МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп’ютерної та програмної інженерії

Кафедра безпеки інформаційних технологій

**Технології забезпечення конфіденційності і цілісності інформаційних ресурсів**

**Лабораторна робота №5**

Тема Поняття антивірусної програми. Огляд найпоширеніших антивірусних програм та їх класифікація.

Тривалість заняття: 90 хв.

Київ 2023

**Тема:** Поняття антивірусної програми. Огляд найпоширеніших антивірусних програм та їх класифікація.

**Мета:** ознайомитися з поняттям антивірусної програми, розглянути методи антивірусного захисту, зробити огляд найпоширеніших антивірусних програм, їх структури та основних функцій.

**Теоретичні відомості**

Антивірусна програма (антивірус) — програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом.

Перші, найпростіші антивірусні програми з'явилися майже одразу після появи вірусів. Зараз розробкою антивірусів займаються великі компанії. Як і в творців вірусів, у цій сфері також сформувались оригінальні засоби — але вже для пошуку і боротьби з вірусами. Сучасні антивірусні програми можуть знаходити десятки тисяч вірусів.

Антивірусне програмне забезпечення складається з комп'ютерних програм, які намагаються знайти, запобігти розмноженню і видалити комп'ютерні віруси та інші шкідливі програми. З усіх методів антивірусного захисту можна виділити дві основні групи:

• Сигнатурні методи - точні методи виявлення вірусів, засновані на порівнянні файлу з відомими зразками вірусів

• Евристичні методи - приблизні методи виявлення, які дозволяють з певною вірогідністю припустити, що файл заражений.

Сигнатурою вірусу вважатиметься сукупність рис, що дозволяють однозначно ідентифікувати наявність вірусу у файлі (включаючи випадки, коли файл цілком є вірусом). Всі разом сигнатури відомих вірусів складають антивірусну базу.

Задачу виділення сигнатур, як правило, вирішують люди - експерти в області комп'ютерної вірусології, здатні виділити код вірусу з коду програми і сформулювати його характерні риси у формі, найбільш зручній для пошуку. Як правило - тому що в найбільш простих випадках можуть застосовуватися спеціальні автоматизовані засоби виділення сигнатур. Наприклад, у разі нескладних по структурі троянів або черв'яків, які не заражають інші програми, а цілком є шкідливими програмами.

Практично в кожній компанії, що випускає антивіруси, є своя група експертів, що виконує аналіз нових вірусів і поповнює антивірусну базу новими сигнатурами. З цієї причини антивірусні бази в різних антивірусах відрізняються. Проте, між антивірусними компаніями існує домовленість про обмін зразками вірусів, а значить рано чи пізно сигнатура нового вірусу потрапляє в антивірусні бази практично всіх антивірусів. Кращим же антивірусом буде той, для якого сигнатура нового вірусу була випущена раніше всіх.

Одна з поширених помилок щодо сигнатур полягає в тому,що кожна сигнатура відповідає рівно одному вірусу або шкідливій програмі. І як наслідок, антивірусна база з великою кількістю сигнатур дозволяє виявляти більше вірусів. Насправді це не так. Дуже часто для виявлення сімейства схожих вірусів використовується одна сигнатура, і тому вважати, що кількість сигнатур рівна кількості вірусів, що виявляються, вже не можна.

Важлива додаткова властивість сигнатур - точне і гарантоване визначення типу вірусу. Ця властивість дозволяє занести в базу не тільки самі сигнатури, але і способи лікування вірусу. Якби сигнатурний аналіз давав тільки відповідь на питання, є вірус чи ні, але не давав би відповіді, що це за вірус, очевидно, лікування було б не можливе - дуже великим був би ризик зробити не ті дії і замість лікування отримати додаткові втрати інформації.

Інша важлива, але вже негативна властивість - для отримання сигнатури необхідно мати зразок вірусу. Отже, сигнатурний метод непридатний для захисту від нових вірусів, оскільки до тих пір, поки вірус не потрапив на аналіз до експертів, створити його сигнатуру неможливо. Саме тому всі найбільш крупні епідемії викликаються новими вірусами. З моменту появи вірусу в мережі Інтернет до випуску перших сигнатур зазвичай проходить декілька годин, і весь цей час вірус здатний заражати комп'ютери майже безперешкодно. Майже - тому що в захисті від нових вірусів допомагають додаткові засоби захисту, розглянуті раніше, а також евристичні методи, використовувані в антивірусних програмах.

Якщо сигнатурний метод заснований на виділенні характерних ознак вірусу і пошуку цих ознак у файлах, що перевіряються, то евристичний аналіз ґрунтується на (вельми правдоподібному) припущенні, що нові віруси часто виявляються схожі на які-небудь з вже відомих. Постфактум таке припущення виправдовується наявністю в антивірусних базах сигнатур для визначення не одного, а відразу декількох вірусів. Заснований на такому припущенні евристичний метод полягає в пошуку файлів, які не повністю, але дуже близько відповідають сигнатурам відомих вірусів.

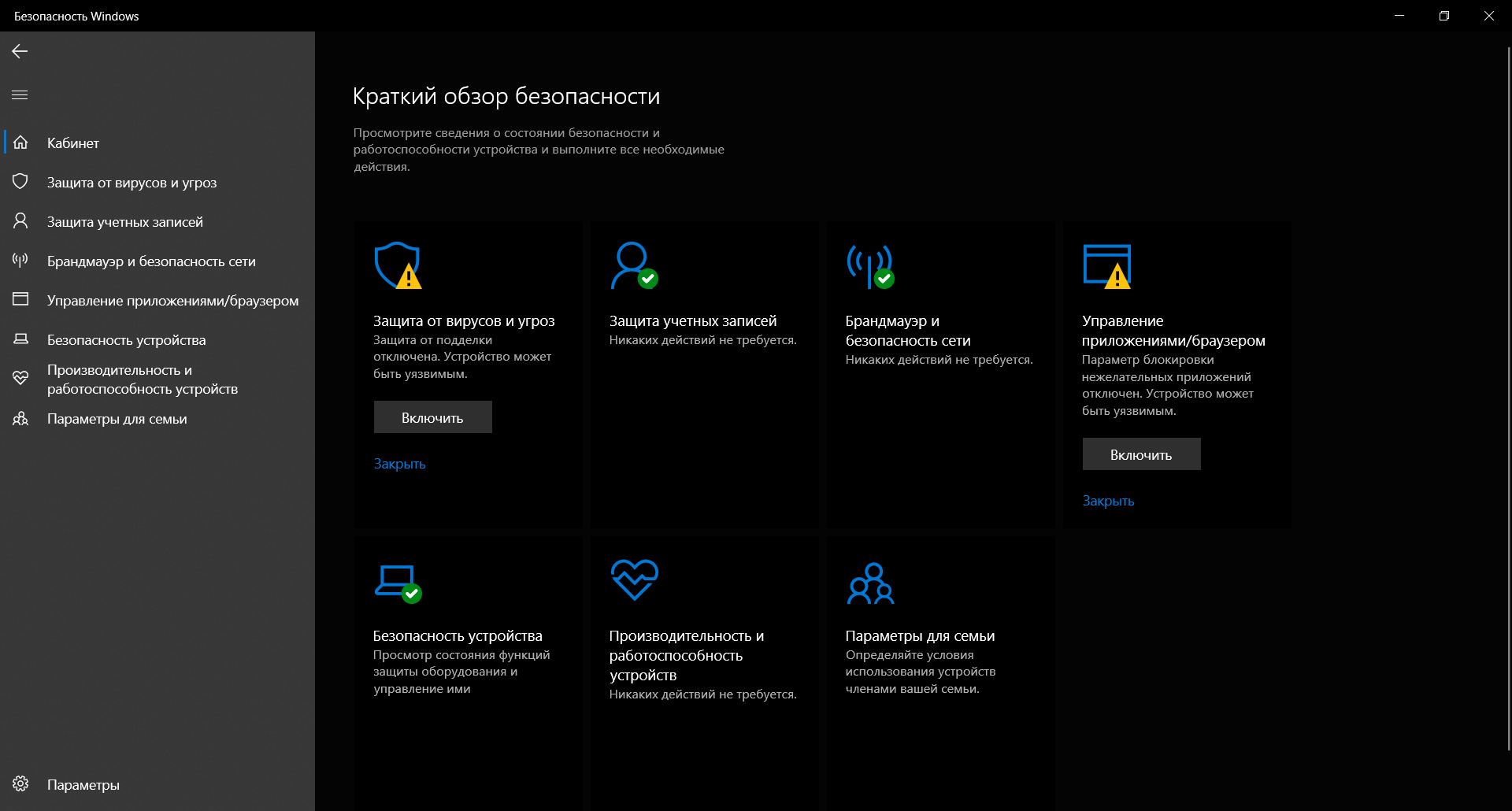
В першу чергу, кожен антивірус повинен містити модуль оновлення. Це пов'язано з тим, що основним методом виявлення вірусів сьогодні є сигнатурний аналіз, який покладається на використання антивірусної бази. Для того, щоб сигнатурний аналіз ефективно справлявся з найостаннішими вірусами, антивірусні експерти постійно аналізують зразки нових вірусів і випускають для них сигнатури.

Другий важливий допоміжний модуль - це модуль планування. Існує ряд дій, які антивірус повинен виконувати регулярно,зокрема: перевіряти ваш комп'ютер на наявність вірусів і оновлювати антивірусну базу. Модуль оновлення якраз і дозволяє набудувати періодичність виконання цих дій.

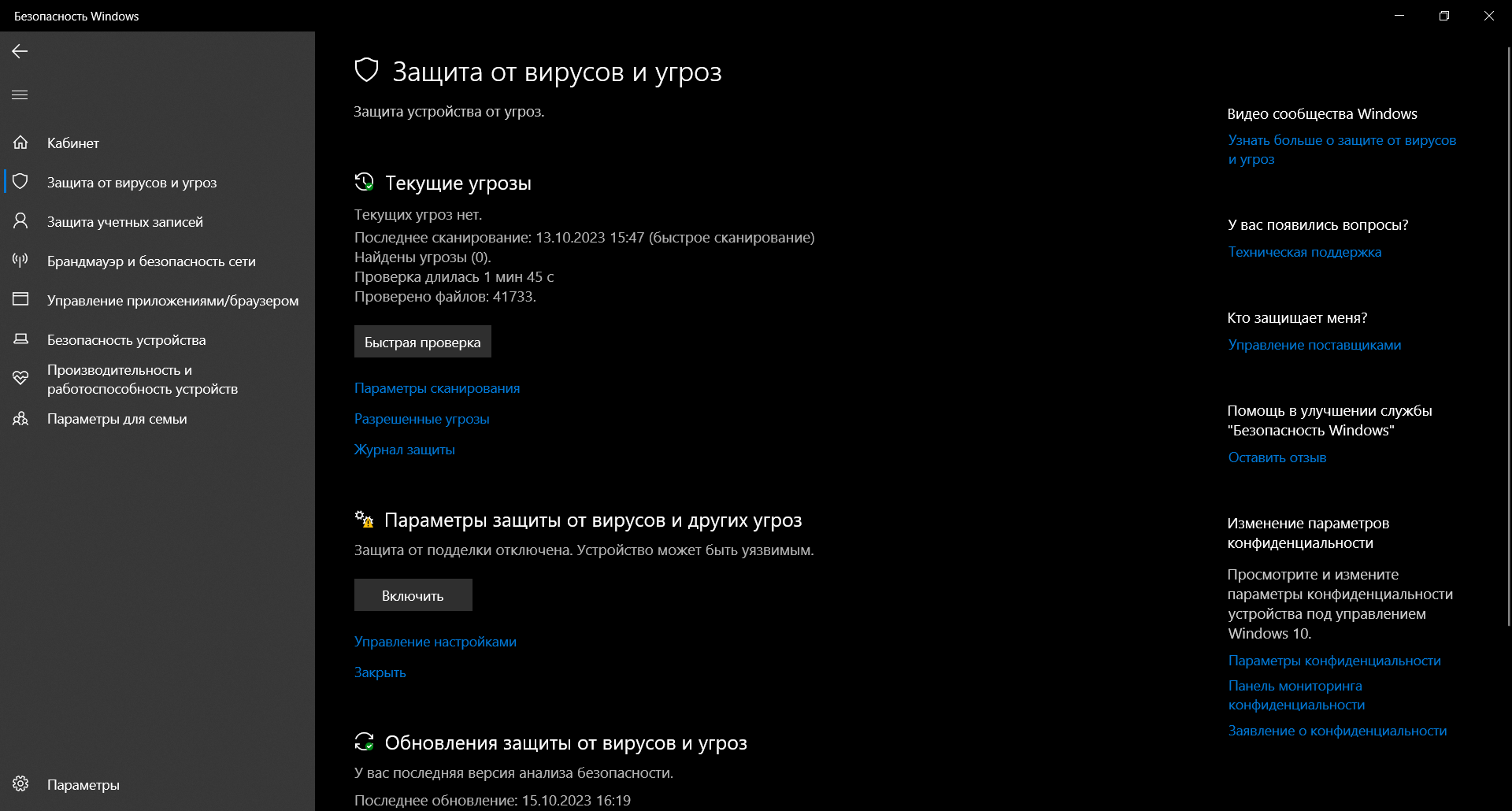
Серед інших допоміжних засобів в багатьох антивірусах є спеціальні технології, які захищають від можливої втрати даних в результаті дій антивіруса. Таким засобом є карантин, в який антивірус розміщує файл, що не вдалося вилікувати, тоді якщо опиниться, що файл був видалений помилково або була втрачена важлива інформація, завжди можна буде виконати відновлення з резервної копії.

**Завдання**

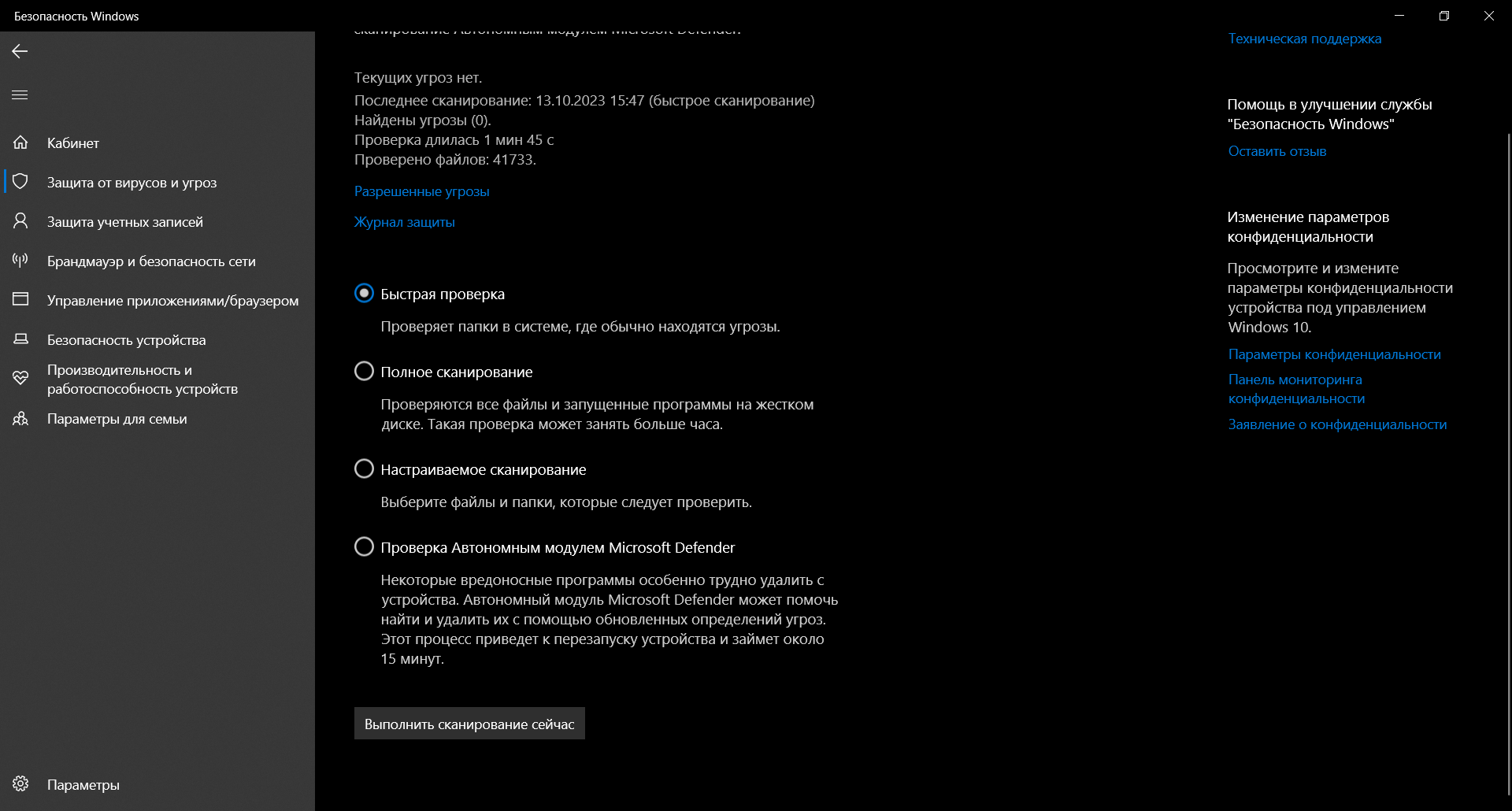
1. Для початку ознайомтесь з теоретичними відомостями.
2. Користуючись пошуковою системою Windows, перейдіть в меню безпеки Windows.



1. У відкритому вікні продивіться всі можливості кожного пункту системи безпеки Windows, опишіть оглянуті вами пункти з скріншотами.
2. Відкрийте вкладку «захист від вірусів та загроз»



1. На відкритій вкладці виберіть «Параметри сканування»



1. Виконайте всі види сканування для вашого комп’ютера. Результати всіх сканувань у вигляді скріншотів занесіть до звіту.
2. Знайдіть в мережі інтернет 5 програм для комп’ютера, опишіть їх можливості в звіті, створіть порівняльну таблицю цих антивірусних програм для комп’ютера. За такими параметрами (наявність безкоштовної версії, наявність сканера мережевої безпеки, зручність інтерфейсу, платформи на яких його можна використовувати, швидкість сканування).
3. Виберіть 3 антивірусні програми для комп’ютера, завантажте їх на свій комп’ютер. (Завантажувати їх потрібно не всі одночасно, а по черзі. Тобто одну антивірусну програму завантажили, виконали пункти 11 та 12 цієї лабораторної роботи, після чого видаляєте встановлену вами антивірусну програму, та завантажуєте наступну антивірусну програму. Знову виконуєте пункти 11, 12, видаляєте антивірусник та качаєте наступний, знову виконуєте пункт 11 та 12, після чого можете видаляти антивірусник).
4. Опишіть всі можливості цих 3 антивірусних програм у звіті з використанням скріншотів.
5. Зробіть сканування свого комп’ютера завантаженими вами антивірусними програмами, результати сканування занесіть у вигляді скріншотів до звіту.
6. Порівняйте завантажені вами антивірусні програми та результати сканування комп’ютера цими програмами між собою та з системою безпеки Windows, отримані результати занесіть до звіту, створіть порівняльну таблицю для завантажених вами антивірусних програм та системи безпеки Windows.
7. Дайте відповідь на контрольні питання.
8. Зробіть висновки та занесіть їх до звіту.

**Контрольні питання**

1. Що таке антивірус?
2. Які бувають види антивірусних програм?
3. Для чого використовувати антивірусні програми?
4. Що таке сигнатурний метод?
5. Що таке евристичний метод?
6. З чого складається антивірусне програмне забезпечення?
7. Які модулі повинен містити в собі антивірусне програмне забезпечення?