МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра кібербезпеки

«До захисту допущено»
Завідувач кафедри
_____ Володимир ЛЮБЧАК
(підпис)
____ _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавр

зі спеціальності 125 Кібербезпека ,
освітньо-професійної програми Кібербезпека
на тему: Порівняльний аналіз комплексних систем захисту цифрового середовища

Здобувача (ки) групи КБ-01 Руднєва Ангеліна Олексіївна
(шифр групи) (прізвище, ім'я, по батькові)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Ангеліна Руднєва
(підпис) (Ім'я та ПРІЗВИЩЕ здобувача)

Керівник _____ _____
(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ) (підпис)

Консультант[1)] _____ _____
(посада, науковий ступінь, вчене звання Ім'я та ПРІЗВИЩЕ) (підпис)

Суми – 2024

Примітки:

1) Зазначається за наявності

Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра кібербезпеки

«Затверджую»
Завідувач кафедри

_____ Володимир ЛЮБЧАК
(підпис)

«___»_____ 20___ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр

зі спеціальності 125 – Кібербезпека, освітньо-професійної програми «Кібербезпека»
здобувача групи КБ-01 Руднєва Ангеліна Олексіївна

1. Тема роботи: «Порівняльний аналіз комплексних систем захисту цифрового середовища».
затверджено наказом по СумДУ №0212-VI від «04» березня 2024 р.
2. Термін подання студентом роботи: «31» травня 2024 р.
3. Вихідні дані до роботи: _____
4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити): інформаційний огляд проблематики, практичне дослідження систем захисту.
5. Перелік графічного матеріалу (із зазначенням плакатів, презентацій тощо) _____
6. Консультанти до проекту (роботи), із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання «____» _____ 20 ___ р.

Завдання прийняв до виконання _____ Керівник _____
(підпис) (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	Огляд проблематики комплексних систем захисту цифрового середовища		
2	Практичне дослідження систем захисту		
3	Оформлення документації		
4			
5			

Здобувач вищої освіти _____ Керівник _____
(підпис) (підпис)

АНОТАЦІЯ

Кваліфікаційна робота виконана на 45 аркушах та містить 29 рисунки, 1 таблицю та 10 джерел.

Об’єкт дослідження. Процеси захисту цифрового середовища.

Мета роботи. Аналіз комплексних систем захисту цифрового середовища у розрізі питань ефективності, гнучкості, та спроможності протистояти сучасним кіберзагрозам.

Методи дослідження. Для досягнення поставленої мети використовувались методи теоретичного аналізу наукової літератури, критичного огляду та аналізу комплексних систем захисту цифрового середовища. Емпіричне дослідження здійснювалось шляхом моделювання атак на комп'ютерні системи з використанням шкідливих файлів, що дозволяло оцінити реакцію та ефективність антивірусних програм у реальному часі. Методи порівняння та узагальнення отриманих даних застосовувалися для формулювання висновків щодо надійності, швидкодії та загальної ефективності досліджуваних систем захисту.

Результат роботи. В ході роботи було проведено порівняльний аналіз комплексних систем захисту цифрового середовища, визначено переваги та недоліки кожної досліджуваної системи захисту. Було проведено моделювання атак за допомогою шкідливих файлів, що дозволило оцінити реакцію та ефективність програм у реальному часі.

Структура роботи. Дипломна робота складається з вступу, двох розділів, висновків та списку використаної літератури. У першому розділі здійснюється інформаційний огляд комплексних систем захисту цифрового середовища та аналізується спектр сучасних загроз, що впливають на цифрові середовища. Другий розділ присвячений практичному дослідженню і порівняльному аналізу ефективності застосування досліджуваних систем захисту. Цей розділ включає тестування систем на виявлення та нейтралізацію шкідливих файлів, а також оцінку їхньої здатності адаптуватися до змінюваних загроз.

Зміст

ВСТУП

У сучасному цифровому світі, де інформація стала ключовим ресурсом, а кіберзагрози посилюються, захист цифрового середовища виходить на передній план. Комплексні системи захисту відіграють ключову роль у гарантуванні безпеки і конфіденційності інформації, що знаходиться під постійною загрозою з боку хакерів, вірусів та інших кіберзлочинців. В контексті зростаючої кількості кібератак, захист інформації стає критичним як для приватного, так і для публічного секторів.

Серед основних загроз, з якими стикаються організації, можна виділити атаки типу "відмова в обслуговуванні" (DDoS), фішинг, інженерні атаки на персонал, зламування за допомогою шкідливого програмного забезпечення, в тому числі троянів і вірусів, які можуть красти, шифрувати або видаляти чутливу інформацію, зловживання доступом внутрішніх користувачів. Зростає загроза і з боку шпигунських програм, які можуть таємно збирати дані без відома користувача, створюючи серйозні ризики для конфіденційності.

Технології захисту динамічно розвиваються, використовуючи новітні досягнення у сфері штучного інтелекту, машинного навчання, та криптографії для створення все більш складних та автоматизованих систем захисту. Сучасні системи можуть не тільки реагувати на загрози, але й прогнозувати їх появу, аналізуючи великі обсяги даних та визначаючи потенційні вразливості. Це створює змогу забезпечити більш високий рівень безпеки, враховуючи потенціал адаптації до непередбачених умов та викликів.

Розвиток кібербезпеки вимагає постійного аналізу сучасних загроз і адаптації до них. Наприклад, розширення хмарних технологій веде до нових викликів у захисті даних, що зберігаються у віртуальному просторі. Кіберзлочинці постійно розробляють нові методи атак на хмарні сервіси, використовуючи вразливості у безпеці програмного забезпечення. Важливо, щоб системи захисту могли швидко ідентифікувати та нейтралізувати такі загрози, перш ніж вони спричинять збитки.

Ця робота спрямована на проведення порівняльного аналізу комплексних систем захисту, щоб виявити їх ключові характеристики, ефективність та можливі недоліки. Особлива увага приділяється не тільки порівнянню технічних параметрів, але й аналізу здатності систем пристосовуватися до нових загроз та їхньої інтеграції з існуючими технологічними рішеннями в організаціях. Такий підхід дозволяє зрозуміти, як системи можуть бути оптимізовані для захисту від специфічних загроз, що постійно еволюціонують.

Мета дослідження — не лише провести порівняльний аналіз існуючих систем захисту, а й розробити рекомендації щодо вибору та оптимізації захисту цифрових активів. Для досягнення цих цілей буде використана систематична методологія порівняльного аналізу, яка дозволить об'єктивно оцінити переваги і недоліки різних систем.

Таким чином, робота має важливе практичне значення, допомагаючи не лише академічній спільноті, а й професіоналам у галузі кібербезпеки оцінити поточний стан технологій та підібрати найкращі стратегії для захисту від зростаючих кіберзагроз.

1 ІНФОРМАЦІЙНИЙ ОГЛЯД

1.1 Визначення комплексних систем захисту цифрового середовища (КСЗЦС)

Комплексні системи захисту цифрового середовища (КСЗЦС) представляють собою сукупність засобів, технологій, методів і процесів, що використовуються для забезпечення безпеки інформаційних систем та мереж. Ці системи розроблені таким чином, щоб захистити дані, програмне забезпечення, апаратне забезпечення, а також інфраструктуру від несанкціонованого доступу, зловмисного втручання, збоїв у роботі, вірусів або інших загроз, що можуть негативно вплинути на роботу системи та безпеку даних.

Основною метою КСЗЦС є не просто захист від відомих загроз, а створення адаптивної системи, яка може протистояти новим загрозам, які розвиваються в реальному часі. Системи інтегрують заходи як на фізичному, так і на програмному рівнях, включаючи, але не обмежуючись, брандмауерами, антивірусним захистом, системами виявлення та запобігання (IDS), криптографічними захисними системами, а також політиками.[1]

Сучасні КСЗЦС також включають застосування інтелектуальних аналітичних інструментів, які використовують машинне навчання та штучний інтелект для прогнозування, виявлення і реагування на потенційні загрози на основі аналізу поведінки користувачів та трафіку в мережі. Це дозволяє системам швидко адаптуватися і реагувати на динамічні умови загроз, забезпечуючи більш ефективний та гнучкий рівень захисту.

Важливим аспектом комплексної системи захисту є її інтегрованість та здатність до синергії різних захисних компонентів, що забезпечує більш глобальний та об'ємний захист. Це означає, що КСЗЦС не тільки обмежується захистом від відомих загроз, але й активно взаємодіє з різними елементами цифрового середовища для прогнозування та нейтралізації потенційних вразливостей перед тим, як вони стануть джерелом проблем.

Таким чином, КСЗЦС є ключовим елементом у забезпеченні стійкості та надійності сучасних інформаційних систем, забезпечуючи необхідний рівень захисту в умовах постійно зростаючих та еволюціонуючих кіберзагроз.

1.2 Історія виникнення та розвитку комплексних систем захисту цифрового середовища (КСЗЦС)

Історія комплексних систем захисту цифрового середовища тісно пов'язана з розвитком комп'ютерних технологій та зростанням кіберзагроз. Основоположним етапом стало виникнення перших комп'ютерних вірусів і несанкціонованих доступів, що змусило розробників та дослідників звернути увагу на необхідність захисту інформаційних систем.

- Ранній період (1980-ті роки)

З появою перших персональних комп'ютерів і мереж, особливо з розвитком Інтернету, з'явилися перші віруси та шкідливе програмне забезпечення. Це спонукало до створення антивірусних програм, які були спрямовані на виявлення та видалення шкідливих програм.

- 1990-ті роки: Початок інтеграції

У цей період почалася інтеграція різних захисних технологій. Було розроблено перші брандмауери та системи виявлення вторгнень (IDS), які дозволяли відстежувати та блокувати потенційно небезпечний мережевий трафік. Завдяки зростанню кількості мережевих атак, з'явилася потреба в більш комплексних системах безпеки, які б могли ефективно захищати великі корпоративні мережі.

- 2000-ті роки: Розширення можливостей

У 2000-х роках з'явились системи запобігання вторгненням (IPS), які не тільки виявляли, але й активно блокували атаки в реальному часі. Відбулося злиття IPS та IDS у єдині рішення, які пропонували більш глибокий аналіз даних та активний захист. Крім того, почалося активне впровадження криптографічних методів для забезпечення конфіденційності та цілісності даних.

- 2010-ті роки: Інтеграція з хмарними обчисленнями

З розвитком хмарних обчислень і масштабної міграції даних та послуг в хмарне середовище, комплексні системи захисту стали включати хмарні технології. Було створено рішення, що інтегрують захист даних на всіх рівнях – від фізичного сервера до застосунків у хмарному середовищі.

- Сучасний період

На сьогоднішній день КСЗЦС використовують штучний інтелект та машинне навчання для прогнозування, виявлення та реагування на загрози. Ці системи є дуже складними і забезпечують захист не тільки від традиційних загроз, але й від складних цілеспрямованих атак. Інтеграція технологій та автоматизація процесів в режимі реального часу дозволяють забезпечити більш високий рівень безпеки та стійкості.

Таким чином, розвиток КСЗЦС проходив паралельно з розвитком інформаційних технологій, ставши невід'ємною частиною забезпечення кібербезпеки у складному та постійно змінюваному цифровому середовищі.

1.3 Основні компоненти та вимоги до комплексних систем захисту цифрового середовища (КСЗЦС)

Комплексні системи захисту цифрового середовища складаються з різноманітних технічних та програмних засобів, які спільно забезпечують ефективний захист інформації. Основні компоненти таких систем мають забезпечувати всебічний захист, включаючи превенцію, виявлення, реагування та відновлення після інцидентів. Це включає різноманітні технології та інструменти, які описуються нижче:

Основні компоненти:

- Брандмауери (Firewalls): Забезпечують контроль заходу та виходу трафіку в мережі на основі визначених правил безпеки.[2]
- Системи виявлення та запобігання вторгненням (IDS/IPS): Аналізують мережевий трафік на предмет аномалій, які можуть свідчити про спроби несанкціонованого доступу або атак.

- Антивірусне програмне забезпечення: Виявляє та усуває шкідливе програмне забезпечення, забезпечуючи захист від вірусів, троянів, черв'яків тощо.
- Криптографічні заходи: Забезпечують шифрування даних для захисту конфіденційності та цілісності інформації.
- Механізми аутентифікації та авторизації: Відповідають за перевірку та підтвердження ідентичності користувачів і забезпечують контроль доступу до ресурсів.
- Програмне забезпечення для управління безпекою (Security Information and Event Management - SIEM): Збирає та аналізує інформацію про події безпеки з різних джерел для своєчасного виявлення та реагування на інциденти.

Ефективність комплексних систем захисту цифрового середовища в значній мірі залежить від дотримання певних вимог, які забезпечують їх здатність адекватно протистояти сучасним загрозам. Ці вимоги стосуються не тільки технічної складової систем, а й організаційних аспектів їх впровадження та управління. Нижче перераховані ключові вимоги, які мають бути враховані при розробці та експлуатації КСЗЦС.

- Інтегрованість: Система повинна забезпечувати цілісність та взаємодію між різними компонентами для ефективної роботи.
- Масштабованість: Система має бути здатна адаптуватися до зростання мережі та збільшення кількості користувачів без втрати продуктивності.
- Надійність: Висока доступність та мінімальні відмови у роботі є критично важливими.
- Адаптивність: Система має бути здатна швидко адаптуватися до нових загроз та змін.
- Здатність до аудиту та звітності: Має існувати можливість легко перевіряти та звітувати про стан безпеки системи.

- Зрозумілий інтерфейс: Інтерфейси управління повинні бути зрозумілими та доступними для адміністраторів безпеки.
- Відповідність законодавству та стандартам: Система повинна відповідати актуальним законодавчим та міжнародним нормам і стандартам у галузі кібербезпеки.

1.4 Класифікація та типологія комплексних систем захисту цифрового середовища (КСЗЦС)

Для ефективного розуміння та вибору комплексних систем захисту цифрового середовища, важливо розглянути їх класифікацію та типологію. Різні системи захисту можуть класифікуватися за багатьма критеріями, що дозволяє організаціям обирати найбільш підходящі рішення відповідно до їхніх специфічних потреб і загроз, з якими вони стикаються. Ось основні типи КСЗЦС, які застосовуються в індустрії кібербезпеки:

За областю застосування:

- Периметральні системи захисту: Встановлюються на межі мережі для захисту від зовнішніх загроз, як-от брандмауери та шлюзи.
- Кінцеві точки захисту: Використовуються для захисту окремих пристроїв, включаючи антивірусні програми та системи запобігання втручанню.
- Системи захисту даних: Забезпечують шифрування та інші заходи для захисту даних, які передаються або зберігаються.[3]

За способом реалізації:

- Апаратні рішення: Фізичні пристрої, які інтегровані в інфраструктуру та забезпечують захист на апаратному рівні.
- Програмні рішення: Програмне забезпечення, яке можна інсталювати на існуючі системи для надання захисних функцій.
- Хмарні рішення: Захист, що здійснюється з використанням хмарних технологій, дозволяючи гнучкість і масштабованість.

За механізмом захисту:

- Реактивні системи: Реагують на вже виявлені загрози і атаки, намагаючись мінімізувати їх вплив.
- Проактивні системи: Використовують передові технології для передбачення і запобігання атакам ще до їх здійснення.
- Гібридні системи: Комбінують реактивні та проактивні підходи для надання комплексного захисту.[4]

За вектором захисту:

- Мережевий захист: Зосереджений на захисті мережевих ресурсів та інфраструктури.
- Захист застосунків: Фокусується на забезпеченні безпеки програмного забезпечення та застосунків.
- Захист ідентичності: Включає механізми для забезпечення аутентичності користувачів та захисту їхніх ідентифікаторів.

Ця класифікація допомагає не тільки в розумінні існуючих рішень, але й в плануванні впровадження та управління захисними системами в залежності від потреб і можливостей організації. Оптимальне поєднання різних типів та механізмів захисту забезпечує максимально ефективне укріплення кібербезпеки в умовах постійної еволюції кіберзагроз.[5]

1.5 Сфери використання комплексних систем захисту цифрового середовища (КСЗЦС)

Комплексні системи захисту цифрового середовища (КСЗЦС) застосовуються у різноманітних галузях і сферах діяльності, де критично важлива безпека даних і інформаційних процесів. Використання цих систем не обмежується лише великими корпораціями чи спеціалізованими IT-компаніями; вони є важливими для широкого спектру організацій, від державних установ до малого та середнього бізнесу. Ось основні сфери, де КСЗЦС знаходять своє застосування:

- Фінансовий сектор: Банки та інші фінансові установи використовують КСЗЦС для захисту конфіденційності клієнтської інформації, транзакцій, а також для протидії шахрайству та кібератакам.
- Охорона здоров'я: Медичні установи впроваджують ці системи для захисту даних пацієнтів, які є особливо чутливими і підлягають суворій конфіденційності згідно з регулятивними вимогами (наприклад, HIPAA в США, в Україні це: Цивільний кодекс України, Закони України «Основи законодавства України про охорону здоров'я», «Про захист персональних даних», Типовий порядок обробки персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 №1/02-14).
- Роздрібна торгівля та електронна комерція: Ретейлери застосовують КСЗЦС для захисту персональних даних клієнтів та фінансової інформації, а також для забезпечення безпечних онлайн-покупок.
- Державний сектор: Державні інституції використовують КСЗЦС для захисту державних секретів, забезпечення національної безпеки, а також для оборони критично важливої інфраструктури.
- Освіта: Навчальні заклади використовують системи захисту для забезпечення безпеки дослідницьких даних та особистої інформації студентів, а також для запобігання кіберінцидентам в мережах університетів.
- Телекомунікації: Компанії цього сектору застосовують КСЗЦС для захисту інформації, що передається через їхні мережі, включаючи голосові дані, текстові повідомлення та інші види даних.
- Виробництво: Виробничі підприємства застосовують комплексні системи захисту для контролю доступу до виробничих ліній, управління промисловими системами та захисту від фізичних кіберзагроз.[6]

Застосування КСЗЦС в цих та інших галузях є ключовим для захисту від сучасних кіберзагроз та забезпечення цілісності, доступності та конфіденційності важливої інформації. Вибір та імплементація відповідних

систем залежить від специфіки галузі, розміру організації та характеру інформації, яка потребує захисту.

1.6 Огляд та класифікація сучасних загроз цифрового середовища

Сучасне цифрове середовище постійно зазнає атак з боку різноманітних кіберзагроз, які еволюціонують і стають дедалі складнішими та небезпечнішими. Розуміння цих загроз є критично важливим для розробки ефективних стратегій кіберзахисту. Нижче представлено класифікацію основних видів кіберзагроз, з якими стикаються організації сьогодні:

- Віруси та черв'яки: Автономні програми, які можуть самостійно реплікуватися та поширюватися з однієї системи на іншу, часто завдаючи шкоди зараженим системам.
- Троянські програми: Шкідливе програмне забезпечення, яке приховується в легітимному програмному забезпеченні. Трояни можуть виконувати різні шкідливі дії, включаючи крадіжку даних або установку інших зловмисних програм.
- Руткіти: Програми, які дозволяють адміністративний доступ до комп'ютера без відома користувача, часто приховуючи себе та інше шкідливе програмне забезпечення від антивірусних програм.
- Спам та фішинг: Небажані або шахрайські повідомлення, спрямовані на заманювання користувачів до виконання небезпечних дій, таких як надання конфіденційної інформації.
- Denial of Service Attack (DoS): напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.
- Розподілені атаки типу «відмова в обслуговуванні» (DDoS): Варіація DoS-атак, де трафік надходить з багатьох джерел, ускладнюючи їх блокування.

- Атаки «людина посередині» (Man-in-the-Middle, MitM): Атаки, при яких зловмисник перехоплює та можливо змінює комунікацію між двома сторонами, які вважають, що вони безпосередньо спілкуються один з одним.
- Ransomware (програми-вимагачі): Шкідливе програмне забезпечення, яке блокує доступ до файлів або систем користувачів і вимагає викуп за їх відновлення.
- Експлойти: Код, що використовує вразливості в програмному забезпеченні для проведення шкідливих дій, включно з отриманням контролю над системою.

Ця класифікація демонструє широкий спектр загроз, що вимагає комплексних підходів до захисту в сучасному цифровому середовищі. Розуміння та аналіз цих загроз є невід'ємною частиною стратегічного планування в області кібербезпеки, що допомагає визначити найбільш вразливі точки і вибрати відповідні заходи захисту.[7]

1.7 Типи кібератак

У сучасному цифровому світі існує широкий спектр кібератак, кожна з яких має свої особливості та потенційні наслідки для інформаційних систем. Основні типи атак, що здійснюються на інформаційні системи, включають:

- Віддалене проникнення (Remote penetration): Атака, яка здійснюється через мережу Інтернет та має на меті отримати контроль над віддаленими системами без фізичного доступу до них.
- Локальне проникнення (Local penetration): Атака, яка виконується безпосередньо з місця, де розташована цільова система, що може включати в себе доступ до корпоративної мережі або фізичний доступ до комп'ютера.
- Атака на відмову в обслуговуванні (Denial of Service): Спроба зробити ресурс недоступним для його призначених користувачів, зазвичай шляхом перевантаження системи зайвим трафіком.

- Мережні сканери (Network scanners): Інструменти, що сканують мережу для виявлення активних хостів, відкритих портів, та використовуваних сервісів, щоб ідентифікувати потенційні вразливості.
- Сканери вразливостей (Vulnerability scanners): Програми, які аналізують системи на наявність відомих вразливостей, які можуть бути використані в ході кібератак.
- Зламувачі паролів (Password crackers): Інструменти, що використовують різні методи (від грубої сили до соціальної інженерії) для вгадування або розшифрування паролів користувачів.
- Аналізатори протоколів (Sniffers): Програми, що перехоплюють та аналізують мережний трафік, дозволяючи зловмисникам виявити чутливі дані, як-от паролі та іншу конфіденційну інформацію.
- Спам e-mail (Mailbombing): Відправлення великої кількості електронних листів на одну адресу, що може перевантажити поштову скриньку або сервер.
- Перехоплення каналу зв'язку (Man-in-the-Middle): Атака, де зловмисник активно перехоплює та можливо альтерує комунікацію між двома сторонами, що вважають, що вони безпосередньо спілкуються один з одним.

Кожен з цих типів атак вимагає від організацій впровадження спеціалізованих заходів безпеки, щоб знизити ризик і забезпечити надійний захист від можливих загроз.[8]

1.8 Аналіз вразливостей цифрового середовища

Аналіз вразливостей цифрового середовища є критично важливим процесом, який допомагає організаціям ідентифікувати, класифікувати та пріоритетизувати потенційні слабкі місця в їхніх інформаційних системах. Цей процес може включати аналіз програмного забезпечення, апаратних засобів, мережевої інфраструктури та процедур кібербезпеки. Основною

метою аналізу вразливостей є мінімізація ризику кібератак. Ось основні етапи, які зазвичай включає цей процес:

- Ідентифікація активів та ресурсів: Перший крок полягає у визначенні всіх активів, які потребують захисту, включаючи програмне та апаратне забезпечення, дані, мережеві компоненти, та застосунки.
- Оцінка вразливостей: Використання сканерів вразливостей та інших інструментів дозволяє автоматизувати процес виявлення вразливих точок. Це може включати аналіз налаштувань, відсутніх патчів, слабких паролів, помилок у програмному забезпеченні та інших потенційних слабкостей.
- Аналіз ризиків: Оцінка потенційного впливу кібератаки на виявлені вразливості, а також ймовірності такої атаки. Цей етап допомагає визначити, які вразливості є найбільш критичними та як їх слід адресувати.
- Пріоритезація виправлень: На основі аналізу ризиків розробляється план виправлень, який вказує, які вразливості потрібно усунути першочергово. Важливо враховувати ресурси та можливості організації при плануванні виправлень.
- Застосування виправлень та мітігаційних заходів: Реалізація технічних виправлень, таких як оновлення програмного забезпечення, зміна конфігурацій, встановлення безпекових патчів, та застосування мітігаційних заходів для зниження ризиків, які не можуть бути повністю усунуті.
- Повторний огляд та моніторинг: Оскільки нові вразливості виявляються регулярно, важливо здійснювати повторний огляд безпеки та постійний моніторинг системи, щоб виявляти та вирішувати нові вразливості в міру їх появи.

Аналіз вразливостей — це неперервний процес, що вимагає регулярного оновлення та адаптації до нових загроз та викликів у цифровому світі. Він допомагає забезпечити вищий рівень захисту та резилієнтність організацій перед лицем кіберзагроз.[9]

1.9 Статистика та тенденції кіберзагроз

За останніми даними, кількість кібератак в Україні у 2023 році зросла на 15,9% порівняно з попереднім роком, досягнувши 2543 інцидентів. Аналітики прогнозують, що до 2025 року глобальні збитки від кібератак можуть сягнути 10,5 трлн доларів. Таке зростання підкреслює не лише посилення загроз, але й необхідність більш активного впровадження заходів кібербезпеки у всіх секторах.

Статистика атак по секторах

Аналіз розподілу інцидентів показує, що у 2023 році 347 атак було спрямовано на урядові установи, 276 – на місцеві органи влади, 175 – на організації сектору безпеки та оборони, та 127 на комерційні організації. Інші значні атаки стосувалися енергетичного сектору (92), телекомунікацій (81), освіти (38), транспорту (32), фінансів (30), IT-сектору (25), ЗМІ (15) та медичних установ (12).

Ці дані підкреслюють наростаючу тенденцію до збільшення кіберзагроз і необхідності розробки більш ефективних заходів кібербезпеки для захисту критично важливих інфраструктур і особистих даних громадян.

Найвідоміші та наймасштабніші кібератаки в світі та іхній вплив на уражені сектори:

- Вірус Мелісса

Одна з перших великих кіберзагроз, вірус Мелісса, була запущена в 1999 році. Програміст Девід Лі Сміт розіслав заражені файли через Microsoft Word, що призвело до серйозних наслідків для сотень компаній, включаючи Microsoft, із збитками, що оцінюються в 80 млн доларів.

- Кібератака на NASA

У 1999 році 15-річний Джеймс Джонатан зламав систему NASA, використовуючи уразливості в її операційній системі. Він викрав програмне забезпечення для управління Міжнародною космічною станцією, загрузивши при цьому 1,7 млн програм та завдавши збитків на 41 тисячу доларів.

- Кібератака на Естонію

У квітні 2007 року Естонія зіткнулася з першою в історії масштабною кібератакою на цілу країну, що призвело до вимкнення близько 58 урядових, банківських та медійних вебсайтів. Збої тривали три тижні, спричинивши економічні збитки.

- Взлом PlayStation Network

У 2011 році PlayStation Network було атаковано, в результаті чого особисті дані близько 77 млн користувачів, включно з платіжними даними, були викрадені.

- Adobe Cyber Attack

У 2013 році Adobe зіткнулася з великим витоком даних, під час якого було викрадено дані 38 млн користувачів та частину вихідного коду Photoshop.

- Атака на енергосистеми України

У 2015 році відбулася перша у світі кібератака на об'єкти енергетики в Україні, коли хакерам вдалося зламати систему управління електропостачанням, в результаті чого було тимчасово відключено електроенергію в значній частині Івано-Франківської області.

- Програма-вимагач WannaCry

У 2017 році вірус WannaCry заблокував десятки тисяч комп'ютерів у більш ніж 150 країнах, вимагаючи викуп у біткоїнах.

- Кібератака на готельну мережу Marriott

У 2018 році виявлено, що дані приблизно 339 млн гостей готелів Marriott і Starwood Hotels Group були скомпрометовані, що призвело до штрафу у розмірі більше 24 млн доларів.[10]

2 ПРАКТИЧНА ЧАСТИНА

У цьому розділі ми будемо порівнювати комплексні системи захисту цифрового середовища. Було обрано три популярні системи: Avast, Bitdefender та Windows Defender. Вони будуть порівнюватися за різними параметрами, такими як функціонал, захищеність, ціна, зручність та інші.

2.1 Avast

Avast - це чеська компанія, заснована в 1988 році, яка розробляє програмне забезпечення для кібербезпеки та захисту конфіденційності. Їхнє флагманське рішення, Avast Antivirus, є одним із найпопулярніших антивірусних програм у світі з понад 400 мільйонами активних користувачів. Avast пропонує широкий спектр продуктів для захисту комп'ютерів, мобільних пристроїв та домашніх мереж.

Функціонал Avast:

- Антивірусний захист: Avast захищає ваш комп'ютер від вірусів, програм-вимагачів, шпигунського програмного забезпечення та інших онлайн-загроз.
- Захист веб-браузера: Avast блокує шкідливі веб-сайти та фішингові атаки, а також захищає ваші особисті дані під час онлайн-шопінгу та банківських операцій.
- Захист файлів: Avast сканує ваші файли та папки на наявність шкідливого програмного забезпечення, а також пропонує шифрування файлів для захисту ваших конфіденційних даних.
- Захист Wi-Fi: Avast сканує вашу домашню мережу на наявність несанкціонованих підключень та захищає ваші пристрої від хакерів.
- Брандмауер: Avast брандмауер захищає ваш комп'ютер від несанкціонованого доступу з Інтернету.
- Захист особистих даних: Avast пропонує інструменти для захисту вашої конфіденційності в Інтернеті, такі як VPN та менеджер паролів.

- Батьківський контроль: Avast пропонує інструменти для моніторингу та контролю онлайн-активності ваших дітей.

Тарифи Avast:

Avast пропонує безкоштовну та платну версії свого програмного забезпечення. Безкоштовна версія забезпечує базовий захист від вірусів та інших онлайн-загроз. Платні версії пропонують додаткові функції, такі як захист веб-браузера, захист файлів, захист Wi-Fi, брандмауер, захист особистих даних та батьківський контроль.

Переваги Avast:

- Безкоштовна версія: Avast пропонує безкоштовну версію свого програмного забезпечення, яка забезпечує базовий захист від вірусів та інших онлайн-загроз.
- Широкий спектр функцій: Avast пропонує широкий спектр функцій для захисту комп'ютерів, мобільних пристроїв та домашніх мереж.
- Простий у використанні: Avast простий у використанні та налаштуванні, навіть для початківців.
- Ефективний захист: Avast отримав високі оцінки від незалежних тестових лабораторій за ефективність захисту від вірусів та інших онлайн-загроз.

Недоліки Avast:

- Безкоштовна версія показує рекламу: Безкоштовна версія Avast показує рекламу, яка може бути дратівливою для деяких користувачів.
- Виток даних: Avast мав проблему з витоком даних користувачів у минулому.

Інтерфейс Avast:

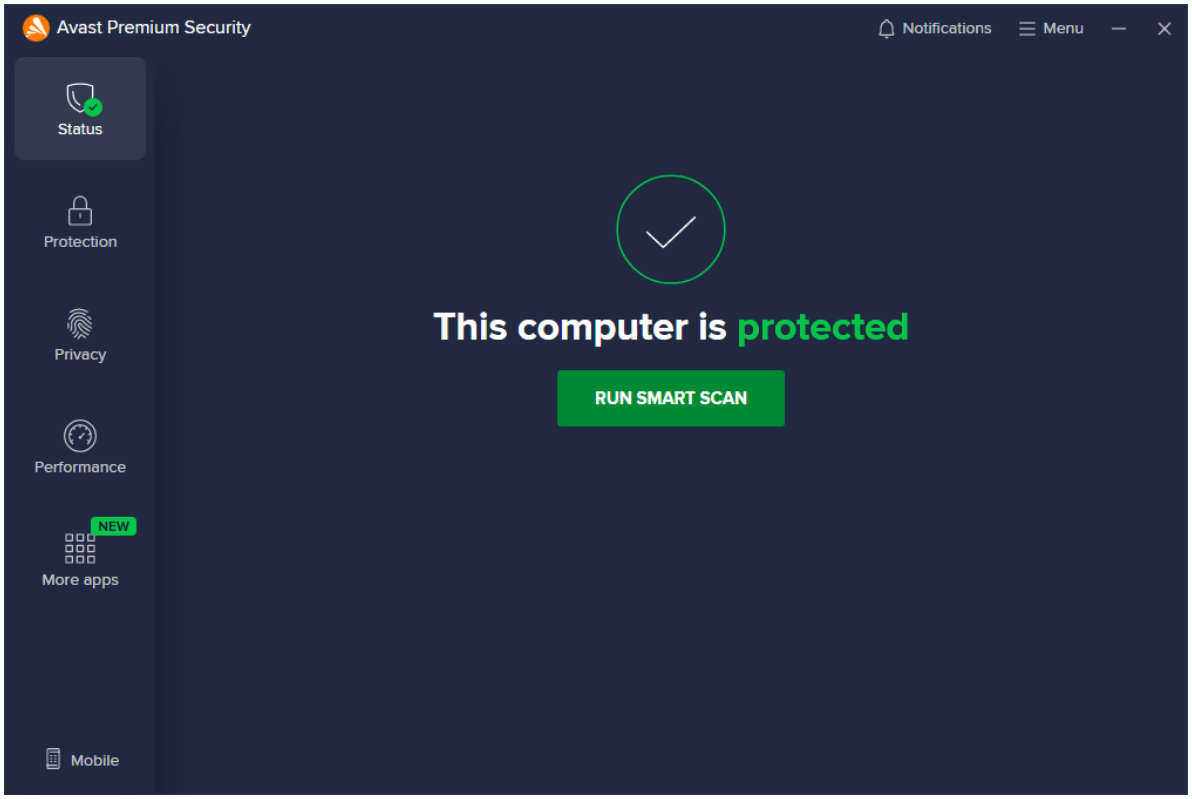

Рисунок 2.1 – сторінка статусу та сканування

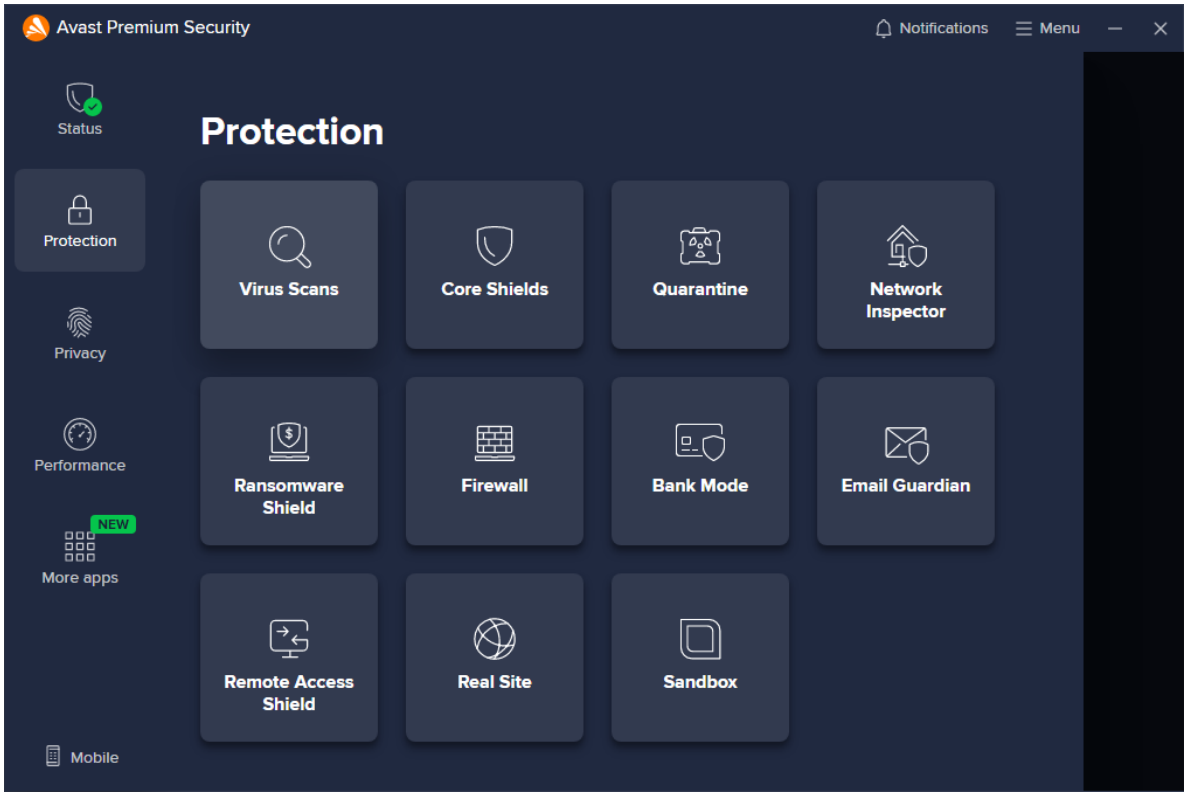

Рисунок 2.2 – сторінка функцій захисту

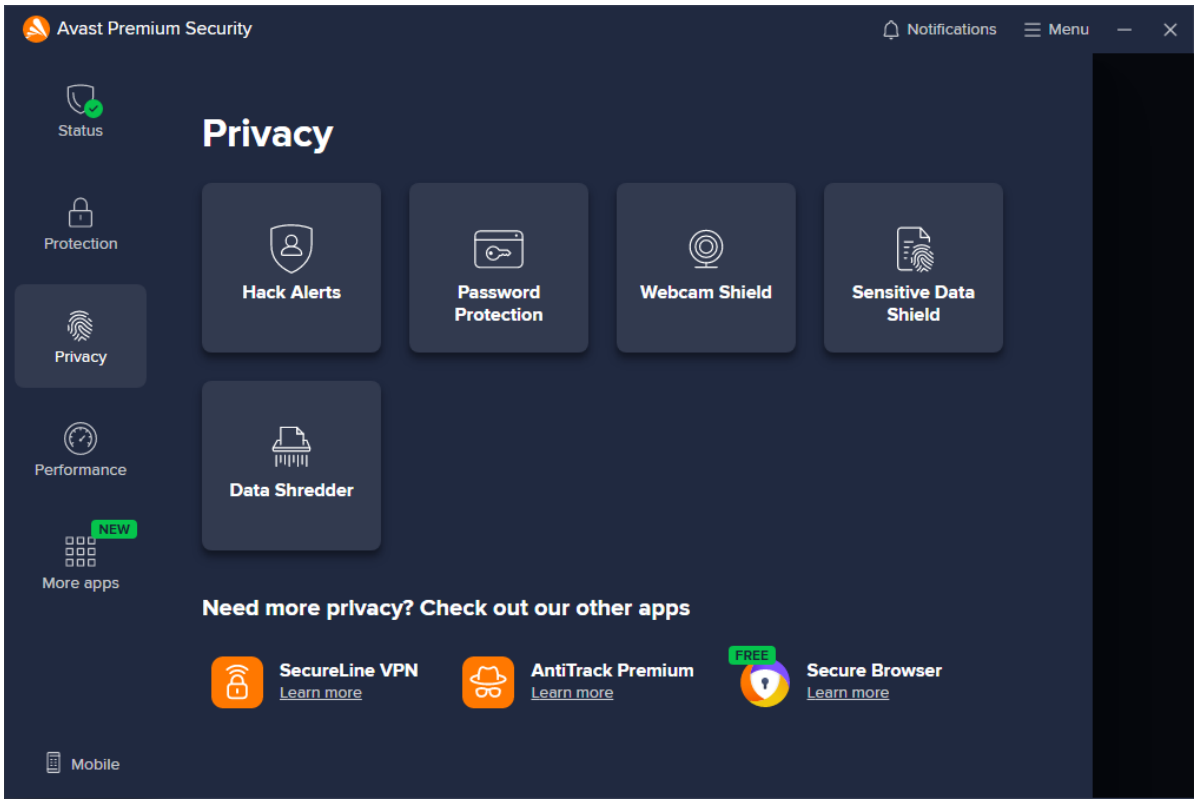

Рисунок 2.3 – сторінка захисту приватності

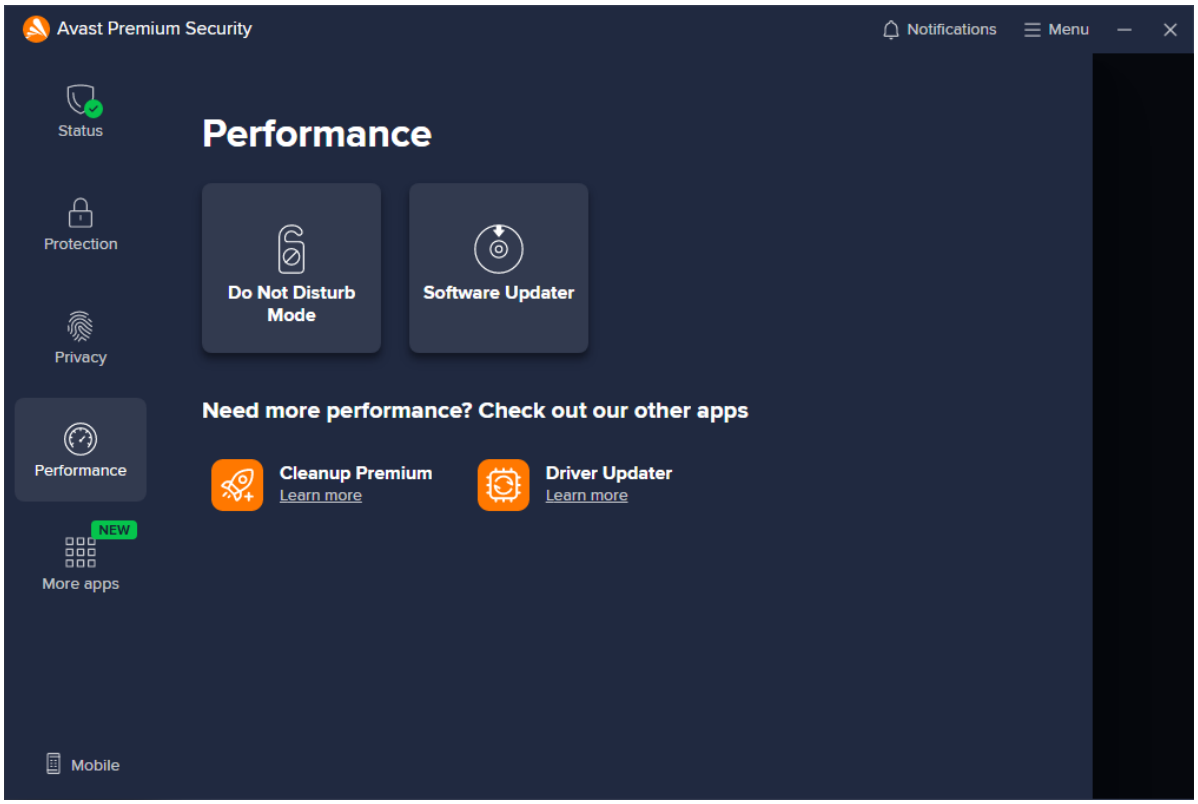

Рисунок 2.4 – сторінка покращення швидкості роботи девайсу

2.2 Bitdefender

Bitdefender - це румунська компанія, заснована в 2001 році, яка спеціалізується на розробці програмного забезпечення для кібербезпеки. Їхнє флагманське рішення, Bitdefender Antivirus, є одним з провідних антивірусних програм у світі з мільйонами користувачів у понад 150 країнах. Bitdefender пропонує широкий спектр продуктів для захисту комп'ютерів, мобільних пристроїв та корпоративних мереж.

Функції Bitdefender:

- Розширений захист від загроз: Bitdefender використовує передові технології, включаючи штучний інтелект та машинне навчання, для виявлення та нейтралізації новітніх вірусів і шкідливого ПЗ.
- Автоматичний апгрейд: Bitdefender автоматично оновлюється до останніх версій, забезпечуючи постійний захист без необхідності ручного втручання.
- Інтеграція з іншими платформами: Bitdefender підтримує інтеграцію з популярними платформами та сервісами, такими як Windows, macOS, Android та iOS, для всебічного захисту.
- Режим безпеки для онлайн-банкінгу: Спеціалізований браузерний режим забезпечує безпечні онлайн-транзакції та захищає від фішингових атак.
- Захист від експлойтів: Bitdefender забезпечує захист від вразливостей у програмному забезпеченні, які можуть бути використані кіберзлочинцями.
- Оптимізація продуктивності: Bitdefender включає інструменти для оптимізації продуктивності системи, такі як очищення непотрібних файлів та прискорення роботи комп'ютера.
- Контроль веб-камери та мікрофона: Bitdefender надає можливість контролювати доступ до вашої веб-камери та мікрофона, запобігаючи несанкціонованому шпигуванню.

Тарифи Bitdefender:

Bitdefender пропонує різноманітні тарифні плани, включаючи безкоштовні та платні версії. Безкоштовна версія надає базовий захист від вірусів та інших загроз. Платні версії включають додаткові функції, такі як розширений захист від загроз, режим безпеки для онлайн-банкінгу, контроль веб-камери та мікрофона, а також інструменти для оптимізації продуктивності.

Переваги Bitdefender:

- Висока ефективність: Bitdefender отримує високі оцінки від незалежних тестових лабораторій за здатність виявляти та нейтралізувати загрози.
- Зручний інтерфейс: Інтуїтивно зрозумілий інтерфейс робить Bitdefender простим у використанні, навіть для новачків.
- Інноваційні функції: Bitdefender постійно впроваджує новітні технології для підвищення рівня захисту та зручності користувачів.
- Висока продуктивність: Завдяки оптимізації системи Bitdefender мінімізує вплив на продуктивність комп'ютера.

Недоліки Bitdefender:

- Вартість: Деякі користувачі можуть вважати вартість платних версій Bitdefender досить високою в порівнянні з іншими антивірусними програмами.
- Ресурсоємність: Попри оптимізацію, під час виконання повного сканування може спостерігатися зниження швидкості роботи комп'ютера.

Інтерфейс Bitdefender:

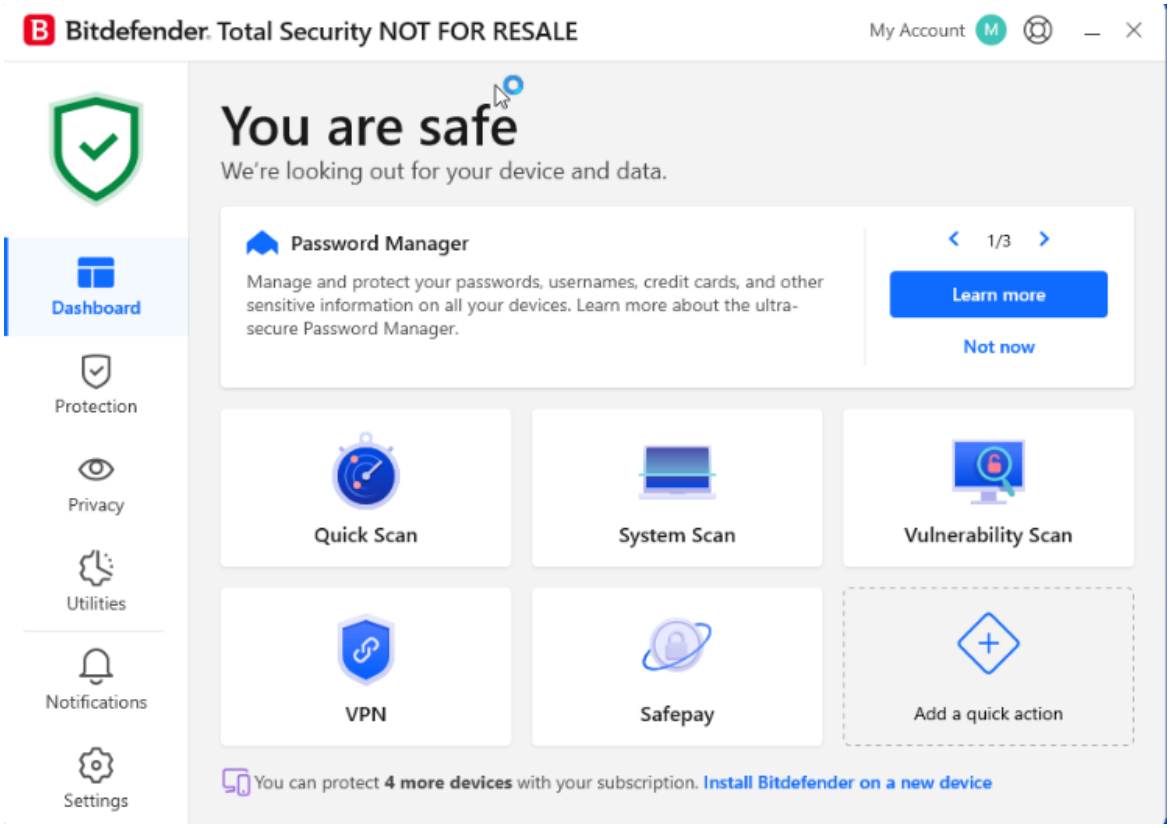

Рисунок 2.5 – головна сторінка

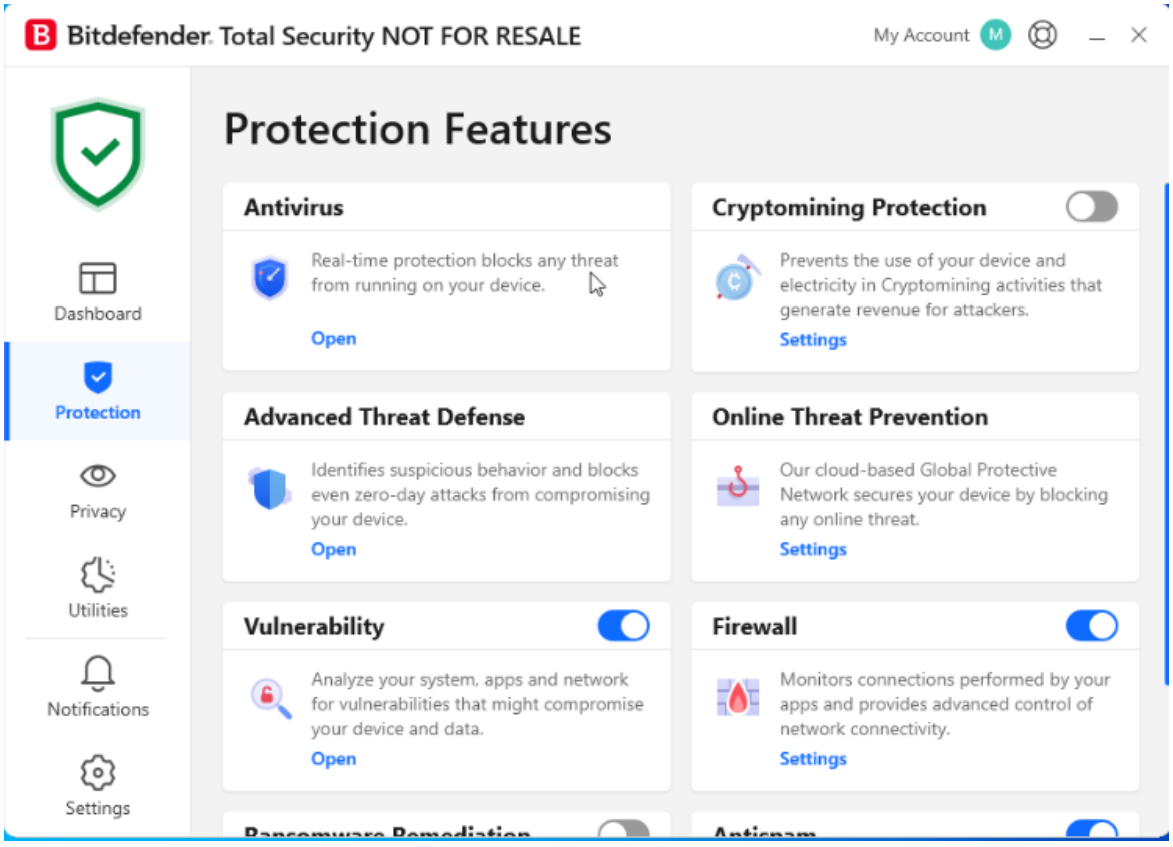

Рисунок 2.6 – сторінка функцій сканувань

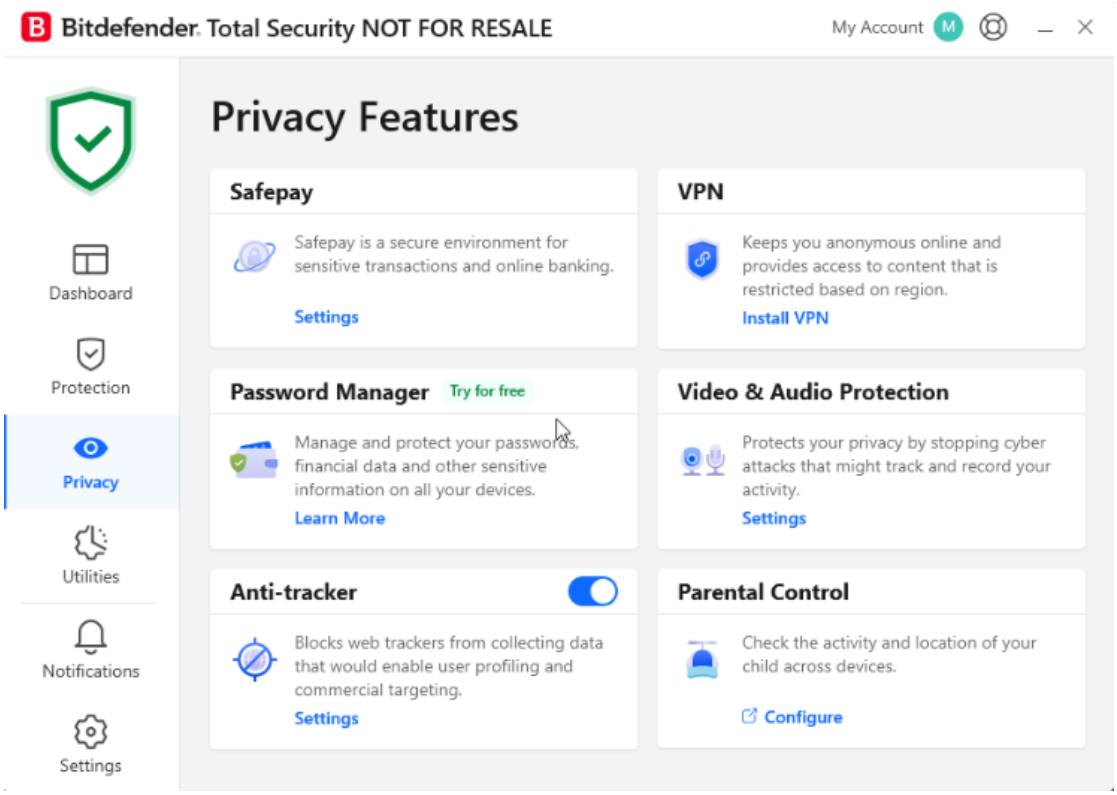

Рисунок 2.7 – сторінка приватності

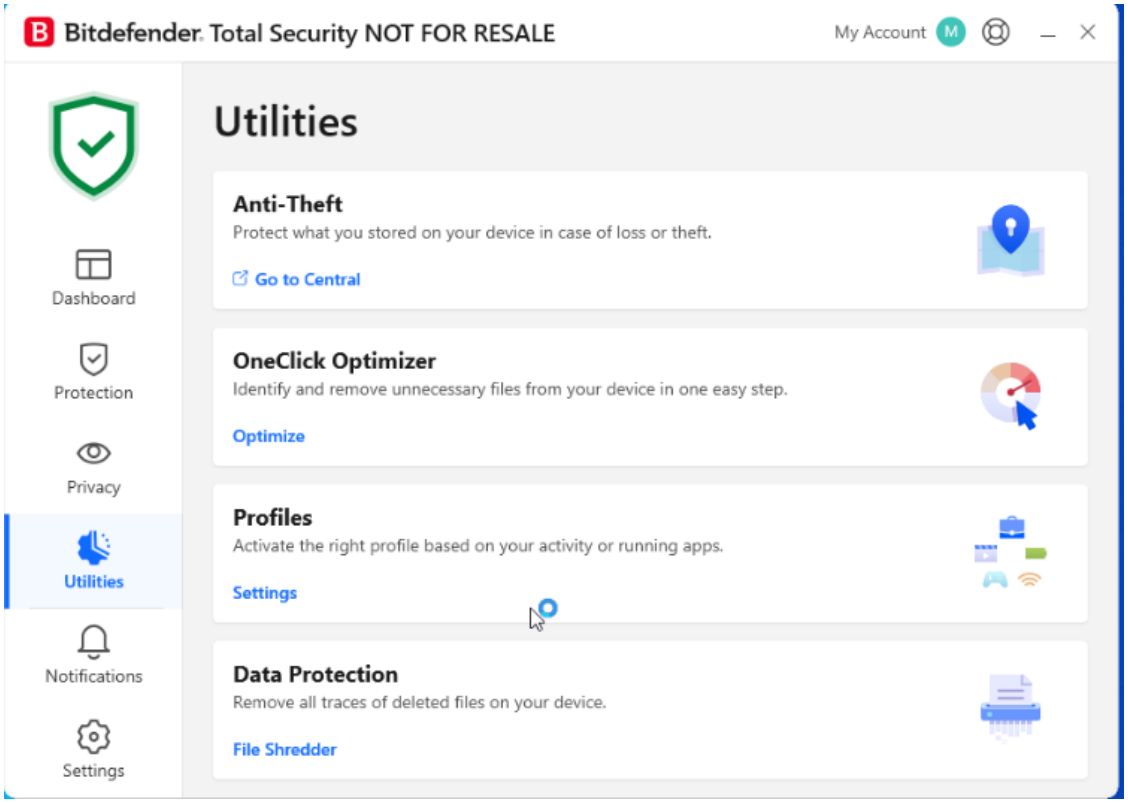

Рисунок 2.8 – усі інші функції

2.3 Windows Defender

Windows Defender - це вбудоване антивірусне програмне забезпечення від Microsoft, яке забезпечує захист від шкідливого програмного забезпечення для операційної системи Windows. Починаючи з Windows 8, Windows Defender є стандартною функцією, яка надає користувачам базовий рівень захисту від вірусів, шпигунського ПЗ та інших загроз без необхідності встановлення сторонніх програм.

Функції Windows Defender:

- Захист у реальному часі: Windows Defender забезпечує постійний моніторинг системи, виявляючи та блокуючи потенційні загрози в режимі реального часу.
- Сканування на вимогу: Користувачі можуть виконувати повне або вибіркове сканування системи для виявлення шкідливого програмного забезпечення.
- Хмарний захист: Використання хмарних технологій для швидкого виявлення нових загроз та отримання останніх оновлень визначень вірусів.
- Захист від експлойтів: Вбудовані інструменти для захисту від уразливостей у програмному забезпеченні, які можуть бути використані зловмисниками.
- Інтеграція з системою: Глибока інтеграція з операційною системою Windows забезпечує оптимальну продуктивність та мінімальний вплив на роботу системи.
- Батьківський контроль: Інструменти для налаштування обмежень і моніторингу активності дітей у мережі Інтернет.
- Фільтрація контенту: Захист від фішингових атак та небезпечних веб-сайтів за допомогою вбудованих функцій фільтрації контенту.

Тарифи Windows Defender:

Windows Defender надається безкоштовно з кожною копією операційної системи Windows, починаючи з Windows 8 і вище. Немає потреби купувати

або оновлювати ліцензії для використання Windows Defender, оскільки він є частиною стандартного пакету безпеки Windows.

Переваги Windows Defender:

- Безкоштовний захист: Windows Defender надає безкоштовний базовий захист для всіх користувачів Windows без додаткових витрат.
- Інтеграція з Windows: Глибока інтеграція з операційною системою забезпечує оптимальну продуктивність та мінімальний вплив на роботу комп'ютера.
- Простота використання: Windows Defender автоматично активується та працює у фоновому режимі, не вимагаючи складного налаштування.
- Регулярні оновлення: Постійні оновлення визначень вірусів та програмного забезпечення забезпечують актуальний захист від нових загроз.

Недоліки Windows Defender:

- Обмежені функції: Порівняно з деякими платними антивірусними рішеннями, Windows Defender має обмежений набір функцій.
- Середній рівень захисту: Хоча Windows Defender забезпечує базовий захист, він може не бути таким ефективним, як деякі сторонні антивірусні програми у виявленні та блокуванні новітніх загроз.
- Менший набір додаткових інструментів: Відсутність розширених функцій, таких як VPN, менеджери паролів чи спеціалізовані інструменти для оптимізації системи, які доступні у платних рішеннях.

Інтерфейс Windows Defender:

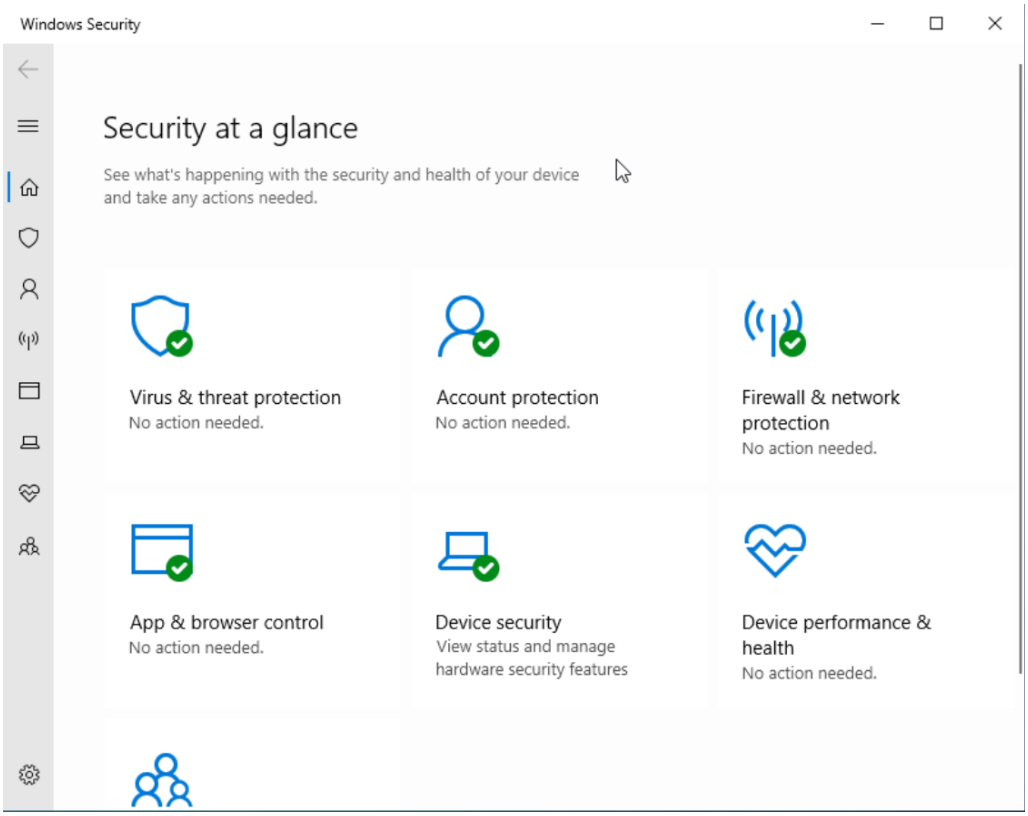

Рисунок 2.9 – головна сторінка

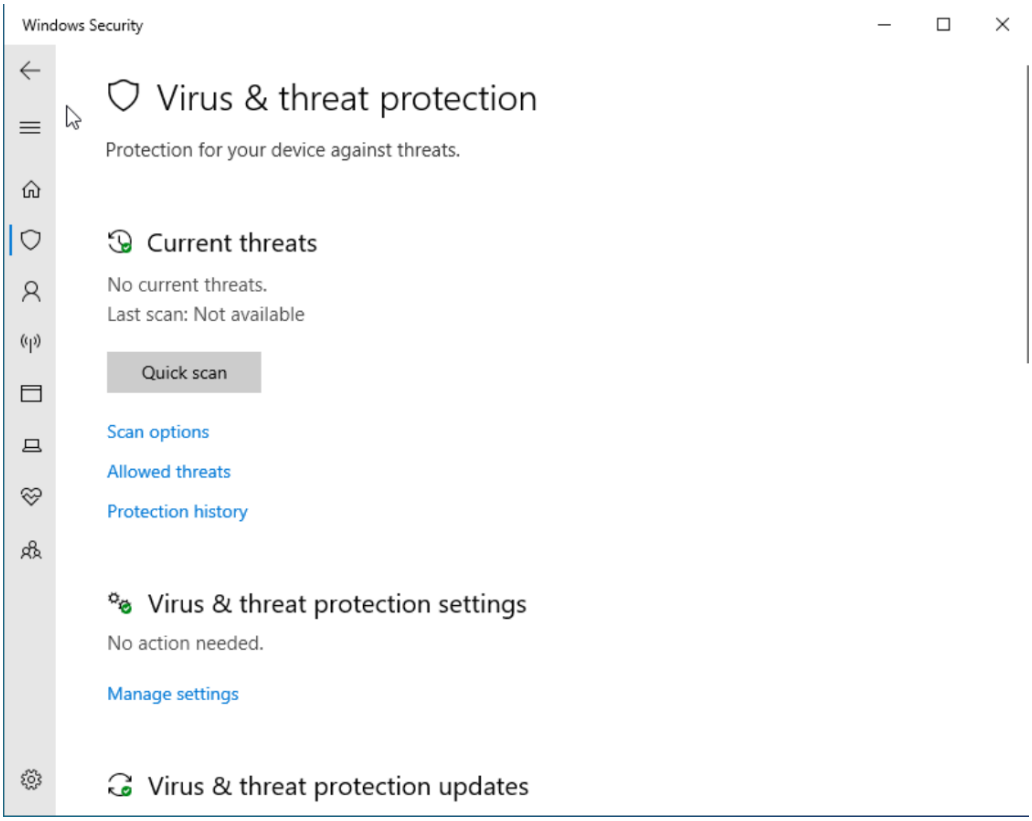

Рисунок 2.10 – сторінка вірусної безпеки

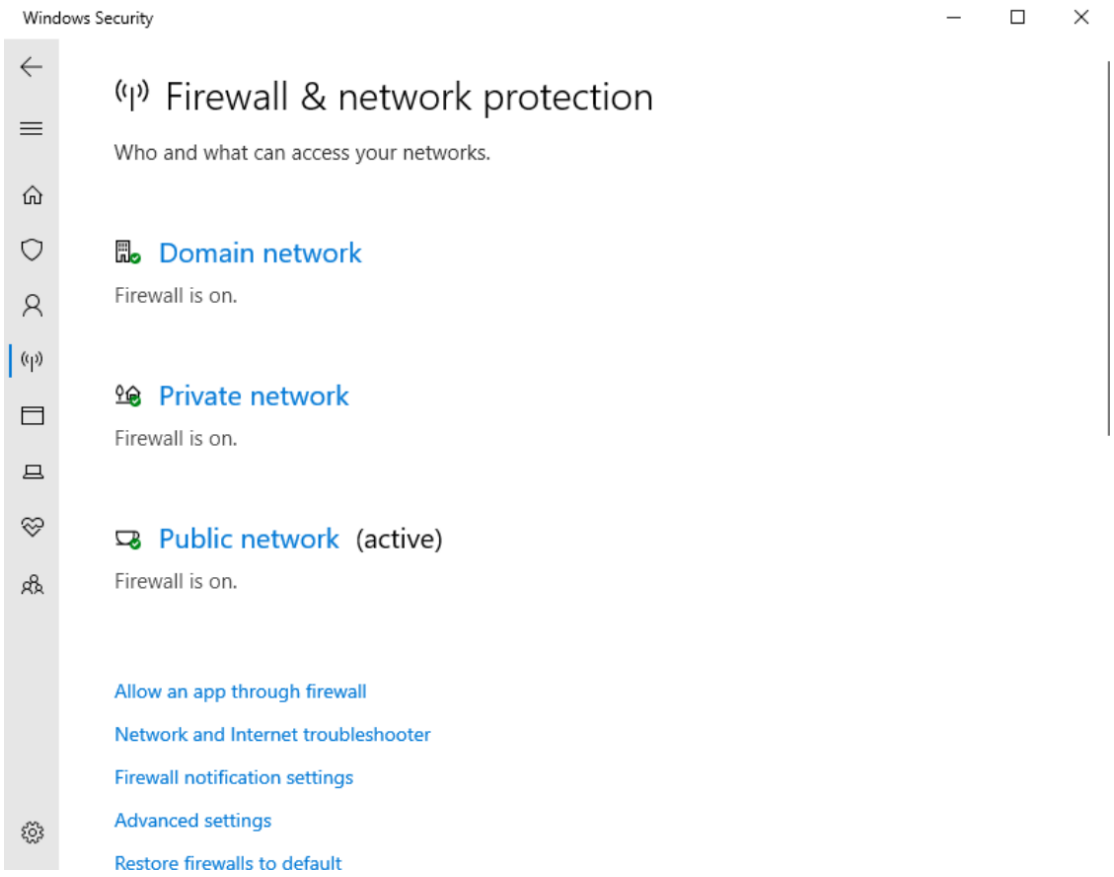

Рисунок 2.11 – сторінка захисту мережи

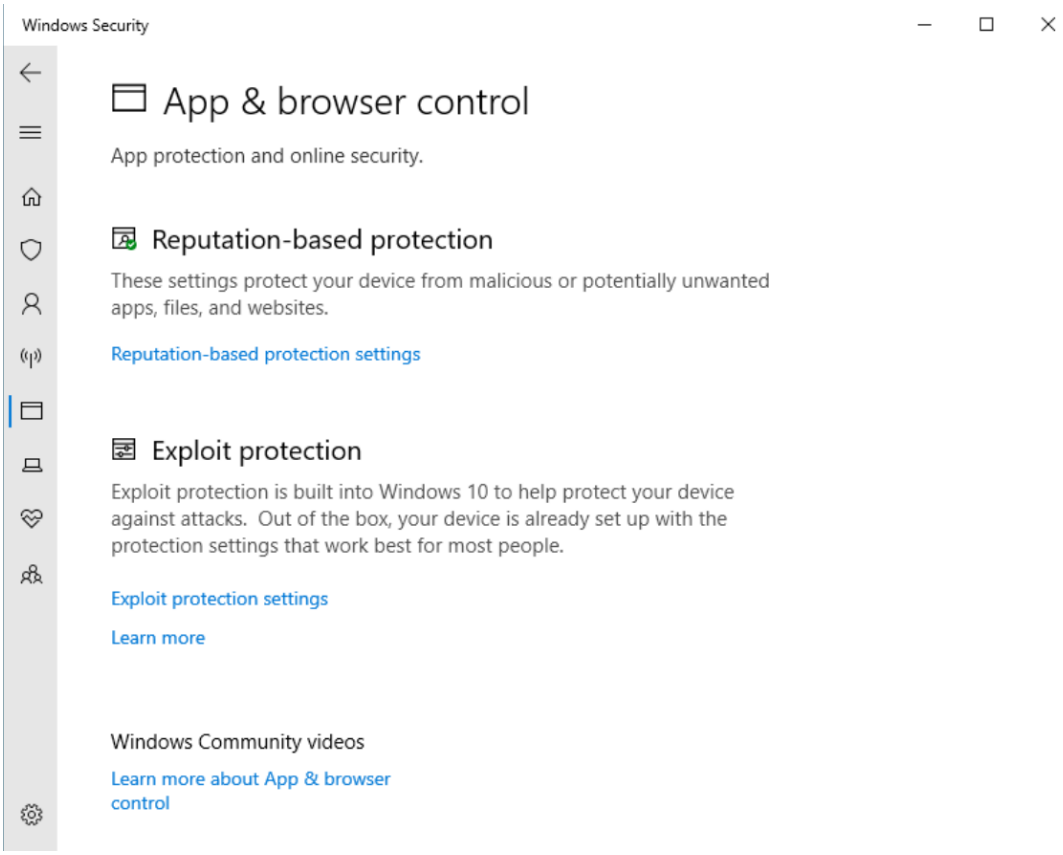

Рисунок 2.12 – сторінка захисту додатків та браузеру

2.4 Порівняння Avast, Bitdefender, Windows Defender

У цьому розділі будуть порівнюватися три обрані комплексні системи захисту цифрового середовища: Avast, Bitdefender та Windows Defender.

Спочатку будемо перевіряти та порівнювати ці системи на практиці.

Встановимо три віртуальні машини з операційною системою Windows 10. На першу віртуальну машину встановимо Avast, на другу – Bitdefender, на третій за замовчуванням буде встановлено Windows Defender. Для першої та другої віртуальної машини вимкнемо повністю усі захисти Windows Defender, щоб він нам не заважав. Ці налаштування можна побачити на рисунках 2.13, 2.14 та 2.15.

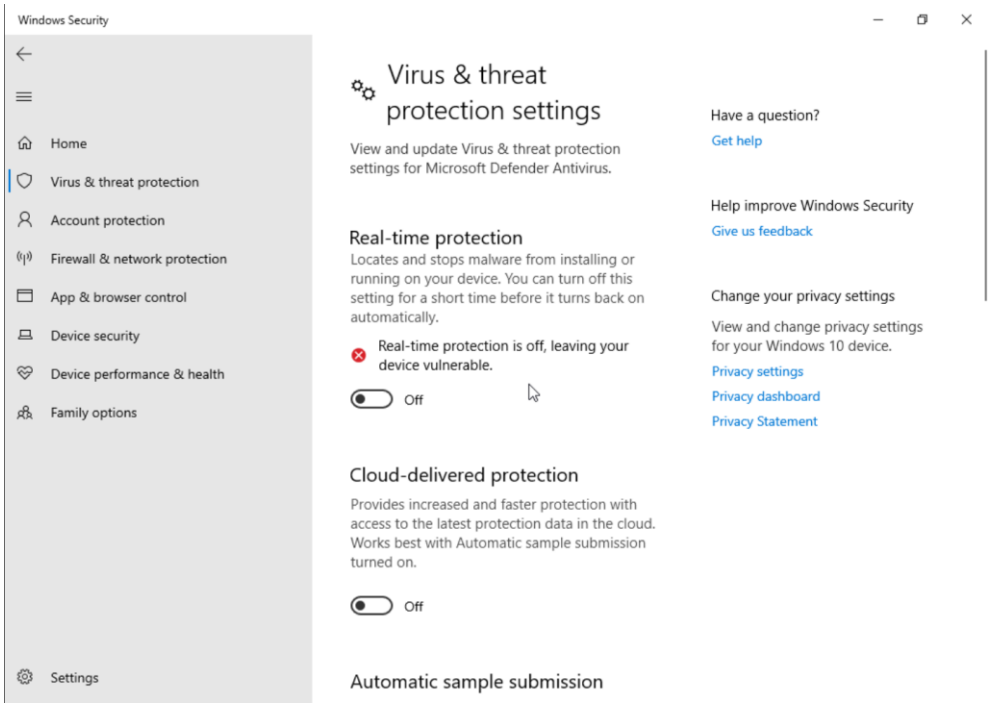

Рисунок 2.13 – вимкнення захисту від вірусів

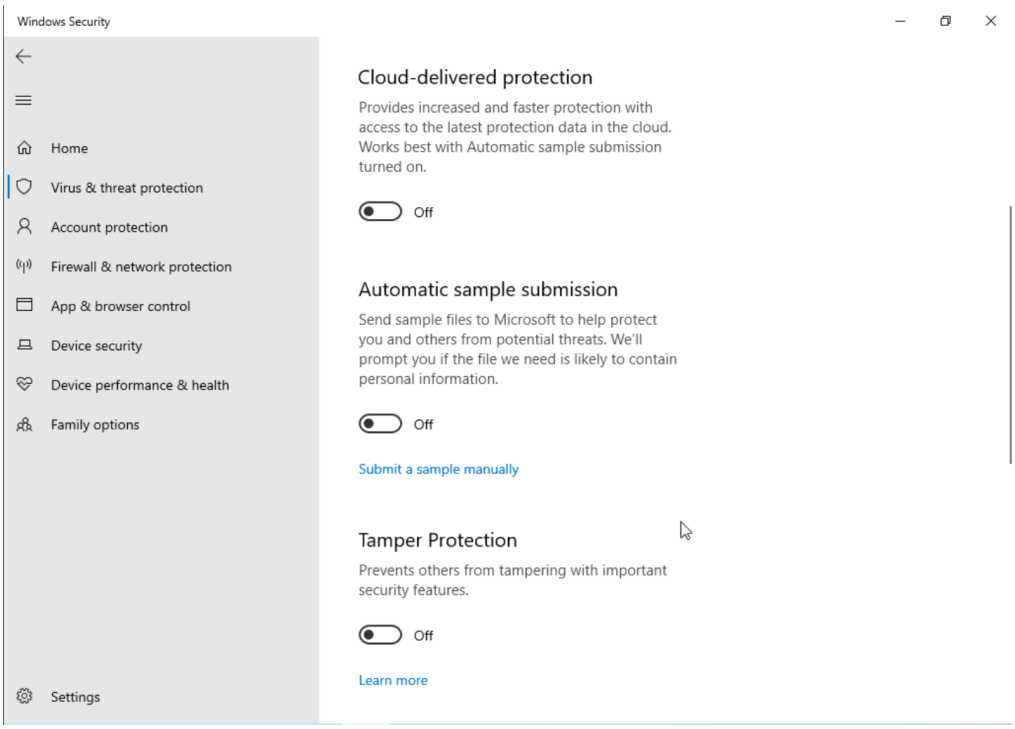

Рисунок 2.14 – вимкнення захисту браузера

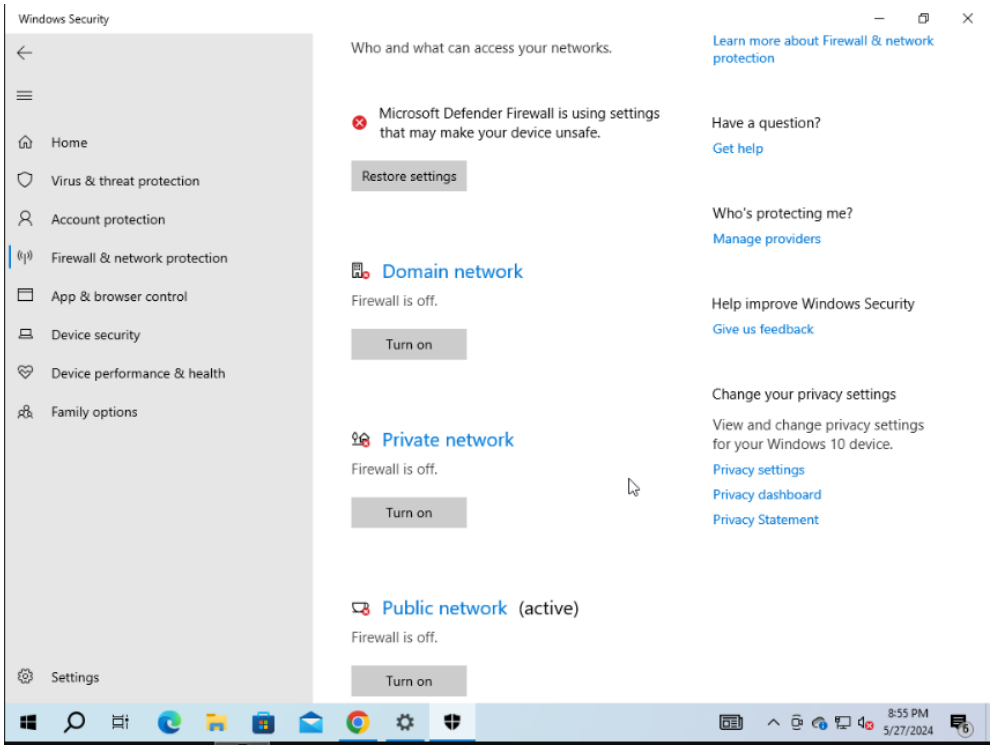

Рисунок 2.15 – вимкнення брандмауеру

На третій віртуальній машині навпаки ввімкнемо усі захисти Windows Defender.(рис. 2.16)

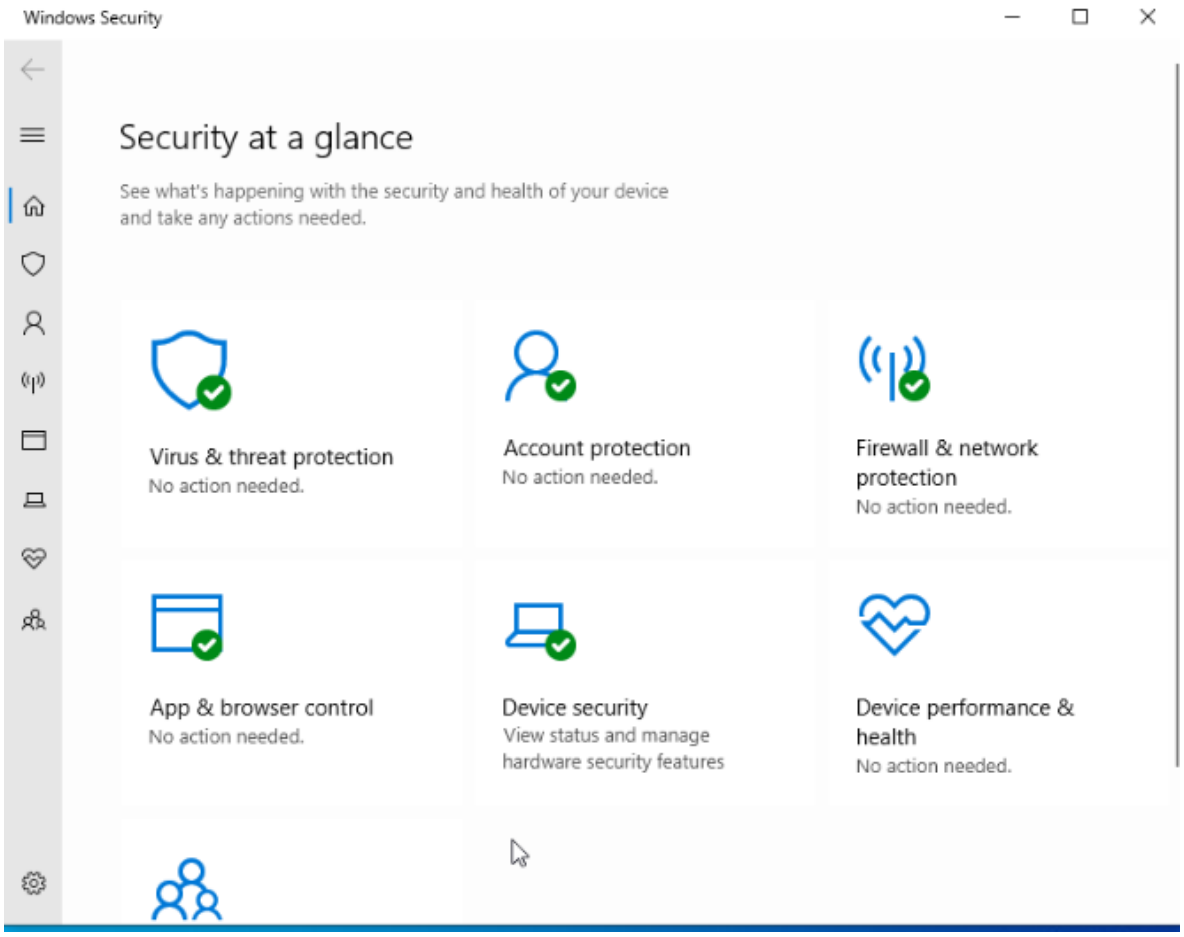

Рисунок 2.16 – налаштування Windows Defender

На усіх трьох віртуальних машинах маємо однакові три вірусні файли: троян, хробак та майнер. Ці файли можна побачити на рисунку 2.17.

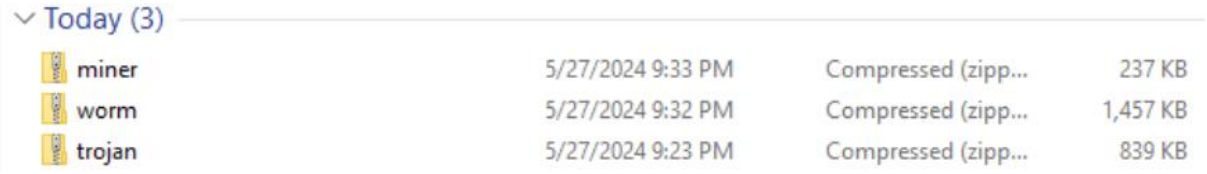

Рисунок 2.17 – вірусні файли

Перевіримо спочатку Avast. Запустивши усі три файли, бачимо, що Avast упорався з усіма, відправивши ці файли у карантин. Результати роботи Avast на рисунках 2.18, 2.19, 2.20.

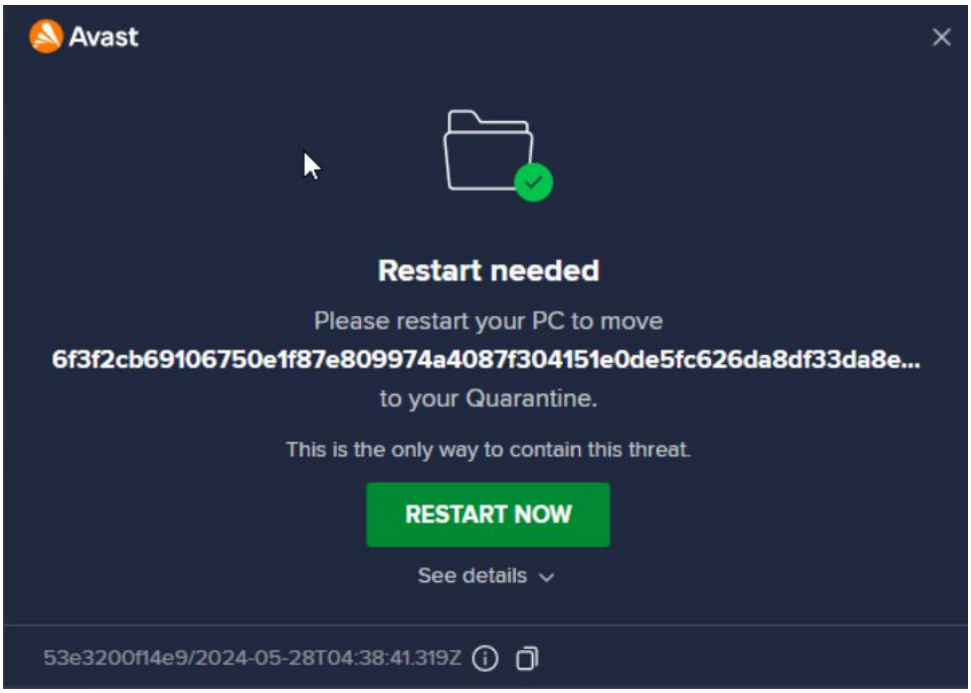

Рисунок 2.18 – реакція Avast на троян

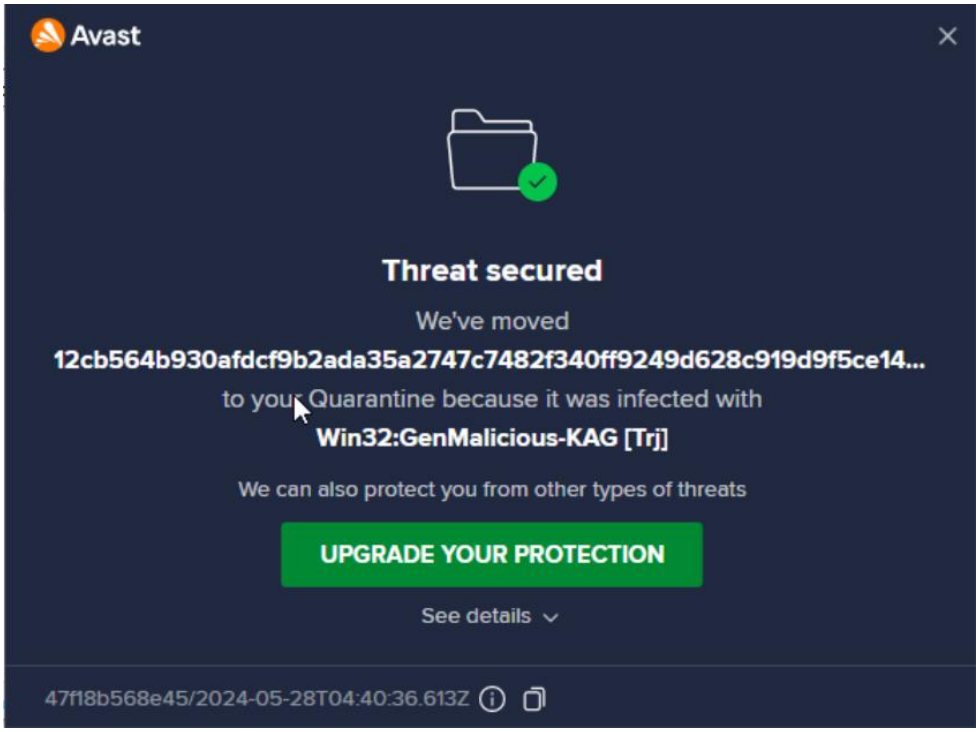

Рисунок 2.19 – реакція Avast на хробака

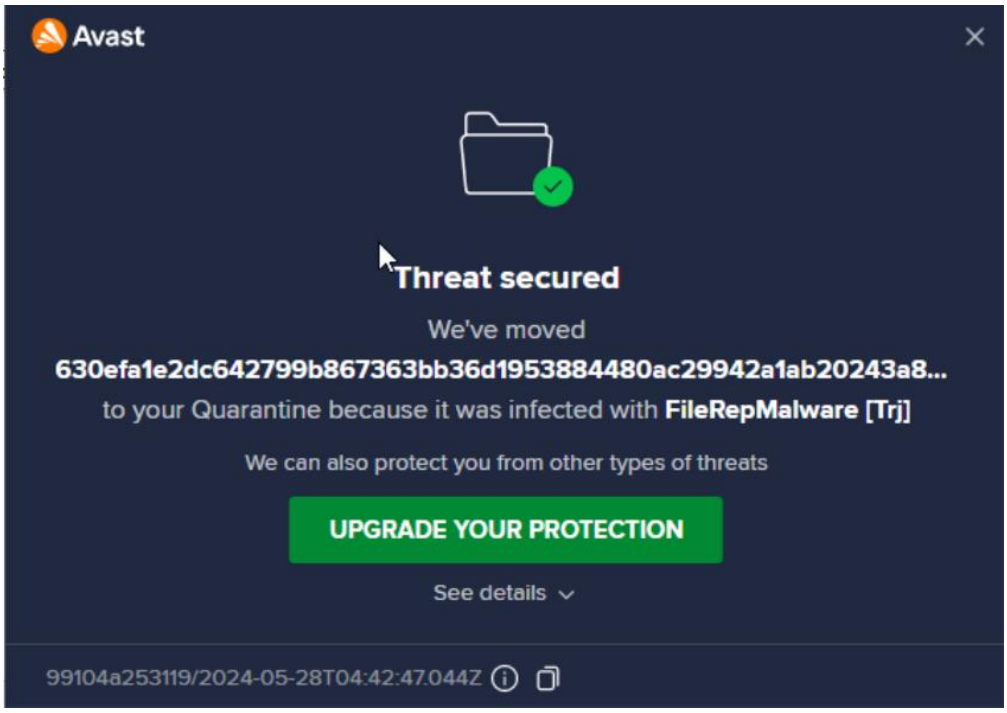

Рисунок 2.20 – реакція Avast на майнер

Далі перевіримо Bitdefender, так само запустивши усі три файли. Bitdefender також впорався з усіма трьома файлами. Результати роботи Bitdefender на рисунках 2.21, 2.22, 2.23.

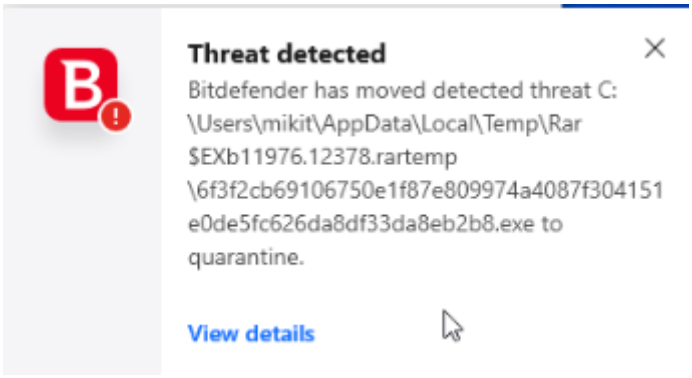

Рисунок 2.21 – реакція Bitdefender на троян

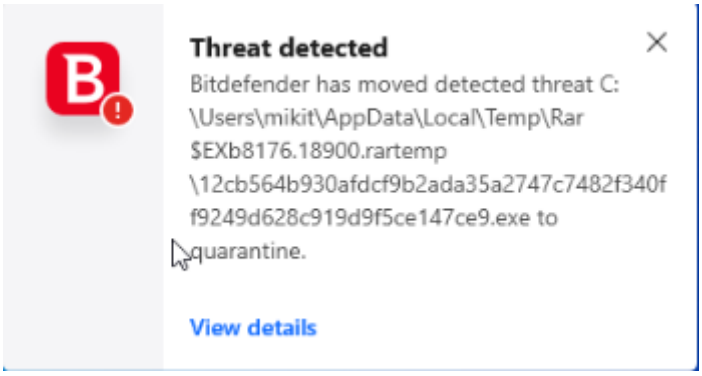

Рисунок 2.22 – реакція Bitdefender на хробака

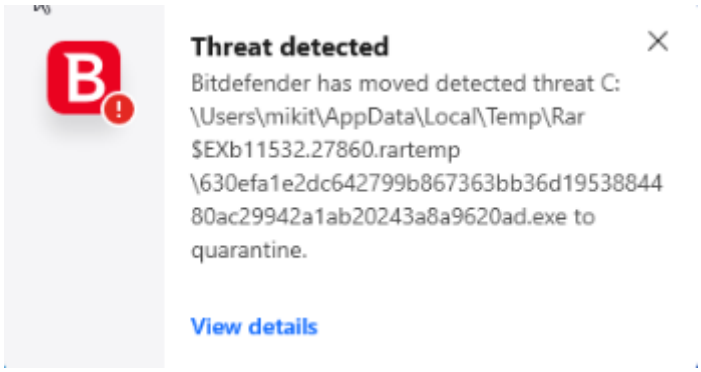

Рисунок 2.23 – реакція Bitdefender на майнер

На останок перевіримо Windows Defender аналогічним методом. Ця комплексна система захисту цифрового середовища також упоралася з усіма трьома вірусами. Результати Windows Defender можна побачити на рисунках 2.24, 2.25, 2.26.

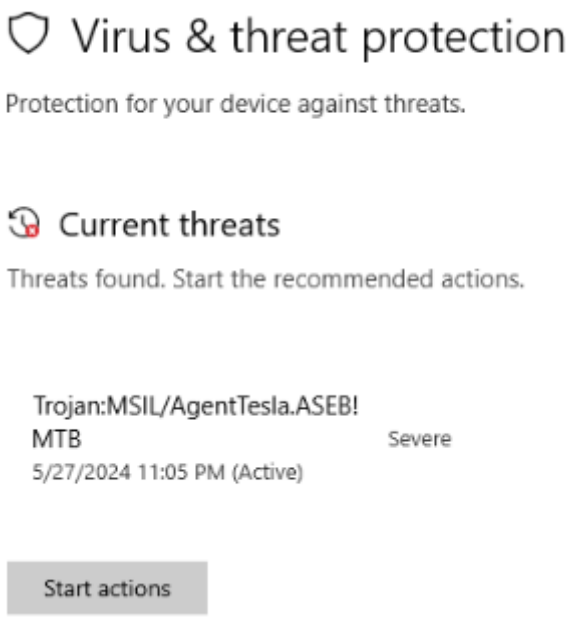

Рисунок 2.24 – реакція Windows Defender на троян

Рисунок 2.25 – реакція Windows Defender на хробака

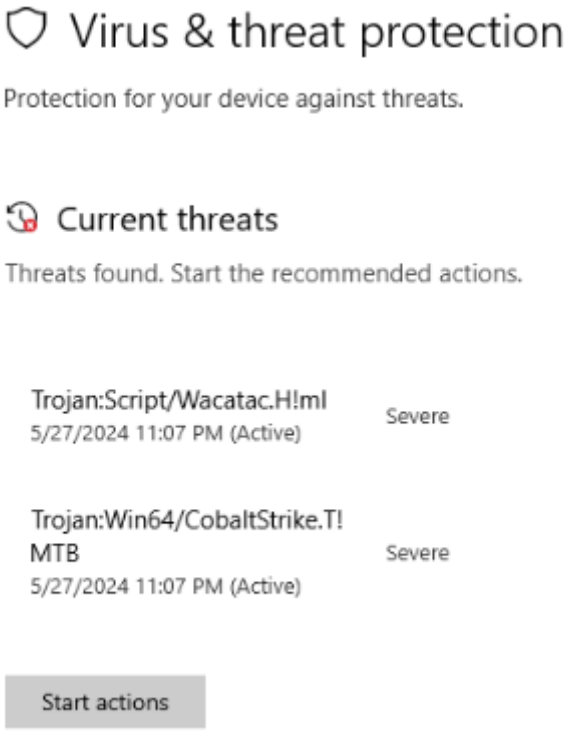

Рисунок 2.26 – реакція Windows Defender на майнер

Також перевіримо, як ці системи впораються с скануванням операційної системи.

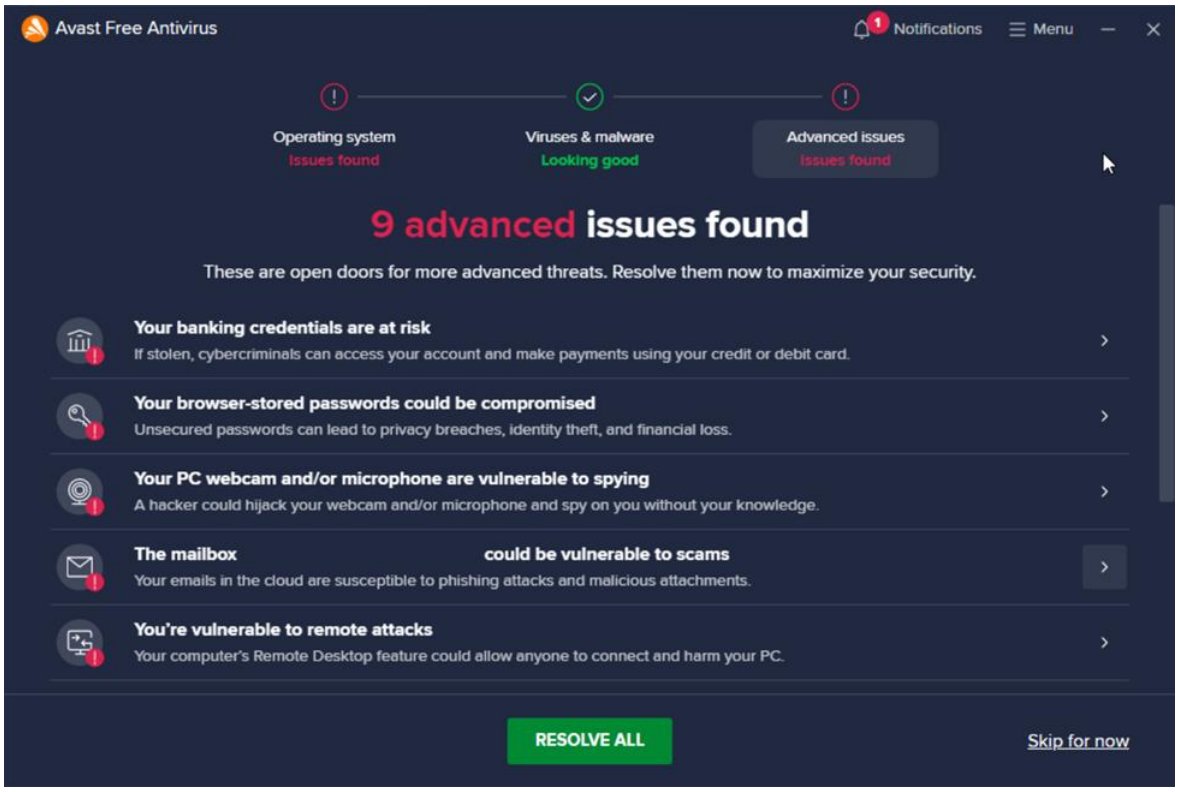

Рисунок 2.27 – результат сканування Avast

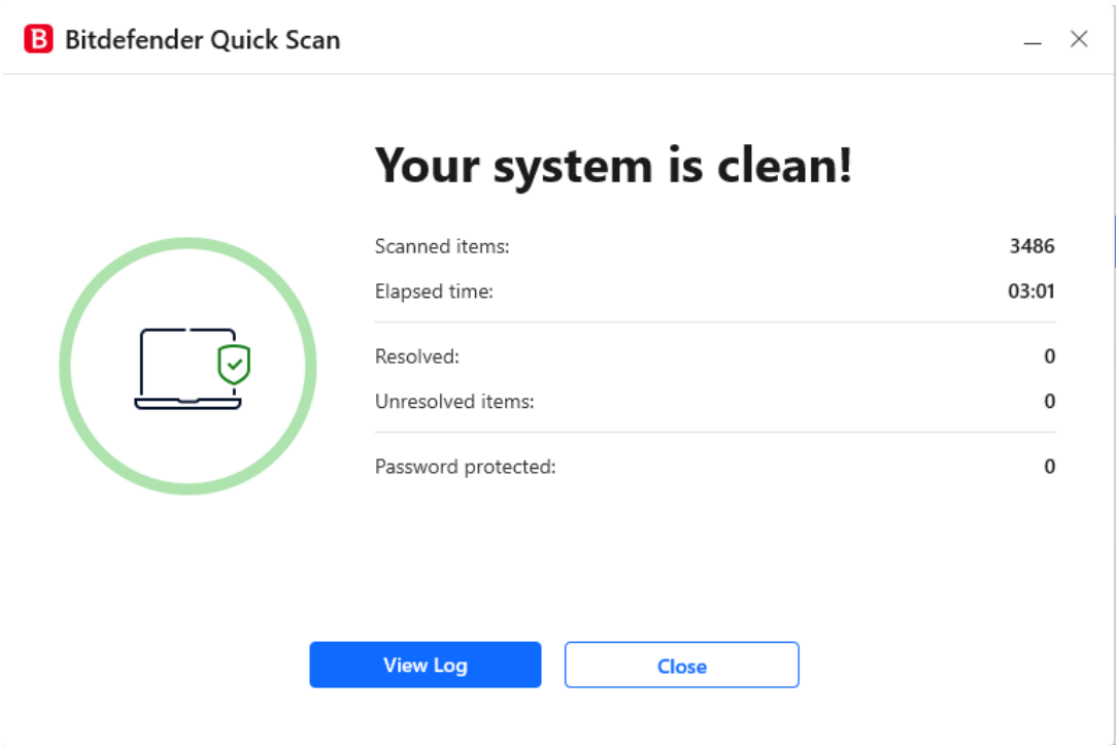

Рисунок 2.28 – результат сканування Bitdefender

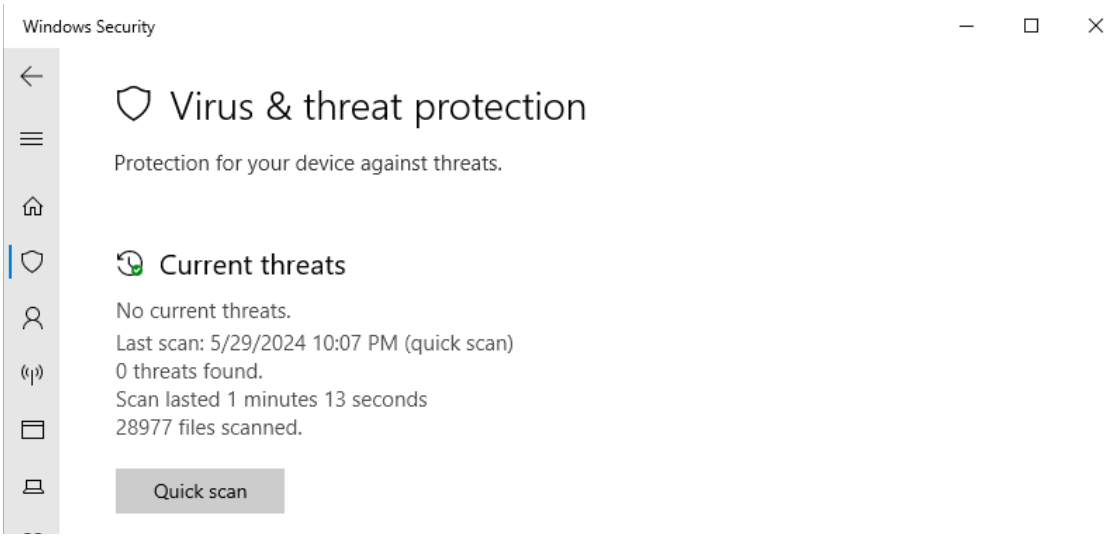

Рисунок 2.29 – результат сканування Windows Defender

На рисунку 2.27 можемо побачити результати сканування Avast. Ця система не знайшла ніяких вірусних файлів, але надала рекомендації, як можна покращити безпеку операційної системи.

На рисунку 2.28 бачимо результати сканування Bitdefender. Система не знайшла вірусні файли та не надала ніяких рекомендацій.

На рисунку 2.29 результати сканування Windows Defender. Як і Bitdefender, ця система не знайшла ніяких вразливостей.

Складемо таблицю порівняння цих трьох комплексних систем захисту цифрового середовища.

Таблиця 2.1 – Порівняльна таблиця Avast, Bitdefender, Windows Defender

Показник	Avast	Bitdefender	Windows Defender
Заснована	1988, Чехія	2001, Румунія	Вбудована в Windows з Windows Vista (2006)
Безкоштовна версія	Так	Так	Так
Платні версії	Так	Так	Ні
Антивірусний захист	Високий	Високий	Середній

Продовження таблиці 2.1

Показник	Avast	Bitdefender	Windows Defender
Захист у реальному часі	Так	Так	Так
Захист веб-браузера	Так (в платній версії)	Так	Так
Захист файлів	Так (в платній версії)	Так	Так
Захист Wi-Fi	Так (в платній версії)	Так	Ні
Брандмауер	Так (в платній версії)	Так	Ні
Захист особистих даних	Так (VPN, менеджер паролів в платній версії)	Так (VPN, менеджер паролів в платній версії)	Ні
Батьківський контроль	Так (в платній версії)	Так (в платній версії)	Так
Оптимізація системи	Ні	Так (в платній версії)	Ні
Хмарний захист	Так	Так	Так
Інтеграція з системою	Середня	Висока	Висока
Простота використання	Висока	Висока	Висока
Ресурсоємність	Середня	Середня/Низька	Низька
Вартість платних версій	Від $50/рік	Від $40/рік	Н/А
Додаткові функції	VPN, менеджер паролів, очищення диску	VPN, менеджер паролів	Ні

Продовження таблиці 2.1

Показник	Avast	Bitdefender	Windows Defender
Переваги	Безкоштовна версія, широкий спектр функцій, простий у використанні, високий рівень захисту	Високий рівень захисту, широкий спектр функцій, інноваційні технології, оптимізація продуктивності	Безкоштовний, глибока інтеграція з Windows, простий у використанні, регулярні оновлення
Недоліки	Показує рекламу у безкоштовній версії, були випадки витоку даних	Висока вартість платних версій, іноді використання ресурсів	Обмежений набір функцій, середній рівень захисту, менше додаткових інструментів

Avast, Bitdefender та Windows Defender є потужними та функціонально багатими системами захисту цифрового середовища. За функціональністю, Avast та Bitdefender знаходяться приблизно на однаковому рівні, в той час як Windows Defender показує трохи гірші результати за цим показником. Що стосується цін, Avast є найдорожчим, тоді як Windows Defender пропонується безкоштовно. Згідно з проведеними функціональними перевірками, усі три системи ефективно справлялись з вірусними файлами, проте найкращі показники сканування демонструє Avast. Якщо аналізувати інтерфейс та зручність користування, Avast та Bitdefender мають переваги перед Windows Defender, оскільки всі функції зібрані у єдиному додатку, на відміну від Windows Defender, де функції розподілені по різних розділах налаштувань операційної системи. Рекомендується обрати між Avast та Bitdefender для забезпечення більш комплексного та надійного захисту.

ВИСНОВКИ

У роботі було проведено порівняльний аналіз комплексних систем захисту цифрового середовища з метою визначення їхньої ефективності, гнучкості та спроможності протистояти сучасним кіберзагрозам.

В рамках дослідження були розглянуті та аналізовані теоретичні відомості щодо комплексних систем захисту цифрового середовища та сучасних загроз його безпеці, використовуючи методи теоретичного аналізу наукової літератури та критичного огляду.

Методами емпіричного дослідження було проведено моделювання атак за допомогою шкідливих файлів, дозволило оцінити реакцію та ефективність програм у реальному часі. Результати дослідження показали, що Avast та Bitdefender забезпечують схожу функціональність і високу ефективність виявлення загроз, тоді як Windows Defender показує трохи нижчі показники за цими критеріями.

Загалом, дослідження підтвердило, що вибір комплексної системи захисту цифрового середовища є складним завданням і кожен користувач повинен ретельно вивчити свої потреби та можливості перед прийняттям остаточного рішення. Важливо враховувати не лише ефективність виявлення загроз і вплив на системні ресурси, але й зручність користування, що може істотно вплинути на досвід взаємодії з програмою. Вибір між Avast, Bitdefender, та Windows Defender залежить від специфічних вимог до ефективності, ціни та користувацького досвіду.

СПИСОК ЛІТЕРАТУРИ

1. Principles of Information Security / Michael E. Whitman and Herbert J. Mattord // Springer, 2022. - C.15-47.

2. Computer Security: Principles and Practice / William Stallings and Lawrie Brown // Apress, 2021.-C.12-74.

3. Computer Security Fundamentals / William (Chuck) Easttom II // No Starch Press, 2022.-C.57-58.

4. Network Security Essentials: Applications and Standards / William Stallings // No Starch Press, 2019.-C.66-90.

5. Cybersecurity: The Essential Body of Knowledge / Dan Shoemaker, Anne Kohnke, and Ken Sigler // Springer, 2021.-C.46-69.

6. Cyber Resilience of Systems and Networks / Alexander Kott and Igor Linkov // Springer, 2019.-C.32-56.

7. Digital Resilience: Is Your Company Ready for the Next Cyber Threat? / Ray Rothrock // AMACOM, 2018. -C.47-66.

8. Risk Management Frameworks for Cybersecurity / John H. Miller and Scott E. Page // Princeton University Press, 2017. -C.23-51.

9. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance / Dhruba Shankar Ray // CRC Press, 2017. -C.43-79.

10. Cybersecurity Attacks - Red Team Strategies: A practical guide to building a penetration testing program inside your organization / Johann Rehberger // Packt Publishing, 2020. -C.31-68.