віруси-бомби, що активуються при виконанні певних дій.
11. Комп'ютерні віруси можуть виконувати різноманітні дії, такі як саморозповсюдження, руйнування або зміна даних, крадіжка конфіденційної інформації, сповільнення або збої в роботі системи та інші шкідливі дії.
12. Для профілактики ураження комп'ютерними вірусами рекомендується встановлювати надійний антивірусний захист, оновлювати програмне забезпечення та операційну систему, не відкривати сумнівні електронні повідомлення або вкладення, використовувати складні паролі та резервне копіювання даних.
13. Антивірусні програми можуть виявляти, блокувати та видаляти комп'ютерні віруси, проводити регулярні перевірки системи на наявність загроз, надавати захист у реальному часі та надсилати повідомлення про потенційні загрози.
14. Найбільш небезпечними діями вірусів можуть бути крадіжки конфіденційної інформації, адже наявність певних даних, наприклад паролів, може «розв’язати руки» цій програмі для більш небезпечних дій, таких як несанкціонований доступ до приватних даних.
15. На моєму домашньому комп'ютері встановлена антивірусна програма Windows Defender. Вона може працювати в таких режимах:
16. Реальний захист: Windows Defender постійно моніторить систему на наявність потенційних загроз, виявляє і блокує шкідливі програми або дії у реальному часі.
17. Сканування: Антивірусна програма може проводити швидке або повне сканування системи, перевіряючи файли, програми та пам'ять на виявлення вірусів та інших загроз.
18. Оновлення: Windows Defender регулярно оновлює свою базу даних вірусних визнаків, що дозволяє виявляти нові шкідливі програми та варіанти вірусів.

Особливість роботи Windows Defender полягає в тому, що вона є вбудованою антивірусною програмою у операційній системі Windows. Це означає, що вона автоматично встановлюється разом з операційною системою і забезпечує базовий рівень захисту без необхідності встановлення стороннього антивірусного програмного забезпечення. Windows Defender володіє достатньою функціональністю для виявлення, блокування та видалення більшості загроз, забезпечуючи базовий рівень захисту комп'ютера.

Висновок: під час виконання практичної роботи мені вдалося дізнатися деталі про антивірусне програмне забезпечення, яке встановлено на моєму комп’ютері, провести сканування системного диска комп’ютера на наявність вірусних загроз та навчитися антивірусній гігієні.