Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету )

Кафедра кібербезпеки
(повна назва кафедри)

# КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

**бакалавр**
**(освітній рівень)**

Натему: " Порівняльний аналіз превентивного та активного захисту пк від вірусів на основі сучасного антивірусного програмного забезпечення "

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Бережник Євгеній Юрійович
підпис (прізвище та ініціали)

Керівник Лечаченко Т. А.
підпис (прізвище та ініціали)

Нормоконтроль Лобур Т.Б.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

Тернопіль 2023

Міністерство освіти і науки України
**Тернопільський національний технічний університет імені Івана Пулюя**

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2023 р.

# ЗАВДАННЯ
## НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

За спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студента Бережнику Євгенію Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Порівняльний аналіз превентивного та активного захисту пк від вірусів на основі сучасного антивірусного програмного забезпечення

Керівник роботи Лечаченко Тарас Анатолійович, PhD доктор філософії., асистент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 03 » 04 2023 року № 4/7-349 .

2. Термін подання студентом завершеної роботи 14.06.2023

3. Вихідні дані до роботи Програмні вимоги до антивірусних програм

4. Зміст роботи (перелік питань, які потрібно розробити)

Провести теоретичний аналіз понять вірус, антивірусні програми, превентивного та активного захисту

Дослідження превентивного та активного захисту ПК

Здійснити порівняльний аналіз програмного забезпечення активного та превентивного захисту

Безпека життєдіяльності, основи охорони праці

5. Перелік графічного матеріалу (з точним зазначенням слайдів)

Тема, мета, задачі. Поняття активного та превентивного захисту. Методи захисту від різноманітних атак.

Захист від мережевих атак .

| |
|---|
| Приклад можливостей налаштування правил брандмауера. |
| Захист від атак з локальної мережі. |
| Приклади різноманітних атак в мережі. |
| Функції блокування IP. |
| Висновки. |

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Безпека життєдіяльності, основи хорони праці | Пилипець М.І., проф. кафедри МТ | | |

7.Дата видачі завдання 20.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

| н/п | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Ознайомлення з завданням до кваліфікаційної роботи | 20.01 – 23.01 | Виконано |
| 2. | Підбір програмного забезпечення для аналізу активного захисту | 25.01 – 05.02 | Виконано |
| 3. | Підбір програмного забезпечення для аналізу превентивного захисту | 06.02 – 20.02 | Виконано |
| 5. | Проведення аналізу активного та превентивного захисту програмного забезпечення. | 15.03-25.03 | Виконано |
| 6. | Здійснив порівняння програм превентивного та активного захисту | 25.02 – 10.04 | Виконано |
| 7. | Оформлення розділу «Теоретичні основи » | 10.02 – 05.03 | Виконано |
| 8. | Оформлення розділу «Превентивний та активний захист ПК » | 26.03 – 04.05 | Виконано |
| 9. | Оформлення розділу «Порівняння антивірусних програм активного та превентивного захисту» | 12.04-20.04 | |
| 10. | Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці» | 25.04 – 10.05 | Виконано |
| 11. | Оформлення кваліфікаційної роботи | 23.05 – 08.06 | Виконано |
| 12. | Нормоконтроль | 10.06 – 15.06 | Виконано |
| 13. | Перевірка на плагіат | 20.06 – 22.06 | Виконано |
| 14. | Попередній захист кваліфікаційної роботи | 14.06 – 15.06 | Виконано |
| 15. | Захист кваліфікаційної роботи | 23.06.2023 | |

Студент _____ Бережник Є. Ю.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Лечаченко Т. А.
(підпис) (прізвище та ініціали)

# АНОТАЦІЯ

Порівняльний аналіз превентивного та активного захисту пк від вірусів на основі сучасного антивірусного програмного забезпечення // Кваліфікаційна робота освітнього рівня «Бакалавр» // Бережник Євгеній Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль 2023 // С.82 , рис. - 33, таблиці - 3.

Ключові слова: ПРЕВЕНТИВНМЙ ЗАХИСТ, АКТИВНИЙ ЗАХИСТ, ФАЄРВОЛ, АНТИВІРУС

Кваліфікаційна робота присвячена порівнянню аналізу превентивного та активного захисту пк від вірусів на основі сучасного антивірусного програмного забезпечення , використовуючи програмне забезпечення для проведення аудиту, а також організаційні заходи. В роботі порівняно превентивний та активний захист пк від вірусів.

При порівнянні превентивного та активного захисту пк від вірусів було виявлено недоліки та переваги антивірусних програм активного та превентивного захисту.

# ANNOTATION

Comparative analysis of preventive and active protection against viruses on PCs based on modern antivirus software // Berezhnyk Yevhenii Yuriyovich/ Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, group SBs-41 // Ternopil 2023 // P.82, fig. - 33, Tables - 3.

Keywords: PREVENTIVE PROTECTION, ACTIVE PROTECTION, FIREWALL, ANTI-VIRUS.

The qualification work is devoted to the comparison of the analysis of preventive and active protection of PCs against viruses based on modern anti-virus software, using audit software, as well as organizational measures. The work is relatively preventive and active protection of the PC against viruses.

When comparing preventive and active PC protection against viruses, the disadvantages and advantages of active and preventive anti-virus programs were revealed.

Зміст

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IDS - Intrusion Detection System

IPS - Intrusion Prevention System

GTOC - Global Trajectory Optimization Competition

# ВСТУП

За останні десятиліття сучасні інформаційні технології зазнали значного розвитку, що призвело до широкого поширення персональних комп'ютерів (ПК) в різних сферах життя. Однак, разом з цим зростає й загроза комп'ютерним вірусам, які можуть спричинити серйозні проблеми та негативно вплинути на безпеку і працездатність ПК. Щоб забезпечити ефективний захист від цих загроз, розробники створюють різні антивірусні програмні продукти.

Однак, вибір оптимального засобу захисту є складним завданням, оскільки на ринку існує багато антивірусних програмних продуктів, які використовують різні підходи до захисту від вірусів. Два основних підходи - превентивний захист та активний захист - заслуговують на особливу увагу.

Превентивний захист базується на попередньому виявленні і блокуванні вірусів шляхом використання антивірусних програм, вірусних баз даних, аналізу поведінки програм та фаєрволів. Цей підхід спрямований на запобігання потенційним загрозам та забезпечення безпеки ПК.

З іншого боку, активний захист передбачає виявлення та блокування вірусів в реальному часі. Цей підхід використовує різноманітні технології, такі як реал-тайм аналіз, інтелектуальні системи виявлення загроз та інші, щоб негайно реагувати на потенційні загрози та забезпечити безпеку ПК.

Предметом дипломної роботи є порівняльний аналіз превентивного та активного захисту ПК від вірусів сучасних антивірусних програмних продуктів Об'єкт дослідження є засоби захисту ПК від вірусів, зокрема превентивний захист та активний захист, які реалізовані у сучасних антивірусних програмних продуктах.

Мета даної дипломної роботи полягає в порівняльному аналізі превентивного та активного захисту ПК від вірусів сучасних антивірусних програмних продуктів. Дослідження спрямоване на визначення переваг і недоліків кожного підходу, їхнього впливу на продуктивність ПК, а також оцінку

вартості та доступності цих засобів захисту. Крім того, робота враховує психологічні причини нещасних випадків і травматизму, а також соціальне значення охорони праці.

Порівняльний аналізу превентивного та активного захисту ПК від вірусів сучасних антивірусних програмних продуктів включає вирішення таких завдань:

1. Проаналізувати основні принципи, технології та функції превентивного захисту ПК, включаючи вірусні бази даних, аналіз поведінки програм, фаєрволи та інші аспекти.
2. Дослідити технології активного захисту ПК, такі як реал-тайм аналіз, системи виявлення загроз, інтелектуальні системи та інші методи, які надають можливість негайно реагувати на потенційні загрози.
3. Здійснити порівняльний аналіз переваг і недоліків превентивного та активного захисту ПК від вірусів сучасних антивірусних програм, зокрема їхньої ефективності, впливу на продуктивність ПК, вартості та доступності для користувачів.
4. Зробити висновки щодо оптимального вибору засобу захисту ПК від вірусів, а також рекомендації щодо покращення захисту ПК.

У подальших розділах дипломної роботи будуть розглянуті теоретичні основи превентивного та активного захисту ПК, огляд сучасних антивірусних програмних продуктів, а також проведений порівняльний аналіз переваг і недоліків цих підходів.

# 1 ТЕОРЕТИЧНІ ОСНОВИ

## 1.1. Історія мережевого вірусу

З поширенням комп'ютерів і підключення їх до глобальної мережі Інтернет стало актуальним питання зараження комп'ютерних вірусами. Комп'ютерний вірус - це невелика програма, яка самовільно приєднується до інших програм і створює свої копії, впроваджуючись у файли і системні області комп'ютера, а також поширюючись до інших підключених комп'ютерів з метою завдання шкоди, перешкоди в роботі програм і пошкодження файлів [2].

Термін "комп'ютерний вірус" був введений Фредеріком Коеном, співробітником Лехайського університету в США, на конференції з безпеки інформації в 1984 році. Однак поява програм, схожих на комп'ютерні віруси, відноситься до середини минулого століття, коли Джон фон Нейман і Норберт Вінер виявили можливість саморозмноження програмного коду.

Згідно з даними інтенсивність вірусних інцидентів у світі постійно зростає. Кількість повідомлень про атаки комп'ютерних вірусів та шкідливих кодів зростає, разом зі збитками, завданими світовому співтовариству. Таким чином, проблема комп'ютерних вірусів стала важливим питанням з поширенням комп'ютерів та підключенням їх до мережі Інтернет. Велика кількість вірусів та шкідливих програм призводить до значних збитків і порушення нормальної роботи систем.

У світовій практиці комп'ютерної вірусології електронна пошта залишається основним джерелом загрози для організацій і приватних осіб. Понад 96% усіх зареєстрованих випадків вірусів були пов'язані з електронною поштою. Через неї поширюються не лише "мережні хробаки", але і звичайні віруси, включаючи "троянські коні". Зараження комп'ютерів вірусами через інші служби Інтернету, такі як FTP, IRC, становило 2,3%. Зараження комп'ютерів вірусами через заражені мобільні носії інформації вірус Emotet, який у 2020 році був

одним з найпоширеніших вірусів. Він поширювався через електронну пошту та використовувався для розповсюдження інших шкідливих програм, таких як троянські коней та рейтингові ботнети. Цей вірус може бути переданий через вкладені файли в електронних листах, включаючи файли, розташовані на мобільних носіях. Більшість вірусів змінюють системні файли комп'ютера, щоб активуватися при кожному завантаженні. Деякі віруси спеціалізуються на інфікуванні файлів завантаження системи, інші на програмних файлах типу EXE, COM і т.д. Кожного разу, коли користувач копіює файли на диск або передає їх по мережі, інфіковані файли намагаються поширитися на новий носій [5].

Зазвичай віруси розробляються з метою активації при виникненні певної події, такої як п'ятниця 13-е, конкретна дата, певна кількість перезавантажень, відсоток заповнення жорсткого диска і т.д.

Після виконання потрібних дій вірус передає керування програмі, в якій він знаходиться, і її робота протягом деякого часу не відрізняється від роботи незараженої програми. Дії вірусу можуть виконуватися швидко і без видимих повідомлень [3].

Для підвищення безпеки важливо звертати увагу на походження програми (чи є вона з надійного джерела, чи має сертифікат, чи була використана раніше і т.д.). Однак головна причина зараження комп'ютерів вірусами полягає в відсутності ефективних захисних засобів в операційних системах для захисту інформації від несанкціонованого доступу.

Згідно з даними спеціалізованої літератури, у світовій практиці зареєстровано близько 70 тисяч комп'ютерних вірусів, і нові віруси з'являються щотижня. Одна зі схем класифікації комп'ютерних вірусів включає такі типи: завантажувальні, файлові, системні, мережеві та файлово-загрузочні:

- Завантажувальні віруси впроваджуються в завантажувальний сектор або диск, що містить програму завантаження системного диска.
- Файлові віруси переважно заражають виконувані файли з розширенням .COM і .EXE.

- Системні віруси проникають до системних модулів і драйверів пристроїв, таблиць розміщення файлів і таблиць розділів.
- Мережеві віруси активні в комп'ютерних мережах, а файлово-загрузочні віруси вражають завантажувальні сектори дисків і файли прикладних програм [2].

За способом зараження середовища віруси можуть бути резидентними або нерезидентними. Резидентні віруси залишають свою резидентну частину в оперативній пам'яті комп'ютера при зараженні, що дозволяє їм перехоплювати звернення операційної системи до інших об'єктів, впроваджуватися в них і виконувати руйнівні дії до моменту вимкнення або перезавантаження комп'ютера. Нерезидентні віруси не заражають оперативну пам'ять ПК і активні лише протягом обмеженого часу.

Алгоритмічні особливості побудови вірусів впливають на їх прояв та функціонування. Наприклад, реплікаторні програми швидко розмножуються, що може призвести до переповнення основної пам'яті, і видалення програм-реплікаторів ускладнюється, якщо відтворені програми не є точними копіями оригіналу.[1]

## 1.2. Визначення понять "превентивний захист" та "активний захист"

В сучасному цифровому світі, де використання персональних комп'ютерів (ПК) є невід'ємною частиною нашого повсякденного життя, захист комп'ютерних систем від вірусів і кіберзагроз стає вельми важливим завданням. Для забезпечення безпеки ПК і збереження важливої інформації існують різні підходи, серед яких превентивний захист і активний захист є ключовими поняттями. У даній роботі ми детально розглянемо ці два поняття та надамо їм визначення [6].

1. Превентивний захист.

Превентивний захист означає прийняття запобіжних заходів та застосування передбачуваних стратегій для запобігання виникненню вірусів та інших кіберзагроз на ПК. Цей підхід передбачає використання заходів безпеки, що спрямовані на запобігання вразливості системи до атак і недозволеному доступу до неї. Превентивний захист включає в себе регулярне оновлення антивірусного програмного забезпечення, встановлення і актуалізацію фаєрволів, сканування на наявність шкідливих програм та вірусів, а також надання рекомендацій щодо безпечного користування ПК. Наприклад, встановлення і регулярне оновлення антивірусного програмного забезпечення є одним із найпоширеніших методів превентивного захисту. Це дозволяє виявляти та блокувати потенційно шкідливі програми перед тим, як вони встигнуть пошкодити систему. Інші заходи превентивного захисту можуть включати налаштування міцних паролів, обмеження прав доступу, резервне копіювання даних тощо [3].

2. Активний захист.

Активний захист відноситься до заходів безпеки, що приймаються для виявлення, блокування та нейтралізації потенційних кіберзагроз на ПК. У цьому підході використовуються різноманітні технології, такі як системи виявлення і запобігання вторгнень (IDS/IPS), антишпигунські програми, анти-фішингові та анти-спам фільтри, а також інші інструменти, які мають на меті виявлення та блокування шкідливих програм і небажаних дій на ПК. Активний захист передбачає також реагування на виявлені загрози шляхом швидкого вжиття заходів для їхнього усунення і мінімізації наслідків.

Наприклад, системи виявлення і запобігання вторгнень є одними з інструментів активного захисту, які аналізують мережевий трафік і шукають ознаки атак або незвичайних поведінкових патернів. Якщо виявляється потенційна загроза, система активно реагує, блокуючи атаку та ізолюючи комп'ютер від загрози. Інші приклади активного захисту включають системи

раннього виявлення загроз, ефективні механізми фільтрації спаму, анти-фішингові та анти-спам фільтри.[3]

Основою системи є Protocol Analysis Module, який поєднує аналізатор поведінки та метод сигнатурного виявлення. Цей модуль може виявляти небезпечний код шляхом аналізу більш як трьох тисяч алгоритмів, включаючи алгоритми виявлення DoS атак. Крім того, система використовує вбудований брандмауер для контролю доступу до портів і IP.

Застосування технології Virtual Patch дозволяє системі блокувати віруси ще на етапі їх поширення, а також забезпечує захист комп'ютерів до оновлення системи захисту. Адміністратори можуть створювати власні сигнатури атак в разі потреби. Також присутній модуль для контролю за додатками, який дозволяє блокувати небезпечні додатки. Для виявлення спроб передачі конфіденційної інформації і переміщення даних в мережі використовується спеціальний модуль DLP [7].

Система Security Network Intrusion Prevention System надає кілька варіантів реагування при виявленні атаки або аномалії, такі як блокування хоста, надсилання попередження, логування трафіку під час атаки і ізоляція вузла мережі. Політику безпеки можна гнучко налаштовувати для кожної окремої IP-адреси або VLAN. Система може працювати навіть у разі виходу з ладу одного з вузлів завдяки спеціальному режиму. Крім того, якщо використовуються декілька продуктів від IBM, їх можна об'єднати в єдину систему та здійснювати управління з центру управління.

Превентивність захисту забезпечується через постійне відстеження різноманітних загроз в спеціально розробленому центрі безпеки – GTOC. Цей центр безпеки дозволяє системі вчасно реагувати на нові загрози та адаптувати свої захисні механізми.[9]

Security Network Intrusion Prevention System має широкий спектр можливостей, що включають [10]:

- Підтримку 167 різних протоколів, включаючи протоколи рівня додатків і формати даних.
- Використання понад 2500 алгоритмів для аналізу трафіка з метою виявлення вразливостей.
- Використання нової технології Virtual Patch, яка забезпечує захист комп'ютерів до встановлення оновлень.
- Наявність вбудованого режиму пасивного моніторингу і двох режимів встановлення на канал.
- Підтримку багатьох зон безпеки одним пристроєм, включаючи зони VLAN.
- Наявність вбудованих та зовнішніх bypass-модулів для безперервної передачі потоку даних при системних помилках або відключенні енергопостачання.
- Використання технології FlowSmart.
- Різноманітні способи реагування на системні події, включаючи логування пакетів атаки.
- Контроль витоків інформації у даних та офісних документах, що передаються по різних протоколах.

Використання рішень Security Network Intrusion Prevention System має такі переваги [10]:

- Превентивний захист забезпечує блокування атак ще на ранніх етапах, запобігаючи несанкціонованому доступу до ресурсів мережі.
- Звіти та архіви подій, які створюються в результаті постійного аналізу, надають повну інформацію про події в мережі і дозволяють відповідати вимогам стандартів безпеки.

Ці можливості і переваги допомагають забезпечити ефективний та надійний захист мережі підприємства від різних загроз.

Превентивний захист і активний захист є двома важливими поняттями у сфері безпеки комп'ютерних систем. Превентивний захист передбачає

застосування запобіжних заходів та стратегій, щоб запобігти виникненню вірусів та кіберзагроз на ПК. Напроти, активний захист включає виявлення, блокування та нейтралізацію потенційних загроз шляхом використання спеціалізованих інструментів та технологій.

Прикладами превентивного захисту є встановлення антивірусного програмного забезпечення, регулярне оновлення програм і операційних систем, налаштування міцних паролів та обмеження прав доступу. У той же час, прикладами активного захисту є системи виявлення і запобігання вторгнень, системи раннього виявлення загроз, фільтри спаму та анти-фішингові заходи.

Усвідомлення різниці між превентивним та активним захистом допомагає користувачам ПК вибрати відповідні інструменти і стратегії для забезпечення безпеки своїх систем. Комбінація обох підходів може стати оптимальним рішенням для ефективного захисту ПК від вірусів та кіберзагроз [11].

Отже, превентивний захист і активний захист відіграють критичну роль у забезпеченні безпеки комп'ютерних систем і повинні розглядатися як взаємодоповнюють один одного, сприяючи надійному захисту від вірусів та інших кіберзагроз.

## 1.3. Роль антивірусних програмних продуктів у захисті ПК

У цифрову епоху, коли наші комп'ютери стали неодмінною частиною повсякденного життя, забезпечення безпеки цих пристроїв має вирішальне значення. З ростом кількості і складності загроз, що існують в онлайн-середовищі, важливо мати надійні і ефективні засоби захисту. Антивірусні програмні продукти є вітальними інструментами, які допомагають убезпечити наші персональні комп'ютери (ПК) від шкідливих програм, зловмисного програмного забезпечення та інших загроз [2]:

1. Виявлення та блокування шкідливого програмного забезпечення: Антивірусні програмні продукти використовують потужні алгоритми та

бази даних для виявлення відомих вірусів, троянських програм, черв'яків та інших шкідливих програм. Вони аналізують активні процеси, файли, архіви та вхідні дані, спостерігають за незвичними діями і підозрілими активностями. Якщо будь-яка загроза виявляється, антивірусна програма вживає заходів для її блокування та нейтралізації.

2. Захист в реальному часі: Сучасні антивірусні програми працюють в режимі реального часу, що означає, що вони постійно моніторять активність системи, вхідні та вихідні файли, електронну пошту та веб-сторінки. Це дозволяє виявляти та блокувати нові загрози негайно, навіть до їх розповсюдження та завдання шкоди.
3. Оновлення вірусних баз даних: Антивірусні програми постійно оновлюють свої вірусні бази даних, щоб розпізнавати нові шкідливі програми, які з'являються щодня. Це важливо, оскільки загрози постійно еволюціонують, і тільки актуальна база даних може надати ефективний захист.
4. Захист від інтернет-загроз: Антивірусні програми забезпечують захист під час веб-серфінгу, блокуючи шкідливі веб-сторінки, фішингові сайти та шкідливі посилання. Вони також забезпечують захист від шкідливих електронних листів, завантажених вкладень та інших онлайн-загроз.
5. Додаткові функції: Сучасні антивірусні програми можуть мати додаткові функції, які покращують загальний рівень захисту ПК. Наприклад, вони можуть включати фаєрволи, які контролюють вхідний та вихідний інтернет-трафік, антиспам-фільтри для захисту від небажаних електронних листів, а також функції шифрування для захисту конфіденційної інформації.

За середовищем існування віруси можна поділити на файлові, завантажувальні, макровіруси та мережеві. Файлові віруси впроваджуються в виконувані файли або створюють файли-двійники, використовуючи особливості файлової системи. Завантажувальні віруси порушують роботу

завантажувального сектора диска. Мережеві віруси використовують мережеві протоколи або електронну пошту для поширення.

Особливості алгоритму роботи вірусів включають резидентність, самошифрування і поліморфізм, а також використання нестандартних прийомів. Резидентний вірус залишає свою частину в оперативній пам'яті комп'ютера, що дозволяє йому перехоплювати звернення операційної системи до заражених об'єктів і виконувати свої дії. Він залишається активним в пам'яті до вимкнення комп'ютера або перезавантаження операційної системи.

Таким чином, розуміння класифікації вірусів за різними ознаками дозволяє краще розуміти їхню природу і виявляти їх для подальшого захисту комп'ютерів та інформації [10].

Нерезидентні віруси відрізняються від резидентних тим, що вони не заражають пам'ять комп'ютера і не зберігають активність постійно. Вони можуть заражати файли або завантажувальний сектор, але їх дія обмежена у часі. Наприклад, макровіруси можна вважати резидентними, оскільки вони завжди присутні в пам'яті комп'ютера. Роль операційної системи при виявленні резидентних вірусів виконує відповідний редактор, а поняття "перезавантаження операційної системи" розглядається як вихід з редактора.

Самошифрування і поліморфізм використовуються практично всіма типами вірусів для ускладнення процедури виявлення. Поліморфні віруси не містять постійних ділянок коду і шифрують основну частину вірусу, використовуючи програму-розшифровувач. Це призводить до того, що два зразки того самого поліморфного вірусу можуть не мати жодних спільних рядків [11].

Віруси часто використовують різні нестандартні прийоми для глибокого приховування в ядрі операційної системи, захисту резидентної частини, ускладнення лікування від вірусу і т.д. Це дозволяє їм бути більш стійкими до виявлення та видалення.

За деструктивними можливостями віруси можна класифікувати на нешкідливі, безпечні і небезпечні. Нешкідливі віруси не завдають шкоди комп'ютеру, крім зменшення вільної пам'яті на диску під час свого поширення. Безпечні віруси також не заважають роботі комп'ютера і мають обмежений вплив, який проявляється у зменшенні вільної пам'яті та створенні ефектів, таких як зміни графіки або звуку. Небезпечні віруси можуть призводити до серйозних збоїв у роботі комп'ютера, втрати програм та даних, знищення важливої інформації, що зберігається в системних областях пам'яті, а навіть до фізичних пошкоджень рухомих частин пристроїв, таких як голівки жорстких дисків [12].

Віруси можна класифікувати і за іншими ознаками, існують різні підходи до цієї класифікації. Деякі з них включають віруси-хробаки, які поширюються по комп'ютерних мережах, віруси-невидимки, які важко виявити і знешкодити, і віруси-мутанти, які мають різні алгоритми шифрування-розшифрування, що призводить до відсутності спільних ланцюжків байтів у копій вірусу. Також існують троянські програми, які, хоч і не можуть самостійно поширюватись, є небезпечними, оскільки маскуються під корисні програми та завдають шкоди системі.

На практиці віруси зазвичай поділяють на три основних класи [14]:

1. Програми-віруси: це програми, які заражають інші програми, змінюючи їх таким чином, щоб "заражені" файли містили копію вірусу. Вони можуть додавати свій модуль до програми або модифікувати її код.
2. Хробаки: це програми, які можуть самостійно поширюватися від одного комп'ютера до іншого, часто через комп'ютерні мережі. Вони можуть розмножуватися, використовуючи різні механізми передачі, і поширюються без потреби "заражених" файлів або програм.
3. Троянські коні: це самостійні програми, які приховуються під корисними або звичайними програмами. Вони намагаються виглядати безпідозренно, але насправді мають зловмисні цілі, такі як збір конфіденційної інформації або незаконний доступ до системи.

Щодо програм виявлення і захисту від вірусів, існує кілька видів антивірусних програм:

- Програми-детектори: вони шукають характерні сигнатури вірусів в пам'яті і файлах, щоб виявити їх наявність.
- Програми-доктори або фаги: вони не тільки виявляють заражені файли, але й спробують вилікувати їх, видаливши вірусну частину.
- Програми-ревізори: ці програми зберігають початковий стан програм, файлів і системних областей диска, а потім порівнюють його з поточним станом для виявлення змін, що можуть свідчити про наявність вірусів.
- Програми-фільтри: вони спостерігають за характеристиками дій, які можуть вказувати на наявність вірусів або зловмисних дій, і вживають заходів для їх блокування або сповіщення про них.
- Програми-вакцини, або імунізатори: ці програми надають проактивний захист, запобігаючи зараженню вірусами шляхом виявлення і блокування потенційно небезпечних файлів або дій.

Сучасні антивірусні програми включають різні модулі, такі як евристичні модулі для виявлення нових вірусів, монітори для постійного контролю в оперативній пам'яті, поштові програми для перевірки електронної пошти, сканери для виявлення і видалення відомих вірусів, мережеві екрани для захисту від хакерських атак тощо [15].

Деякі популярні антивірусні програми, які вважаються ефективними, включають, Norton 360, AVAST і багато інших.

Антивірусні програмні продукти грають важливу роль у захисті ПК від шкідливого програмного забезпечення та онлайн-загроз. Вони забезпечують виявлення, блокування та нейтралізацію вірусів та інших шкідливих програм у режимі реального часу. Завдяки постійному оновленню вірусних баз даних, вони здатні розпізнавати нові загрози та надавати надійний захист. Додаткові функції дозволяють підвищити рівень безпеки ПК і захистити користувачів від широкого

спектру загроз в онлайн-середовищі. Отже, використання надійних антивірусних програмних продуктів є необхідним елементом безпеки в цифровому світі [10].

## 1.4. Огляд сучасних антивірусних програмних продуктів

Антивірусні програмні продукти виконують важливу роль у захисті комп'ютерів і інших пристроїв від шкідливих програм, вірусів і інших загроз з Інтернету. Нові загрози постійно з'являються, тому важливо мати ефективні антивірусні рішення, які можуть ефективно виявляти і нейтралізувати ці загрози. У цьому огляді ми розглянемо деякі з найкращих сучасних антивірусних програмних продуктів, які забезпечують надійний захист для користувачів [11].

При виборі антивірусного програмного продукту важливо враховувати власні потреби, можливості та надійність компанії-розробника. Завжди рекомендується також оновлювати програму й використовувати додаткові заходи безпеки, такі як оновлення операційної системи і застосунків, для максимального захисту вашого комп'ютера чи пристрою.

В комп'ютерних мережах поширені різноманітні види шкідливих програм, таких як хробаки, троянські коні, логічні бомби, програми-мутанти, віруси-невидимки та макровіруси. Кожен з цих типів вірусів має свої особливості та можливості, і їх вплив на комп'ютерні системи може бути різним [4].

Хробаки є програмами, які незалежно розповсюджуються через комп'ютерну мережу, використовуючи адреси інших комп'ютерів. Вони можуть підтримувати зв'язок між собою та ширитися, намагаючись знайти нові цільові комп'ютери. Якщо один з хробаків припиняє своє існування на певному ПК, решта може впровадити свої копії на інших вразливих комп'ютерах.

Троянські коні маскуються під корисні програми та виконують додаткові функції, які можуть бути шкідливими для користувача. Вони можуть збирати конфіденційну інформацію, таку як паролі і імена, і передавати їх зловмисникам або навіть руйнувати файлову систему.

Логічні бомби є програмами, які активуються при настанні певної події або умови. Вони можуть спрацювати після певної кількості виконання програми, наявності або відсутності певного файлу і т. д. Логічні бомби можуть мати негативний вплив на комп'ютерну систему або призвести до втрати даних.

Програми-мутанти самостійно відтворюються і створюють копії, які відрізняються від оригіналу. Це ускладнює виявлення і лікування таких вірусів.

Віруси-невидимки або стелс-віруси перехоплюють звертання операційної системи до заражених файлів і секторів дисків, замінюючи їх на незаражені об'єкти. Такі віруси використовують складні алгоритми, щоб ухилятися від резидентних антивірусних моніторів [5].

Макровіруси використовують можливості макромов, що вбудовані в офісні програми, такі як текстові редактори та електронні таблиці. Вони можуть впроваджувати свій код в макроси і ширитися через документи, що містять такі макроси.

Залежно від ступеня впливу на ресурси комп'ютерних систем і мереж та від рівня деструктивних можливостей, віруси можуть бути класифіковані як нешкідливі, безпечні, небезпечні або руйнівні. Нешкідливі віруси не завдають серйозної шкоди, але можуть спричиняти переповнення оперативної пам'яті через своє розмноження. Безпечні віруси можуть впливати на роботу системи шляхом зменшення вільного простору на диску, відображення графічних ефектів тощо. Небезпечні віруси можуть призводити до серйозних порушень у роботі комп'ютера, а руйнівні віруси можуть спричинити повне або часткове знищення даних і прикладних програм [6].

Для боротьби з комп'ютерними вірусами було розроблено антивірусні програми. Вони використовують різні методи, включаючи пошук сигнатур вірусів, щоб виявляти і знищувати шкідливі програми. Бази даних сигнатур вірусів регулярно оновлюються, щоб забезпечити ефективне виявлення нових вірусів. Крім того, існують інші методи боротьби з вірусами, такі як фільтри, ревізори-доктори, детектори та вакцини.

Загалом, антивірусні програми відіграють важливу роль у захисті комп'ютерних систем від шкідливих програм і допомагають забезпечити безпеку даних та стабільну роботу комп'ютерів [7].

Програми-фільтри, також відомі як "сторожі", постійно знаходяться в оперативній пам'яті комп'ютера і перехоплюють запити до операційної системи, що мають підозрілий характер. Вони перевіряють ці запити на виконання дій, які часто використовуються вірусами для пошкодження комп'ютера або його даних, наприклад, зміну атрибутів файлів, корекцію виконуваних файлів, запис у завантажувальні сектори диска та інші. Кожен раз, коли такий запит надходить, програма-фільтр виводить повідомлення на екран комп'ютера, вказуючи, яка дія була запитана і яка програма намагається її виконати. Користувач може дозволити або заборонити виконання цієї дії. Однак, постійна наявність програми-фільтра в оперативній пам'яті і повторюваність цих повідомлень можуть стати дратівливими для користувача, а також зменшити обсяг доступної пам'яті. Програми-фільтри не можуть "лікувати" або відновлювати пошкоджені файли або диски, для цього потрібно використовувати інші антивірусні програми. Більш надійним засобом захисту від вірусів є програми-ревізори. Вони запам'ятовують початковий стан програм, каталогів і системних областей диска, коли комп'ютер ще не був заражений вірусом, і періодично порівнюють його з поточним станом. Якщо виявляються невідповідності (наприклад, зміна розміру файлу, дати модифікації, контрольної суми файлу тощо), програма повідомляє про це користувача. Програми-доктори, які також відомі як антивіруси, можуть виявляти та "лікувати" заражені файли або диски, видаляючи віруси з них. Ці програми поділяються на фаги та поліфаги. Фаги призначені для виявлення і знищення конкретного вірусу, тоді як поліфаги здатні виявляти і знищувати багато різних вірусів. Програми-детектори дозволяють виявляти файли, які заражені відомими розробниками вірусів. Вакцини-імунізатори, також відносяться до резидентних програм. Вони модифікують файли або диски таким чином, що вірус вже розглядає їх як заражені, і не може впровадитись у них.

Існує велика кількість антивірусних програм, розроблених компаніями та фахівцями як в іноземних, так і вітчизняних організаціях. Багато з них постійно оновлюються новими методами боротьби з вірусами і супроводжуються розробниками. В Україні популярністю серед користувачів комп'ютерів користується антивірусний комплект "Доктор Веб", розроблений ЗАТ "Діалог-Наука". Він включає різні компоненти, призначені для захисту корпоративних мереж, робочих станцій, автономних комп'ютерів (для домашнього користування) та спеціалізованих рішень. "Доктор Веб" підтримує різні операційні системи, включаючи Windows, DOS, OS/2, Novell NetWare, Linux, FreeBSD, Solaris і багато інших. Особливістю антивірусної програми "Доктор Веб" є наявність трьох методів виявлення вірусів: за їх сигнатурою, за допомогою евристичного аналізатора і за допомогою емулятора процесора. Пошук за сигнатурою дозволяє швидко виявити відомі вірусні зразки, використовуючи базу даних антивірусної програми. Евристичний аналізатор дозволяє виявити віруси, для яких ще немає сигнатур у базі даних. Емулятор процесора допомагає боротися зі складними шифрованими і поліморфними вірусами [8].

Сімейство програм Doctor Web має модульну структуру, що дозволяє їм працювати на різних програмних платформах. Воно складається з таких компонентів: оболонка, спеціально розроблена для конкретного середовища; ядро, яке незалежне від середовища; та вірусна база, яка постійно оновлюється. Ця структура дозволяє використовувати ту саму вірусну базу Doctor Web для різних платформ, підключати ядро до різних оболонок і додатків, а також автоматично оновлювати вірусні бази і версії оболонки і ядра через Інтернет.

Антивірусний сканер Doctor Web проводить перевірку файлів, каталогів і дисків комп'ютера відповідно до налаштувань користувача. Він також здійснює повну перевірку всієї пам'яті комп'ютера, включаючи системну пам'ять і пам'ять віртуальних машин. Цей сканер виявляє і ліквідовує складні віруси, включаючи "троянські коні" і програми-крадії паролів для доступу до Інтернету.[9]

Антивірусна програма SplDer Guard є резидентним сторожем, тобто постійно перебуває в пам'яті комп'ютера. Вона використовує те ж ядро і вірусну базу, що й інші сканери Doctor Web, але може автоматично виконувати всі перевірки без втручання користувача. Програма виявляє і ліквідує різні типи вірусів, включаючи завантажувальні, файлові, макрокомандні та HTML-віруси, а також здійснює перевірку і видалення вірусів з оперативної пам'яті.[9]

Для операційної системи Novell NetWare в сімействі Doctor Web існує антивірусна програма, яка запускається на сервері і дозволяє проводити перевірку томів сервера за попередньо заданим розкладом, перевіряти прихожих файлів, повідомляти адміністратора про інфіковані файли та вести протокол перевірки.

Антивірусний модуль Dr. Web для операційних систем Linux, FreeBSD і Solaris, який називається програмою-демоном. Ця програма перевіряє електронну пошту, яка проходить через поштовий сервер, і виступає також як спамфільтр.

Також у сімействі Doctor Web є антивірусний модуль для поштової програми The Bat!, який дозволяє перевіряти вхідну пошту на наявність вірусів і вживати відповідні заходи, такі як переміщення листів до карантину, вилікування заражених частин листів або їх видалення.

Doctor Web регулярно оновлює вірусні бази, щоб швидко реагувати на нові віруси. Доповнення до вірусної бази доступні для завантаження з їхнього веб-сервера.[10]

Антивірусна програма Doctor Web працює як у повноекранному режимі з використанням меню і діалогових вікон, так і в режимі командного рядка. Користувач може використовувати потрібні налаштування через основне меню, такі як тестування, налаштування і доповнення.

Окрім цього, з'явилися антивірусні програми, призначені для захисту в мережевих операційних системах. AntiViral Toolkit Pro для Novell NetWare (AVPN) може виявляти, лікувати, видаляти і переміщати заражені файлі на

серверах Novell NetWare. Вона може сканувати файли, що надходять і відправляються через сервер, і має режими фільтра і сканера для постійного контролю.[12]

Антивірусні програми, такі як AVPN, також мають можливість видалення, переміщення і лікування заражених об'єктів, детектування невідомих вірусів за допомогою евристичного аналізу, перевірки упакованих і архівних файлів, а також можуть відключати заражені станції від мережі. Вони також мають зручні схеми поповнення антивірусної бази, можуть надсилати повідомлення про зараження по мережі, електронній пошті і на пейджер, а також здійснювати автоматичне ведення файлу-звіту про виконані операції і керування програмою з робочої станції.

# 2 ПРЕВЕНТИВНИЙ ТА АКТИВНИЙ ЗАХИСТ ПК

## 2.1. Принципи та функції активного та превентивного захисту

Превентивний захист є важливою складовою в сфері кібербезпеки і має на меті запобігати появі загроз і вразливостей, а не просто реагувати на них після виникнення. Основні принципи та функції превентивного захисту включають [7]:

1. Регулярні оновлення: Превентивний захист передбачає постійне оновлення програмного забезпечення, операційних систем, антивірусних баз та інших компонентів системи. Це дозволяє отримувати нові версії з виправленнями помилок, патчі безпеки і оновлення, які запобігають використанню вразливостей зловмисниками.
2. Встановлення міцних паролів: Використання складних і унікальних паролів для доступу до систем і облікових записів є важливим принципом превентивного захисту. Міцні паролі мають складатися з комбінації великих і малих літер, цифр та спеціальних символів.
3. Використання двофакторної аутентифікації: Використання двофакторної аутентифікації (2FA) додає додатковий рівень захисту до процесу автентифікації. Крім пароля, користувач повинен підтвердити свою особу через додатковий фактор, наприклад, через SMS-повідомлення, мобільний додаток або апаратний пристрій.
4. Захист від шкідливих програм: Встановлення і оновлення антивірусного програмного забезпечення, яке виявляє та блокує шкідливі програми, віруси і троянські програми, є важливою функцією превентивного захисту. Регулярне сканування системи на наявність вірусів також допомагає запобігти їх поширенню.
5. Захист мережі: Встановлення брандмауера, мережевих маршрутизаторів і інших засобів захисту допомагає забезпечити безпеку мережі.

Налаштування фільтрації трафіку, блокування небезпечних портів і контроль доступу до мережевих ресурсів допомагають уникнути несанкціонованого доступу до системи.

6. Регулярні резервні копії: Виконання регулярних резервних копій важливих даних і системних налаштувань дозволяє відновити інформацію в разі втрати або пошкодження. Це допомагає запобігти втратам даних внаслідок атак, помилок або випадкових ситуацій.
7. Навчання користувачів: Проведення навчання користувачів про основні принципи кібербезпеки, виявлення фішингових атак, безпечну роботу з електронною поштою та іншими онлайн-ресурсами є важливим аспектом превентивного захисту. Інформовані користувачі зменшують ризик виконання небезпечних дій та падають жертвами шахраїв і зловмисників.

Ці принципи та функції превентивного захисту допомагають зменшити ризик кібератак і зберегти систему та дані в безпеці.

Активний захист ПК - це підхід до захисту комп'ютера, який передбачає активне втручання інструментів і технологій для запобігання атакам і негативним наслідкам безпекових загроз. Він забезпечує проактивний підхід до захисту, активно виявляючи, блокуючи і усуваючи загрози, навіть перед тим, як вони завдають шкоди системі [11].

Основні принципи та функції активного захисту ПК включають:

1. Виявлення загроз: Активний захист включає в себе механізми, які аналізують активність інформаційної системи, виявляють підозрілу або небажану активність, таку як спроби вторгнення, віруси, шпигунське програмне забезпечення тощо.
2. Блокування загроз: Після виявлення загроз активні захисні механізми можуть автоматично блокувати атаку або небажану активність. Це може включати блокування шкідливого трафіку, програм або вторгнення, а також обмеження доступу до вразливих ділянок системи.

3. Антивірусний та антималварний захист: Активний захист включає в себе застосування антивірусних і антималварних технологій для виявлення, блокування і видалення вірусів, шкідливого програмного забезпечення і інших загроз.
4. Захист від фішингу і шахрайства: Активний захист може включати функції, які захищають користувачів від фішингових атак, шахрайства та інших видів соціально-інженерних загроз. Він може блокувати підозрілі веб-сайти, перевіряти електронну пошту на наявність шахрайських повідомлень та надавати попередження користувачам про потенційні ризики.
5. Моніторинг системи: Активний захист може включати моніторинг системи в реальному часі для виявлення незвичайної активності або аномалій. Він може використовувати методи аналізу журналів, мережевого трафіку, системних параметрів тощо для виявлення потенційних загроз.
6. Захист від вторгнень: Активний захист може включати застосування інструментів, таких як брандмауери і системи виявлення вторгнень, для захисту від нелегітимного доступу до системи. Він може блокувати небажаний мережевий трафік і сповіщати про можливі вторгнення.
7. Захист від витоку даних: Активний захист може включати механізми захисту від витоку конфіденційної інформації, таких як перехоплення даних, несанкціонований доступ до файлів тощо. Він може застосовувати шифрування даних, контроль доступу і моніторинг даних для запобігання витоку інформації.

Ці принципи та функції активного захисту спільно допомагають забезпечити безпеку комп'ютерної системи, захистити дані і ресурси від вторгнень, вірусів, шкідливого програмного забезпечення та інших загроз.

Ось кілька прикладів функцій активного захисту ПК [13]:

1. Антивірусне програмне забезпечення: Воно виявляє та блокує віруси, троянські програми, шпигунське ПЗ та інші шкідливі програми.

Наприклад, антивірусна програма може автоматично сканувати файли та папки на наявність вірусів, а також аналізувати веб-трафік для виявлення потенційно небезпечних веб-сайтів.

2. Брандмауер: Це програма, яка контролює мережевий трафік і встановлює правила доступу до комп'ютера. Брандмауер може блокувати небажаний вхідний трафік, захищаючи систему від несанкціонованого доступу та атак з мережі.
3. Антишпигунське програмне забезпечення: Воно виявляє та видаляє шпигунське програмне забезпечення, яке збирає особисту інформацію користувача без його дозволу. Таке програмне забезпечення може перешкоджати шпигунським програмам відслідковувати активність користувача та викрадати конфіденційні дані.
4. Анти-фішинговий захист: Ця функція виявляє фішингові атаки, які намагаються вибрати конфіденційну інформацію (таку як паролі, номери банківських карт) шляхом підробки веб-сайтів або електронних повідомлень. Вона сповіщає користувача про підозрілі веб-сайти та намагається запобігти втраті конфіденційних даних.
5. Захист від вторгнень (Intrusion Prevention System, IPS): Ця технологія аналізує мережевий трафік для виявлення атак зламу або вторгнень і приймає заходи для їх блокування. Вона може реагувати на підозрілий трафік, блокувати атаки та захищати систему від несанкціонованого доступу.

Ці функції активного захисту працюють разом для забезпечення безпеки ПК, допомагаючи виявляти, блокувати та нейтралізувати потенційні загрози.

## 2.2. Технології активного та превентивного захисту

Ось кілька прикладів використання принципів та функцій превентивного захисту в реальному житті [9]:

1. Оновлення програмного забезпечення: Користувач регулярно оновлює операційну систему свого комп'ютера, а також встановлює оновлення для веб-браузера, антивірусного програмного забезпечення та інших програм. Це дозволяє отримувати нові версії з виправленнями помилок і патчами безпеки, що запобігають використанню вразливостей зловмисниками.
2. Використання міцних паролів: Користувач створює складний пароль для свого облікового запису, використовуючи комбінацію великих і малих літер, цифр та спеціальних символів. Він також уникав використання очевидних паролів, таких як "password" або "123456", і створює унікальні паролі для кожного свого облікового запису.
3. Використання двофакторної аутентифікації: Користувач активує двофакторну аутентифікацію на своєму електронному поштовому акаунті. Тепер, крім введення пароля, він отримує SMS-повідомлення з одноразовим кодом, який потрібно ввести для підтвердження своєї особи. Це додає додатковий рівень захисту до його облікового запису.
4. Використання антивірусного програмного забезпечення: Корпорація встановлює антивірусне програмне забезпечення на всі свої комп'ютери та сервери. Програма регулярно сканує системи на наявність шкідливих програм і блокує їх виявлення. Вона також автоматично оновлюється, щоб розпізнавати нові види загроз.
5. Резервне копіювання даних: Користувач регулярно створює резервні копії своїх важливих даних на зовнішній жорсткому диску або в хмарному сховищі. Це забезпечує можливість відновлення даних у разі їх втрати або пошкодження внаслідок кібератаки, технічної несправності або інших непередбачуваних ситуацій.

Ці приклади ілюструють, як принципи та функції превентивного захисту можуть бути застосовані у практиці для забезпечення безпеки і захисту від кіберзагроз.

Превентивний захист включає в себе широкий спектр технологій і підходів, спрямованих на запобігання і виявлення потенційних загроз безпеці інформації. Ось деякі з найпоширеніших технологій превентивного захисту [11]:

1. Фаєрволи (Firewalls): Фаєрволи - це програми або пристрої, які контролюють мережевий трафік між внутрішньою мережею і зовнішнім середовищем. Вони аналізують мережеві пакети і приймають рішення про допуск або блокування засноване на заданих правилах безпеки.
2. Антивірусні програми: Антивірусні програми виявляють, блокують і видаляють віруси, шпигунське програмне забезпечення, троянські програми та інші шкідливі програми з комп'ютера. Вони перевіряють файли, електронну пошту, веб-сайти та інші джерела на наявність загроз.
3. Антиспам-фільтри: Антиспам-фільтри використовуються для виявлення і блокування небажаних електронних листів (спаму). Вони аналізують вхідну пошту і застосовують різні методи, такі як фільтрація на основі ключових слів, списки блокування і аналіз поведінки, щоб виділити і блокувати спамові повідомлення.
4. Антишпигунське програмне забезпечення: Це програми, які виявляють і блокують шпигунське програмне забезпечення, яке збирає інформацію про користувача без його згоди. Вони перевіряють систему на наявність шпигунського програмного забезпечення і забезпечують його видалення.
5. Оновлення програмного забезпечення: Регулярне оновлення операційних систем, веб-браузерів, антивірусного програмного забезпечення та інших програм дозволяє заповнити вразливості і виправити відомі помилки, що можуть бути використані зловмисниками. Оновлення також включають в себе сигнатури вірусів і нові методи виявлення загроз.
6. Антифішингові заходи: Ці заходи призначені для виявлення і блокування фішингових атак, які спробують отримати конфіденційну інформацію, таку як паролі, кредитні картки тощо. Вони перевіряють веб-сторінки і

електронні повідомлення на ознаки шахрайства і попереджають користувачів про можливі ризики.

Це лише декілька прикладів технологій превентивного захисту, які використовуються для забезпечення безпеки інформації. Комбінування різних технологій та стратегій допомагає зменшити ризики виникнення загроз і зберегти дані в безпечності [2].

Вірусні бази даних є важливою складовою антивірусного програмного забезпечення. Вони містять інформацію про відомі віруси, їх характеристики, сигнатури (узори) і правила для їх виявлення. Вірусні бази даних оновлюються регулярно, щоб враховувати нові загрози, які постійно з'являються.

Вірусні бази даних антивірусного програмного забезпечення зазвичай містять інформацію про різні типи вірусів, такі як файлові віруси, макровіруси, троянські програми, черв'яки тощо. Кожен запис в базі даних містить опис віруса, його сигнатуру (узор), яка є унікальним ідентифікатором для виявлення віруса, та вказівки щодо дій для його нейтралізації або видалення.

Антивірусні програми використовують ці вірусні бази даних для перевірки файлів і системи на наявність вірусів. Під час сканування, антивірусна програма порівнює сигнатури файлів зі записами в базі даних і, якщо знайдено відповідність, виявляє потенційну загрозу. Деякі антивірусні програми також використовують евристичний аналіз, щоб виявляти нові або невідомі віруси, необхідність яких ще не включена до вірусних баз даних [11].

Оновлення вірусних баз даних є критичним аспектом ефективної роботи антивірусного програмного забезпечення. Виробники антивірусних програм надають регулярні оновлення баз даних, які містять нові сигнатури вірусів і інші зміни для забезпечення оптимального рівня захисту. Користувачі повинні регулярно оновлювати свої антивірусні програми, щоб мати доступ до найновіших вірусних баз даних і ефективно захищати свої системи від потенційних загроз.

Аналіз поведінки програм є важливою складовою активного захисту ПК. Він базується на спостереженні та аналізі дій і активності програм з метою виявлення небажаної або шкідливої поведінки, яка може вказувати на наявність загрози безпеці [5].

Основні принципи та функції аналізу поведінки програм включають [3]:

1. Виявлення аномалій: Аналіз поведінки програм дозволяє виявляти аномальну активність, яка відрізняється від типового звичайного поводження програми. Це може включати незвичайні системні виклики, зміни файлів, модифікацію реєстру, з'єднання з підозрілими серверами тощо.
2. Виявлення шкідливого програмного забезпечення: Аналіз поведінки програм допомагає виявляти шкідливе програмне забезпечення, яке може мати відмінну від звичайної поведінку. Він може виявляти спроби створення, копіювання або модифікації файлів системи, нелегітимний доступ до ресурсів, зміни налаштувань системи без дозволу тощо.
3. Виявлення вразливостей: Аналіз поведінки програм може допомагати виявляти вразливості програмного забезпечення шляхом спостереження за неправильною або потенційно небезпечною взаємодією програми з системою. Це допомагає виявляти можливі точки входу для зловмисників або експлойтів.
4. Динамічний аналіз: Аналіз поведінки програм може проводитись у реальному часі під час виконання програми для виявлення шкідливих дій. Він може включати моніторинг системних викликів, мережевої активності, змін файлів, змін реєстру та інших дій програми з метою виявлення потенційних загроз.
5. Створення профілів програм: Аналіз поведінки програм може використовувати створення профілів програм для визначення типової поведінки і стандартних дій програм. При виявленні відхилень від цих

профілів можна вважати, що програма виявляє небажану або шкідливу активність.

Аналіз поведінки програм є ефективним інструментом для встановлення нових і нещодавно виявлених загроз безпеці, так як він не обмежується підписами відомих вірусів чи шкідливого програмного забезпечення. Він допомагає виявляти невідомі загрози та захищати систему від їхньої дії.

Для проведення аналізу поведінки програм потрібно мати конкретний приклад програми або сценарій дії, який можна проаналізувати. Без конкретної програми чи сценарію важко провести аналіз. Однак, я можу навести загальний приклад процесу аналізу поведінки програми.

Припустимо, у нас є програма, яка заявлена як текстовий редактор. Щоб проаналізувати її поведінку, ми можемо виконати наступні кроки [10]:

1. Встановити програму: Запускаємо процес встановлення програми і спостерігаємо, які файли вона копіює на систему, які ключі реєстру вона змінює, які служби чи процеси вона створює.
2. Запустити програму: Після встановлення запускаємо програму і спостерігаємо її активність. Можемо відслідковувати, з якими файлами вона взаємодіє, які мережеві з'єднання вона встановлює, які системні виклики вона робить.
3. Аналізувати системну активність: Спостерігаємо, як програма впливає на систему. Чи збільшується завантаження процесора або використання пам'яті? Чи змінюються системні налаштування? Чи виникають підозрілі процеси або служби?
4. Перевірити мережеву активність: Аналізуємо, з якими серверами або доменами встановлюється з'єднання програми. Чи є підозрілі мережеві активності, які можуть вказувати на небажану комунікацію з зовнішніми джерелами?

5. Перевірити системні зміни: Слідкуємо за змінами, які програма вносить у систему. Чи змінює вона файли або реєстрові ключі? Чи створює нові процеси чи служби? Чи змінює системні налаштування?
6. Визначити відхилення: Порівнюємо спостережені дії програми зі стандартними та очікуваними діями текстового редактора. Якщо виявляються незвичні або підозрілі дії, це може вказувати на потенційну загрозу чи небажану активність.

Це загальний приклад процесу аналізу поведінки програми. Залежно від конкретного випадку можуть використовуватися різні інструменти і методи для більш детального аналізу [6].

Фаєрволи фільтрують мережевий трафік, контролюючи передачу даних між мережею та інтернетом або між різними сегментами мережі. Вони діють на різних рівнях мережевої архітектури, включаючи мережевий рівень (IP-адреса, порти), транспортний рівень (TCP, UDP), а також додаткові рівні, такі як застосунковий рівень (протоколи HTTP, FTP, SMTP і т.д.).

Основна функція фаєрвола полягає в перевірці трафіку на відповідність заданим правилам доступу і блокуванні небажаних підключень або потенційно шкідливих пакетів даних. Вони можуть блокувати спроби вторгнення, DDOS атаки, атаки з використанням вразливостей, а також фільтрувати небажаний або шкідливий контент [5].

Додаткові можливості фаєрволів можуть включати логування подій, моніторинг мережевої активності, розподіл мережевих ресурсів, налаштування віртуальних приватних мереж (VPN) тощо.

Існують різні типи фаєрволів, включаючи мережеві фаєрволи (загальна точка контролю для всієї мережі), периметрові фаєрволи (захист зовнішніх точок доступу до мережі) і хост-фаєрволи (захист окремих комп'ютерів або серверів) [4].

Фаєрволи є важливою складовою системи безпеки для будь-якої комп'ютерної мережі. Вони допомагають запобігати несанкціонованому

доступу, зберігають конфіденційність та цілісність даних, а також забезпечують безпеку мережевої інфраструктури.

Реал-тайм аналіз, або аналіз в реальному часі, є важливою складовою сучасних систем захисту і дозволяє виявляти потенційно небезпечні дії програм під час їх виконання. Цей метод аналізу базується на спостереженні за активністю програми на протязі її роботи, а не на перевірці файлів або виконанні сканування після завершення роботи.

Основним принципом реал-тайм аналізу є спостереження за змінами у поведінці програми під час її виконання. Наприклад, аналізатор може відслідковувати доступ програми до файлової системи, мережевих ресурсів, реєстру, взаємодії з іншими процесами та багато іншого. Якщо програма виявляє підозрілі дії, наприклад, спроби модифікувати системні файли або відправляти дані на незнайомий сервер, аналізатор може спрацювати і прийняти відповідні заходи для блокування або зупинки такої активності.

Однією з переваг реал-тайм аналізу є його здатність виявляти нові атаки та невідомі загрози. Традиційні антивірусні програми, які працюють на основі сигнатур або евристичних методів, можуть бути недостатньо ефективними проти нових варіацій шкідливих програм. Реал-тайм аналіз дозволяє виявити підозрілі дії, навіть якщо загроза раніше не була відома.

Програми, що використовують реал-тайм аналіз, зазвичай мають різноманітні функції, включаючи моніторинг активності, аналіз поведінки, блокування шкідливої активності, оповіщення про потенційні загрози та багато іншого. Ці програми можуть бути встановлені на комп'ютерах, серверах або інших пристроях для забезпечення захисту в реальному часі.

Один з прикладів програми, яка використовує реал-тайм аналіз – Wireshark [11].

Wireshark є відкритим інструментом аналізу мережі, який дозволяє перехоплювати та аналізувати мережевий трафік в реальному часі. Він може

бути використаний для моніторингу та аналізу мережевих пакетів, що проходять через комп'ютерну мережу.

Wireshark дозволяє перехоплювати дані з різних мережевих інтерфейсів, аналізувати заголовки пакетів, переглядати та фільтрувати мережевий трафік за різними параметрами. Він надає можливість докладного розбору мережевих протоколів, виявлення аномалій, перевірки безпеки мережі, аналізу проблем мережевої продуктивності та багато іншого.

Wireshark дозволяє вам побачити, які дані передаються через мережу в реальному часі і дослідити їх детальні характеристики. Це може бути корисним для виявлення вразливостей мережі, атак або ненормальної активності, яка може бути зв'язана зі шкідливими програмами або проблемами мережевої безпеки.

Узагалі, реал-тайм аналіз є важливим компонентом сучасного захисту від кіберзагроз. Він дозволяє виявити і зупинити потенційно небезпечну активність програм у реальному часі, що допомагає запобігти атакам та захистити системи та дані користувачів [14].

Реал-тайм аналіз також забезпечує швидку реакцію на потенційні загрози. За допомогою алгоритмів моніторингу та аналізу, програми можуть виявити аномальні дії та негайно вжити заходів для їх припинення. Це важливо, оскільки деякі кібератаки можуть швидко поширюватися і завдати значних шкоди, якщо не будуть прийняті негайні заходи.

Крім того, реал-тайм аналіз може виявляти інсайдерські загрози, тобто дії внутрішніх користувачів, які намагаються отримати несанкціонований доступ до конфіденційної інформації або зламати безпекові політики компанії. Виявлення таких загроз дозволяє своєчасно реагувати на них і запобігти можливим витокам даних чи фінансовим збиткам.

Ще однією перевагою реал-тайм аналізу є його здатність адаптуватися до нових загроз. Постійне оновлення алгоритмів і баз даних дозволяє програмам розпізнавати нові типи шкідливих програм і атак, які можуть з'явитися. Це

дозволяє забезпечити більш ефективний рівень захисту, навіть у змінних умовах кібербезпеки [15].

Загалом, реал-тайм аналіз є важливим компонентом сучасних систем захисту, що дозволяє виявляти, аналізувати та припиняти потенційно небезпечну активність програм у реальному часі. Це допомагає забезпечити надійний рівень кібербезпеки та захистити системи, дані та конфіденційну інформацію від різноманітних загроз.

Виявлення та блокування загроз є важливими аспектами систем активного захисту, які допомагають запобігати інфікуванню систем шкідливими програмами та кібератакам. Для досягнення цього мети використовуються різні технології та методи, що забезпечують ефективний аналіз та блокування загроз.

Одним з ключових методів виявлення загроз є використання сигнатурних аналізаторів. Ці аналізатори перевіряють програми та файли на наявність спеціальних підписів або сигнатур, які є характерними для відомих шкідливих програм або вразливостей. Якщо сигнатура виявляється, система реагує, блокуючи або ізолюючи підозрілий об'єкт.

Крім сигнатурного аналізу, використовуються також евристичні аналізатори, які базуються на аналізі поведінки програм. Ці аналізатори виявляють незвичайні дії, зміни в системних налаштуваннях чи інші ознаки, що можуть свідчити про потенційну загрозу. Наприклад, якщо програма починає змінювати системні файли або спробує встановити додаткові компоненти без дозволу користувача, система може реагувати, блокуючи або сповіщаючи про цю дію [11].

Також для виявлення загроз використовуються системи виявлення вторгнень (IDS) і системи запобігання вторгнень (IPS). Ці системи моніторять мережевий трафік та системну активність з метою виявлення аномальних або підозрілих дій. Якщо система виявляє вторгнення або шкідливу активність, вона може прийняти заходи для блокування атаки або відхилення підозрілих пакетів.

З метою ефективного блокування загроз, системи активного захисту також використовують оновлення баз даних, що містять інформацію про нові види шкідливих програм, вразливості та методи атак. Регулярні оновлення дозволяють системам бути в курсі останніх загроз та вживати заходів для їх блокування.

Загалом, виявлення та блокування загроз є критично важливими елементами активного захисту. Комплексне використання сигнатурного та евристичного аналізу, систем IDS/IPS та оновлення баз даних дозволяє системам швидко реагувати на потенційні загрози, блокувати їх та забезпечувати високий рівень безпеки для систем і даних користувачів.

Для кращого розуміння виявлення та блокування загроз, розглянемо кілька прикладів технологій і методів, що застосовуються в системах активного захисту [6]:

1. Сигнатурний аналіз: Одним з найпоширеніших методів виявлення загроз є використання бази даних з сигнатурами відомих шкідливих програм. Наприклад, антивірусна програма виявляє загрозу, порівнюючи хеш-суму або підпис файлу зі списком відомих шкідливих програм. Якщо збіг знайдений, програма реагує, блокуючи або переміщуючи файл у карантин.
2. Евристичний аналіз: Евристичні аналізатори базуються на виявленні незвичайних або підозрілих дій програм. Наприклад, якщо програма спробує змінити системні файли або встановити додаткові компоненти без дозволу користувача, система може вважати це підозрілим і реагувати шляхом блокування або сповіщення користувача.
3. Системи виявлення вторгнень (IDS): Системи IDS виявляють аномалії та незвичайну активність в мережі. Наприклад, якщо система виявляє підозрілу мережеву активність, яка вказує на можливу кібератаку, вона може прийняти заходи для блокування цих пакетів або відхилення атаки.
4. Системи запобігання вторгнень (IPS): Системи IPS працюють подібно до систем IDS, але вони можуть надавати активну захист, наприклад, шляхом

блокування атакуючих IP-адрес або перехоплення пакетів, що містять зловмисні коди.

5. Оновлення баз даних: Оновлення баз даних є критичними для підтримки актуальності системи виявлення загроз. Регулярні оновлення забезпечують отримання нових сигнатур шкідливих програм, вразливостей та інших видів загроз, що допомагають системі виявляти та блокувати їх.

Ці приклади демонструють, що виявлення та блокування загроз - це складний процес, що вимагає поєднання різних методів та технологій. Використання комплексного підходу дозволяє забезпечити ефективний реал-тайм аналіз і запобігти шкоді, яку можуть завдати шкідливі програми та інші загрози.

Інтелектуальні системи виявлення загроз (ІСВЗ) - це комплексні програмні рішення, що використовують штучний інтелект (наприклад, машинне навчання, глибоке навчання, аналітику даних тощо) для виявлення, аналізу та реагування на потенційні загрози безпеці інформаційних систем.

ІСВЗ використовуються для пошуку аномалій, несправедливих поведінкових зразків та вразливостей в комп'ютерних мережах, системах або додатках. Вони можуть виявляти шкідливі програми, вторгнення, вразливості, атаки з використанням відомих і невідомих методів, а також інші загрози безпеці.

Основні принципи роботи ІСВЗ включають наступні етапи [15] :

1. Збір даних: система збирає дані про мережеву активність, системні журнали, аудит-логи, потоки даних тощо.
2. Аналіз даних: застосовуються алгоритми машинного навчання та аналітики даних для виявлення аномалій, відхилень від нормальної поведінки та потенційних загроз.
3. Виявлення загроз: система порівнює аналізовані дані з відомими шаблонами атак, сигнатурами вірусів, зловмисними зразками та іншими моделями для виявлення потенційних загроз.

4. Реагування: після виявлення загрози система може автоматично вживати заходів для запобігання атаки або сповіщати адміністратора про виявлену загрозу.
5. Навчання та адаптація: ІСВЗ можуть навчатися на основі нових даних та оновлювати свої моделі для вдосконалення виявлення загроз та адаптації до нових видів атак.

ІСВЗ використовуються в різних сферах, включаючи комп'ютерну безпеку, мережеву безпеку, фінансові установи, телекомунікаційні компанії, організації електронної комерції та інші, де висока надійність та безпека є критичними факторами [4].

Ось декілька прикладів інтелектуальних систем виявлення загроз [17] :

1. Системи виявлення вторгнень (Intrusion Detection Systems, IDS): Наприклад, Snort та Suricata є популярними відкритими системами виявлення вторгнень, які використовують правила, сигнатури та аналітику даних для виявлення вторгнень у комп'ютерні мережі.
2. Антивірусні програми: Сучасні антивірусні програми, такі як Kaspersky, McAfee, Symantec, використовують інтелектуальні техніки для виявлення та блокування шкідливих програм, включаючи машинне навчання для виявлення нових вірусів та аналізу поведінки програм.
3. Системи виявлення аномалій: Модерні системи виявлення аномалій, наприклад, Splunk, LogRhythm, використовують аналітику даних та машинне навчання для виявлення несправедливих зразків поведінки у великих обсягах лог-даних, що може свідчити про атаку або порушення безпеки.
4. Системи виявлення фішингу: Деякі компанії, наприклад, Cofense та Proofpoint, розробляють інтелектуальні системи виявлення фішингу, які використовують аналіз поведінки, імітацію користувача та інші техніки для виявлення та блокування шахрайських електронних листів та веб-сайтів.

5. Системи виявлення атак на мережевий рівень: Bro/Zeek є однією з популярних систем виявлення атак на мережевому рівні, яка здатна аналізувати мережевий трафік і виявляти аномальну або шкідливу активність.

Це лише кілька прикладів інтелектуальних систем виявлення загроз, існує багато інших рішень, які використовують інтелектуальні методи для забезпечення безпеки і виявлення загроз у різних областях [3].

## 2.3.Ефективність превентивного та активного захисту ПК

1. Превентивний захист ПК включає заходи, спрямовані на запобігання вразливостям і атакам до того, як вони відбудуться. Це включає встановлення і оновлення антивірусного програмного забезпечення, використання фаєрволів, налаштування безпеки мережі, резервне копіювання даних та інші заходи. Превентивний захист дозволяє попередити багато загроз і запобігти їхньому потенційному впливу на ПК. Наприклад, антивірусне програмне забезпечення може виявити і блокувати віруси та шкідливі програми до їхнього запуску на ПК. Фаєрволи можуть перешкоджати несанкціонованому доступу до ПК та контролювати комунікацію з мережею.

2. Активний захист ПК

Активний захист ПК передбачає реагування на актуальні загрози і виявлення шкідливих програм у реальному часі. Це включає використання антивірусного програмного забезпечення з можливістю виявлення нових вірусів та інших шкідливих програм, систем виявлення вторгнень (IDS) і систем управління вторгненнями (IPS), а також використання інтелектуальних систем виявлення загроз (IDS). Активний захист дозволяє реагувати на нові та невідомі загрози, що не були враховані превентивним захистом. Наприклад, система виявлення вторгнень може аналізувати мережевий трафік і виявляти підозрілу активність, таку як спроби несанкціонованого доступу або атаки.

3. Переваги та обмеження превентивного та активного захисту

Превентивний захист має декілька переваг. Він дозволяє запобігати багатьом загрозам, забезпечує безпеку на рівні системи та допомагає попередити потенційні проблеми. Однак, превентивний захист може мати обмеження в ефективності при виявленні нових та невідомих загроз, які не враховані в антивірусних базах даних або інших засобах захисту. Також, він може вимагати значних ресурсів для оновлення програмного забезпечення та налаштування системи [18].

Активний захист, з іншого боку, може реагувати на нові та невідомі загрози, що забезпечує більш високий рівень захисту. Використання інтелектуальних систем виявлення загроз може поліпшити ефективність активного захисту шляхом аналізу поведінки, виявлення аномальної активності та шаблонів загроз. Однак, активний захист також може мати обмеження, такі як можливість спричинити помилкові спрацювання або збільшення навантаження на систему.

В контексті забезпечення безпеки ПК, ефективність превентивного та активного захисту залежить від поєднання обох підходів. Превентивний захист допомагає запобігти багатьом загрозам і забезпечує основний рівень безпеки. Активний захист дозволяє реагувати на нові та невідомі загрози, що забезпечує додатковий рівень захисту. Використання інтелектуальних систем виявлення загроз покращує ефективність активного захисту шляхом аналізу поведінки та виявлення аномалій [10].

Ураховуючи конкретні потреби та обмеження користувача, рекомендується поєднання превентивних та активних заходів забезпечення безпеки ПК. Це може включати використання актуального антивірусного програмного забезпечення, фаєрволів, систем виявлення вторгнень, а також інтелектуальних систем виявлення загроз. Додатково, важливо підтримувати регулярні оновлення програмного забезпечення і здійснювати навчання користувачів щодо безпечного використання ПК та мережі.

# 3 ПОРІВНЯННЯ АНТИВІРУСНИХ ПРОГРАМ АКТИВНОГО ТА ПРЕВЕНТИВНОГО ЗАХИСТУ

## 3.1. Порівняння антивірусних програм превентивного захисту

Наведу приклади фаєрволів, а саме вбудований фаєрвол Windows а також відомий як брандмауер:

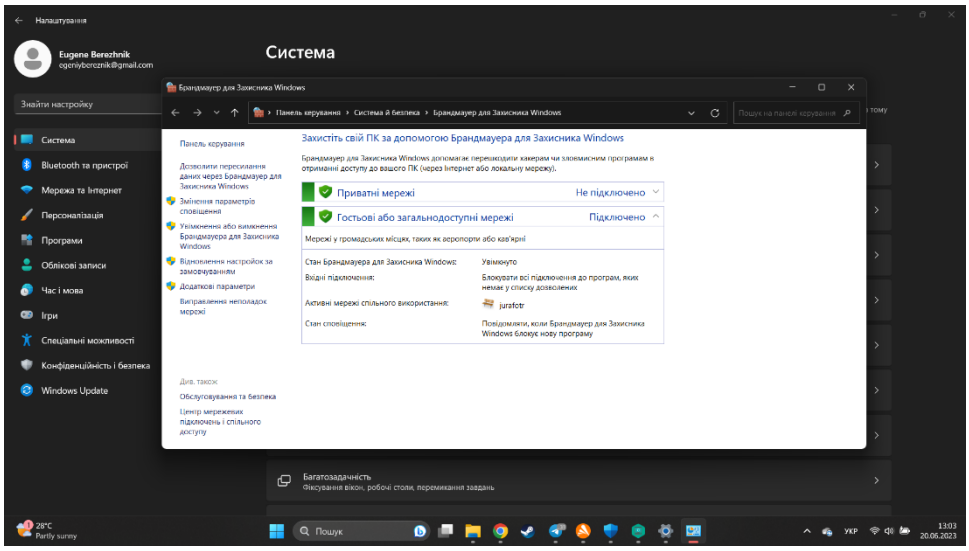



Рисунок 3.1.1. - Початковий інтерфейс Windows Firewall

При відкритті його інтерфейсу зразу показує статус вашого комп’ютера, чи захищений він, чи можливо є якісь проблеми. На даному скриншоті показано, що захист на комп’ютері активний. Також в нього є панель керування через яку ми можемо ним керувати а саме:

1. “Змінення параметрів сповіщення” та ”Увімкнення або вимкнення Брандмауера для захисника Windows”. Мають спільну сторінку на якій можна, як і вмикати й вимикати роботу фаєрвола, так і вмикати й вимикати сповіщення які будуть приходити під час роботи, які будуть сповіщати про виявлені та знешкоджені загрози.

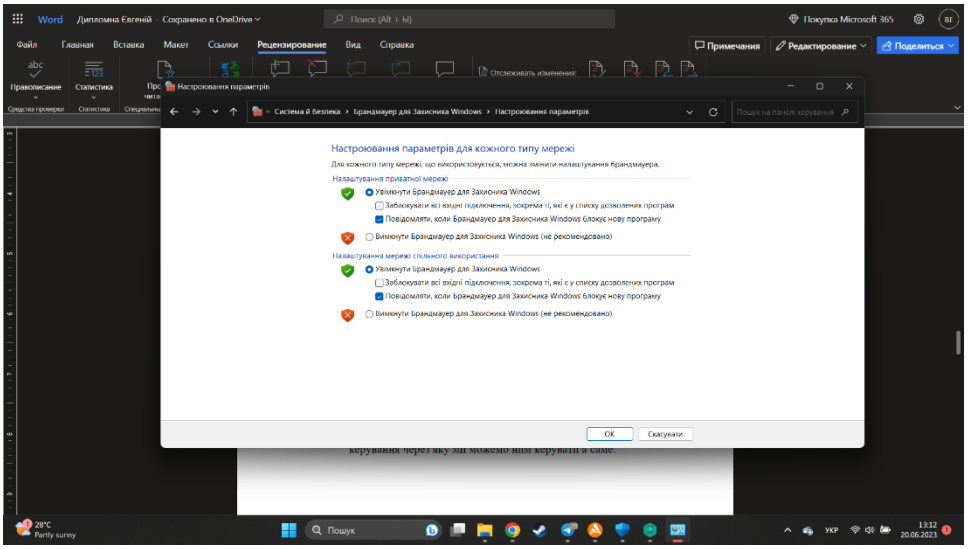



Рисунок 3.1.2. - Налаштування параметрів

2. Відновлювання за замовчуванням. При переході в даний розділ нам пропонують можливість очистити всі налаштування на за замовчуванням.
3. Додаткові параметри. В даному пункті показується всі процеси запущені фаєрволом, перевірки та результати перевірок.

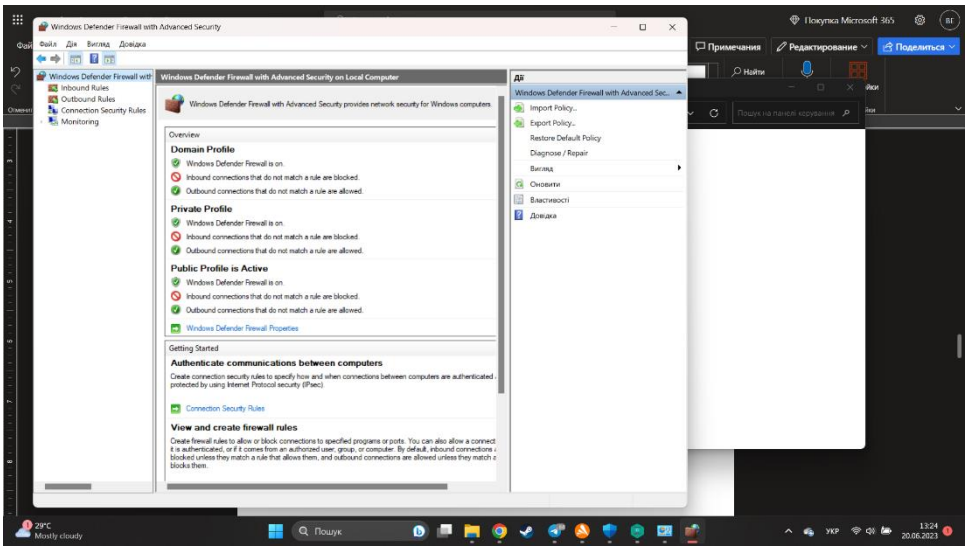



Рисунок 3.1.3. - Додаткові параметри

Другим прикладом є фаєрвол Comodo

Comodo - програмний комплекс, що складається з антивірусу та персонального фаєрволу, а також пісочниці, системи запобігання вторгненням HIPS та віртуального середовища «Virtual Kiosk»

Початковий інтерфейс Comodo

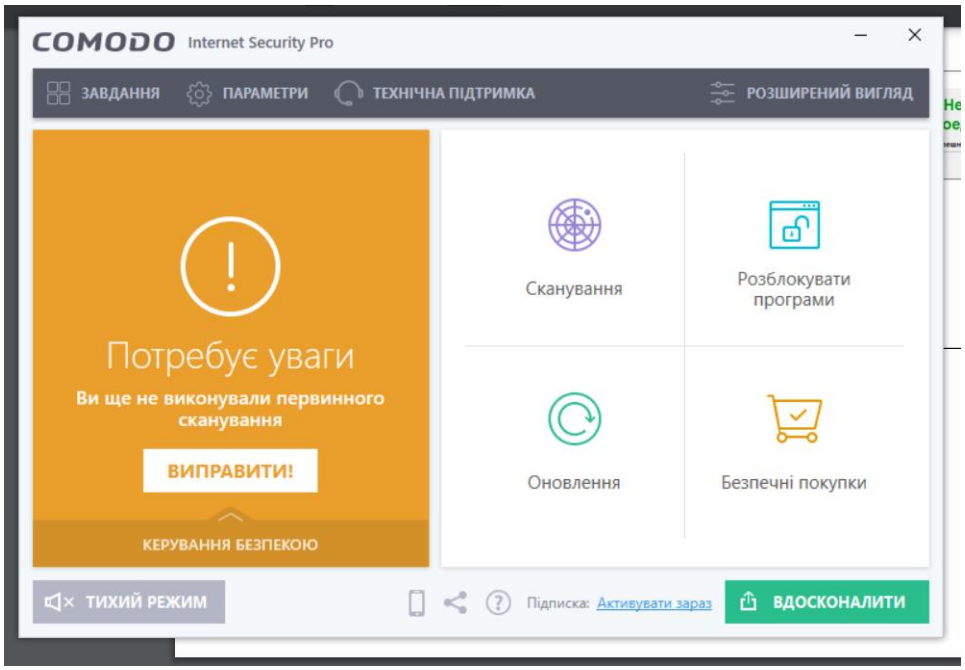



Рисунок 3.1.4. - Початковий інтерфейс Comodo

В налаштуваннях даного антивірусу можна налаштувати брандмауер

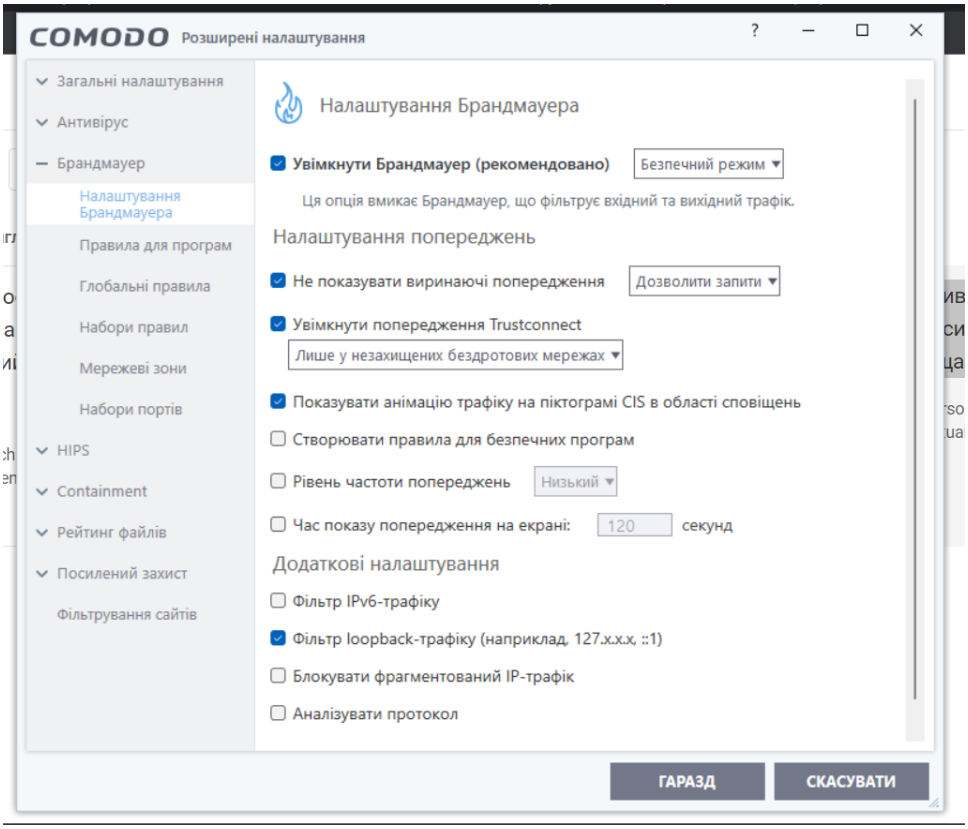



Рисунок 3.1.5. - Розширені налаштування

Можна вибрати чотири режима роботи брандмауера:

1. Блокувати все
2. Власні правила (тобто свої налаштування)
3. Безпечний режим
4. Режим навчання

Переходячи з головного меню в меню “Завдання” можна побачити додаткові функції брандмауера

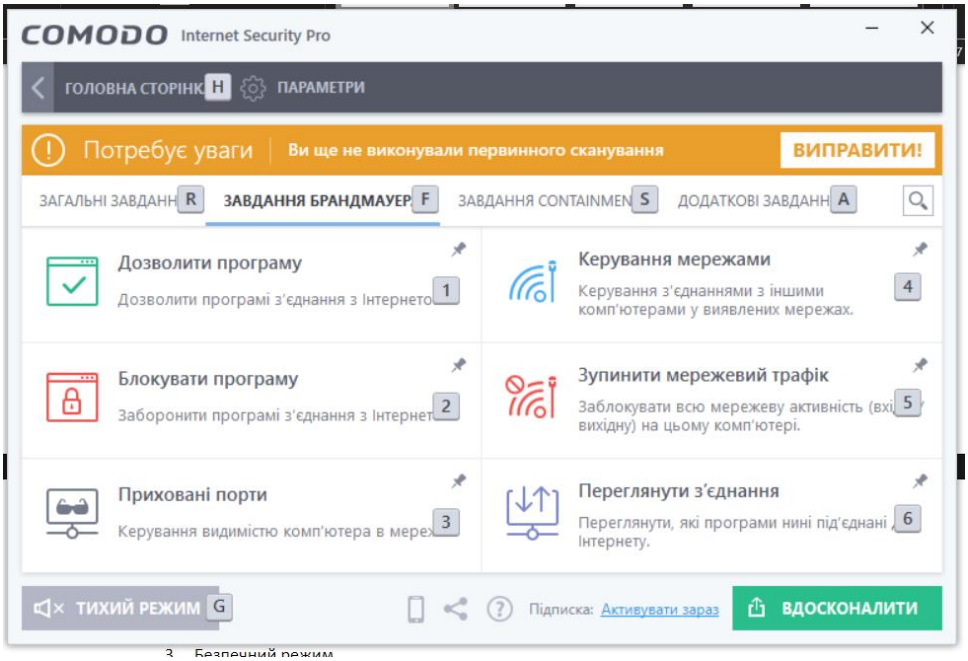



Рисунок 3.1.6. - Брандмауер Comodo

Також можна керувати підключеннями, дозволяти та забороняти програми і тд.

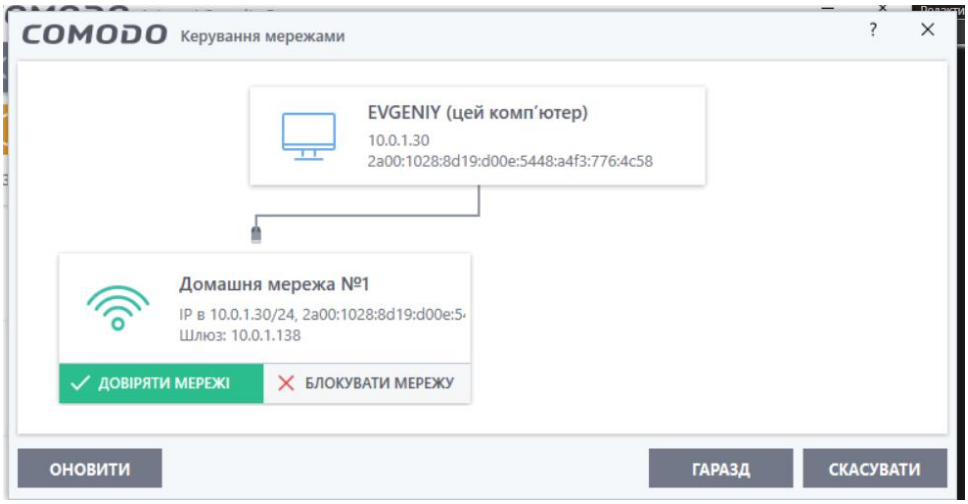



Рисунок 3.1.7. - Керування мережами

TinyWall - це персональний фаєрвол, який знаходиться в безкоштовному доступі та має покликання зробити більш безпечною операційну систему та зміцнити її захист.

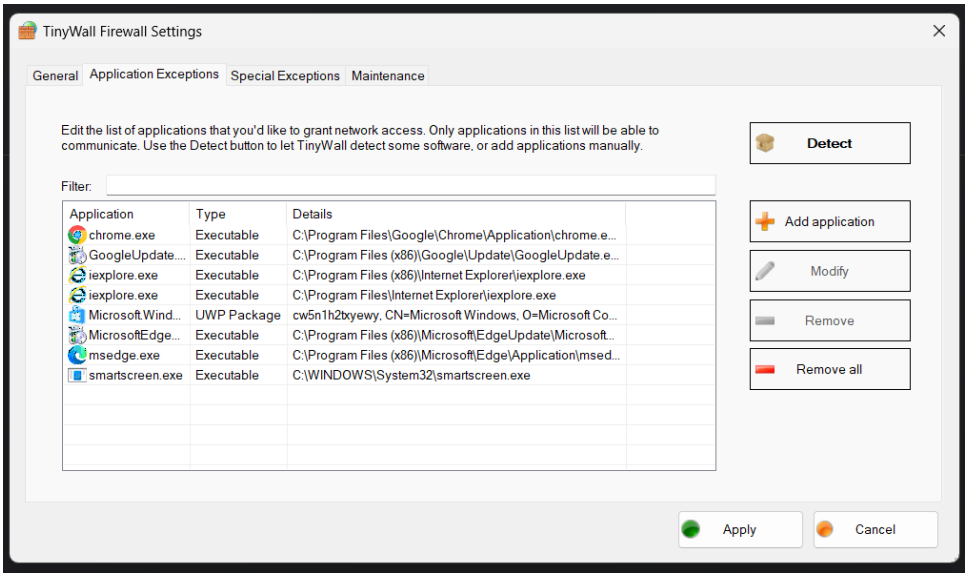



Рисунок 3.1.8. - Початковий інтерфейс TinyWall Firewall

Керувати нею можна через випадаюче вікно яке відкривається внизу комп’ютера

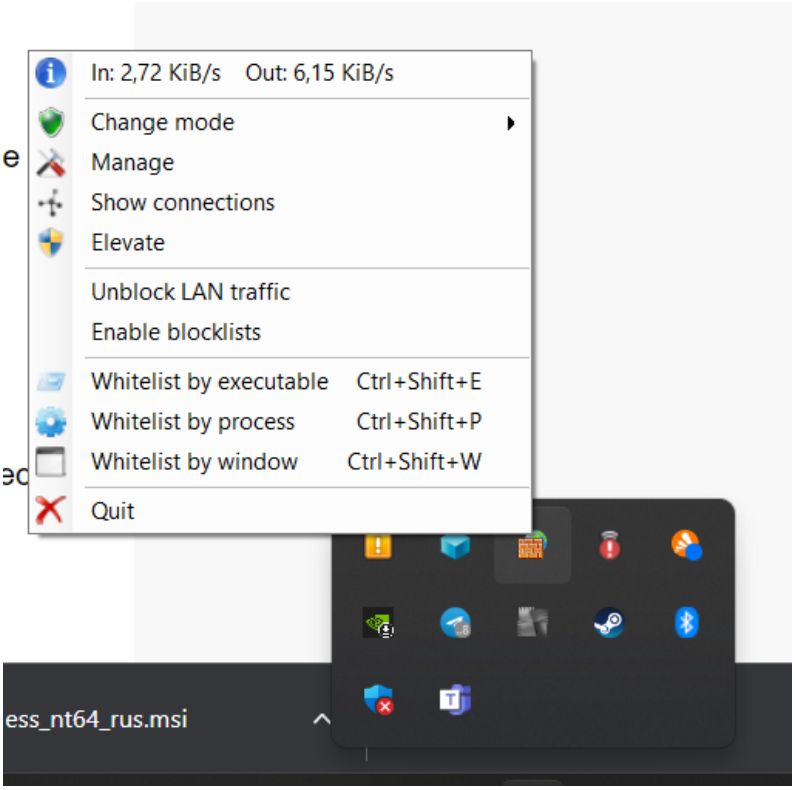



Рисунок 3.1.9. - Керування TinyWall

PeerBlock - це безкоштовний персональний брандмауер з відкритим вихідним кодом, який блокує пакети, що виходять або направляються з списку хостів, що підтримуються, внесених до чорного списку. PeerBlock є наступником програмного забезпечення PeerGuardian для Windows.

Інтерфейс PeerBlock

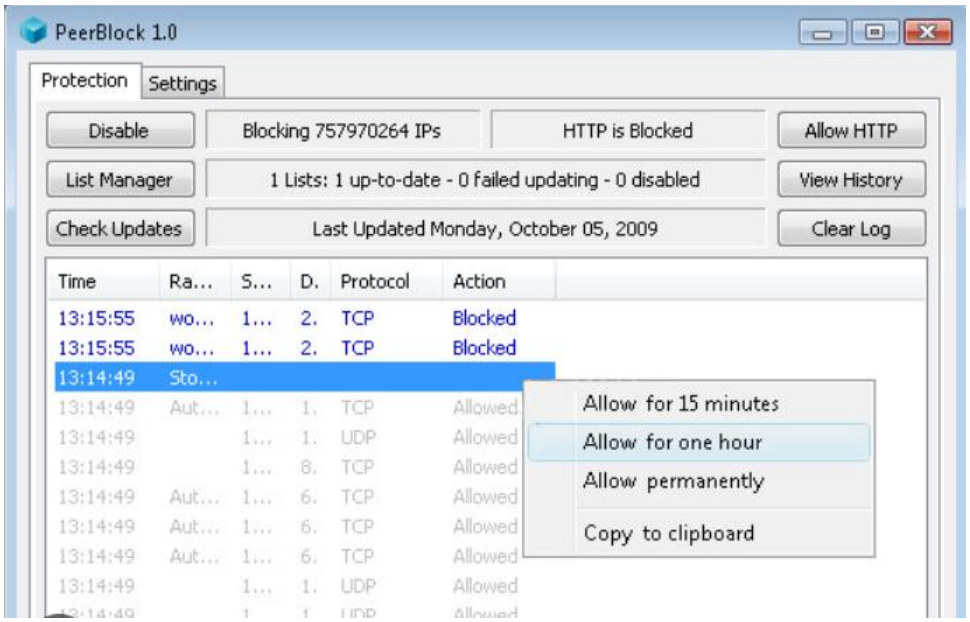



Рисунок 3.1.10. - Початковий інтерфейс PeerBlock

Всі наведені фаєрволи різні, кожен має свої особливі функції (хоча багато однотипних). У таблиці 3.1, показані основні характеристики брандмауерів.

Таблиця 3.1. Характеристики програмних брандмауерів

| Назва | Ключові функції |
|---|---|
| Windows firewall | • Допомагає знизити ризик загроз мережевої безпеки.<br>• Може зменшувати область атаки пристрою, додаючи нові моделі глибинного захисту.<br>• Зменшування поверхні атаки пристрою.<br>• Захищає інтелектуальну власність та дані. Завдяки інтеграції з IPsec<br>• Так як він вшитий в систему Windows то додаткове програмне забезпечення не потрібне.<br>• За допомогою програмних інтерфейсів (API), може доповнювати рішення для безпеки мережі |

| | |
|---|---|
| Comodo | • Stealth Mode це режим, який робить повністю прихованим комп'ютер для сканування портів;<br>• Перевіряє цілісність кожної програми, після чого вже дозволяє її завантаження в пам'ять комп'ютера;<br>• Блокує віруси, програми-шпигуни та трояни;<br>• Запобігає несанкціонованій зміні важливих системних файлів Windows;<br>• Функцію автоматичної пісочниці, вона повністю ізолює ненадійні файли;<br>• Захист від руткітів, впровадження у процеси;<br>• Створення власних правил. |
| TinyWall | • Блокує сотні троянів (і робить це активно), вірусів та інтернет хробаків;<br>• Не вимагає технічних знань про порти, протоколи та різні деталі;<br>•Він використовує мережеві зони, які дозволяють налаштовувати поведінку фаєрволу під власні потреби.<br>• Не дозволяє зловмисному забезпеченню змінити параметри брандмауера |
| PeerBlock | • Запобігає надання доступу до комп'ютера незахищеним пристроям (веб-сервера, інші ПК), які розміщені в інтернеті;<br>• Можливість створювати списки користувачів або імпортувати їх<br>• Можливість надання дозволу комп'ютеру підключатися через порт 80 і 443.<br>• Перегляд журналу з'єднань або очистка лог-файлу. |

Після аналізу превентивного захисту, можна зазначити, що кращим фаєрволом на мою думку є Comodo, до основних переваг якого можна віднести: захист від руткітів, блокує програми шпигуни, запобігає несанкціонованій зміні важливих системних файлів Windows.

## 3.2. Порівняння антивірусних програм активного захисту

Розлянемо інтерфейс та налаштування антивірусних програм:

1. Norton AntiVirus: Norton AntiVirus від компанії Symantec вважається одним з найбільш популярних антивірусних програмних продуктів на ринку. Він має широкий спектр функцій, включаючи захист в реальному часі, виявлення шкідливих програм, фаєрвол, захист від фішингу та інших загроз. Norton AntiVirus працює на різних платформах і має

користувальницький інтерфейс, який легкий у використанні. Але в нього немає безплатної або пробної версії, тільки платні.

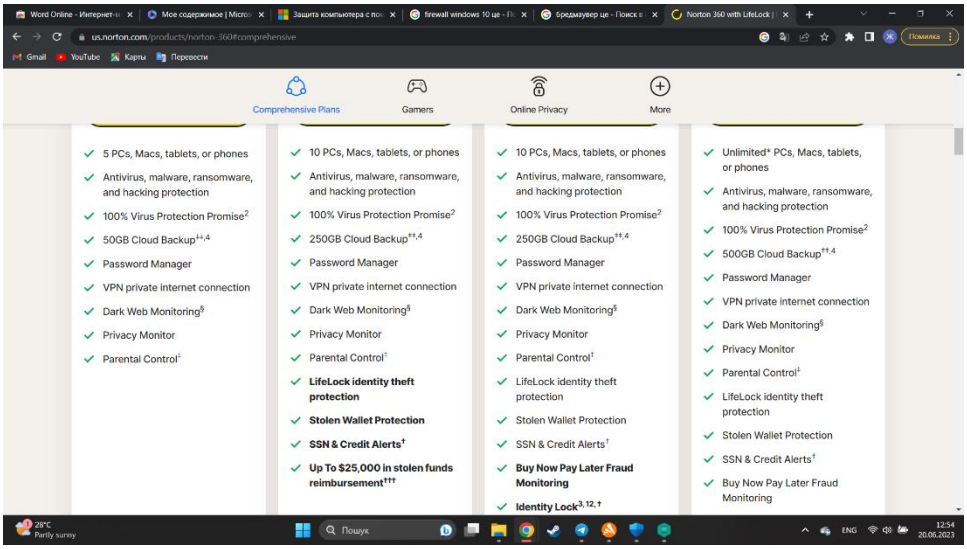



Рисунок 3.2.1 - Веб сторінка Norton 360

2. AVG Free AntiVirus забезпечує базовий рівень захисту комп'ютера. Однак, вона може не мати деяких додаткових функцій, таких як антиспам, брандмауер та захист грошових операцій. Технічна підтримка також може бути обмеженою або відсутньою у безкоштовній версії. Тому, якщо користувачам потрібні ці додаткові функції або підтримка, вони можуть бути зацікавлені придбанні платної версії продукту.

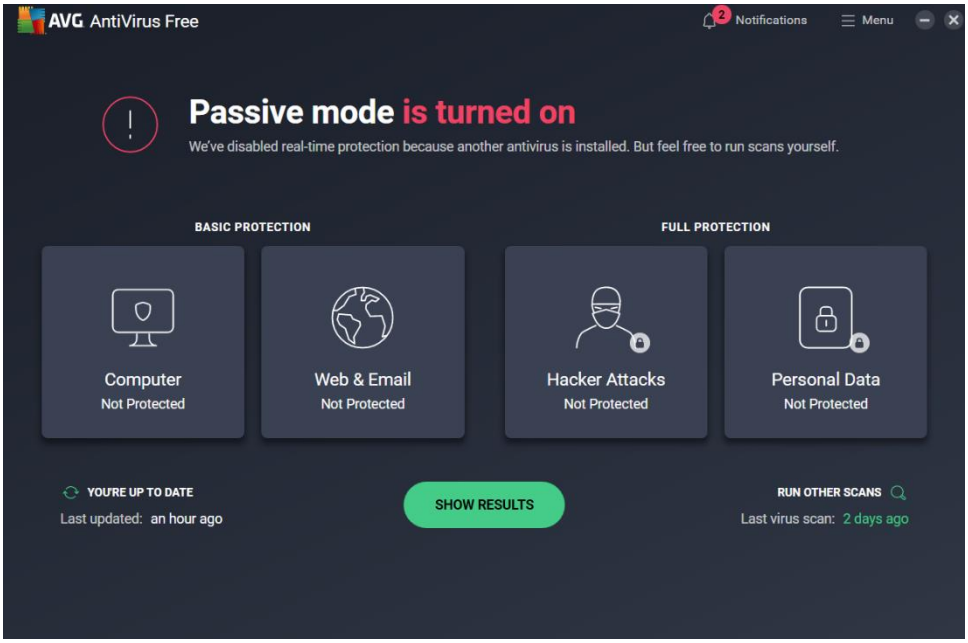



Рисунок 3.2.2 - Початковий інтерфейс AvgAntivirus

Так виглядають розділи налаштування антивірусу

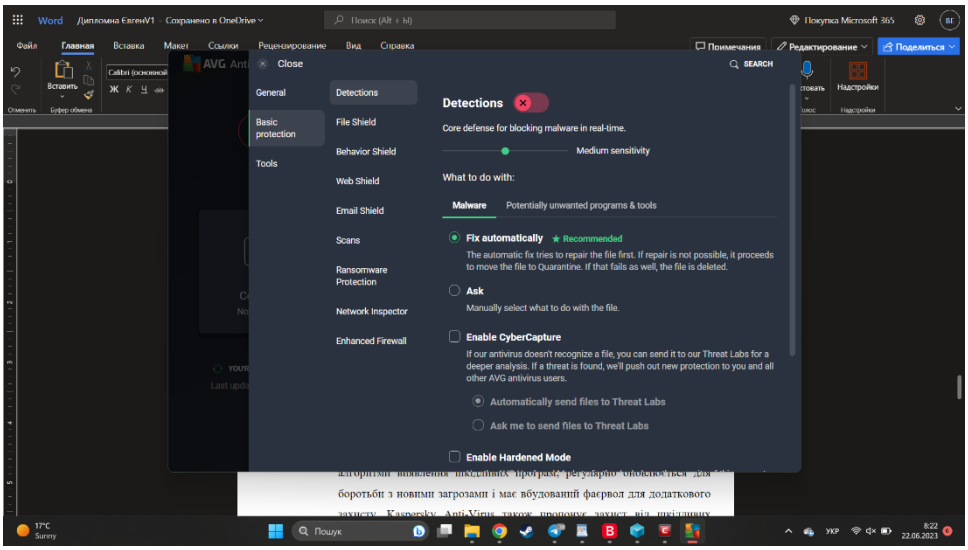



Рисунок 3.2.3. - Налаштування Avg Antivirus

Основні відмінності у функціональності між AVG Antivirus та AVG Antivirus Free Edition:

AVG Antivirus:

- Антивірус, антишпигун, антируткіт функції.

- Захист ідентичності AVG (проактивний захист конфіденційної інформації).
- Захист в соціальних мережах AVG (захист під час роботи в соціальних мережах).
- AVG LinkScanner (перевірка посилань та веб-сторінок).
- AVG Online Shield (перевірка мережевого трафіку та систем миттєвих повідомлень);
- Пріоритетні оновлення.
- Технічна підтримка виробника.

AVG Antivirus Free Edition:

- Антивірус, антишпигун, антируткіт функції.

Основні переваги AVG Antivirus по відношенню до AVG Antivirus Free Edition включають:

- Перевірка файлів перед завантаженням (компонент Online Shield), що підвищує рівень безпеки, блокуючи шкідливі програми до потрапляння на комп'ютер користувача.
- Перевірка безпеки посилань, що передаються у повідомленнях (компонент Online Shield).
- Пріоритетні оновлення (ці оновлення включають, крім антивірусних баз, оновлення модулів антивірусу).
- Доступ до технічних експертів для отримання підтримки та допомоги.

3. Kaspersky Anti-Virus: від компанії володіє визнаним статусом одного з найкращих антивірусних програмних продуктів у світі. Він має потужні алгоритми виявлення шкідливих програм, регулярно оновлюється для боротьби з новими загрозами і має вбудований фаєрвол для додаткового захисту. Kaspersky Anti-Virus також пропонує захист від шкідливих посилань, фішингу і спаму.

На даному скриншоті показаний початковий інтерфейс програми, який є при відкритті програми.

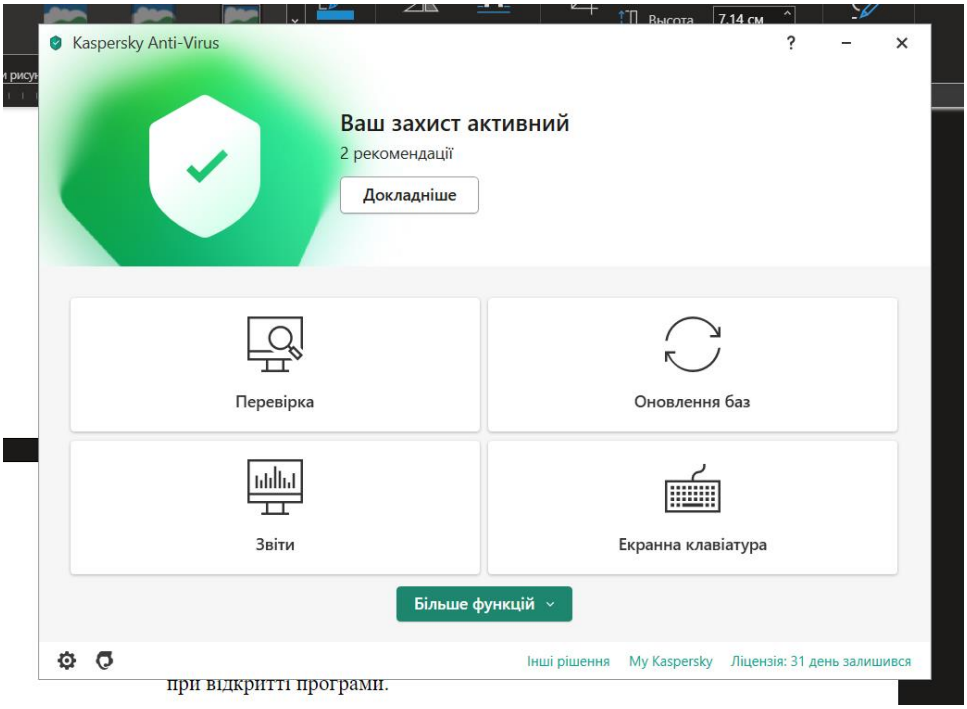



Рисунок 3.2.4. - Початковий інтерфейс

В нижньому просторі інтерфейсі знаходиться кнопка “Більше функцій” при натисканні показує всі додаткові функції антивірусу

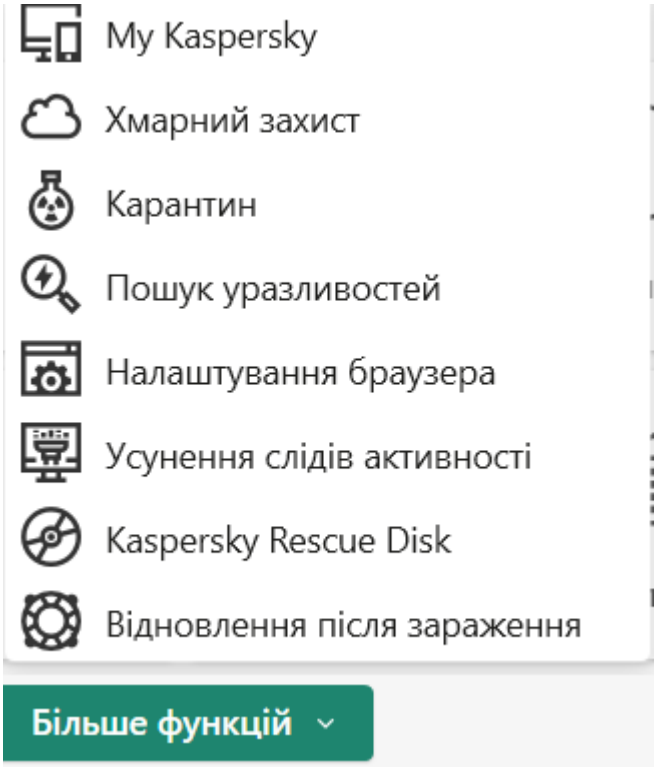



Рисунок 3.2.5. - Функції

Є два елементи інтерфейсу налаштування. Перший знаходиться з права та показує стан захисту комп’ютера, а другий це - панель керування

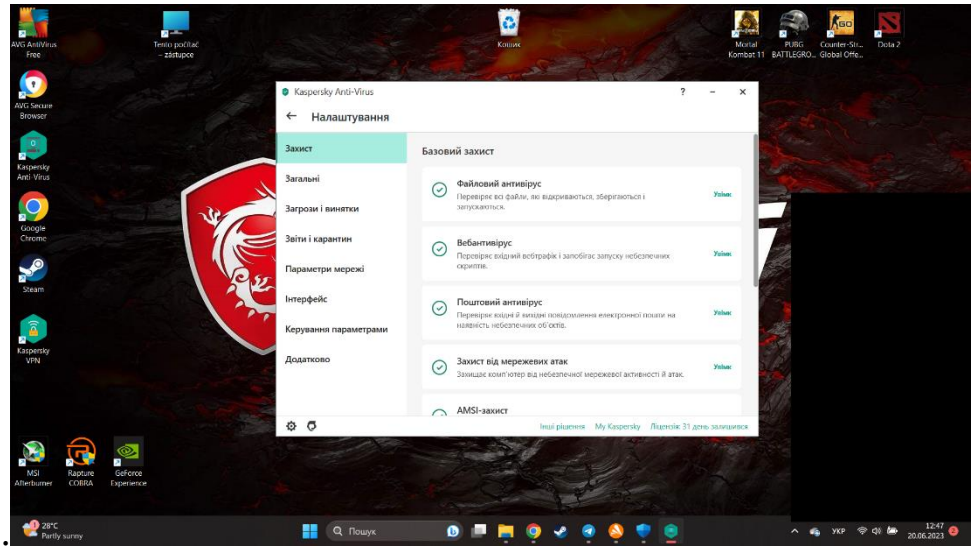



Рисунок 3.2.6. - Налаштування

Панель керування виглядає так:

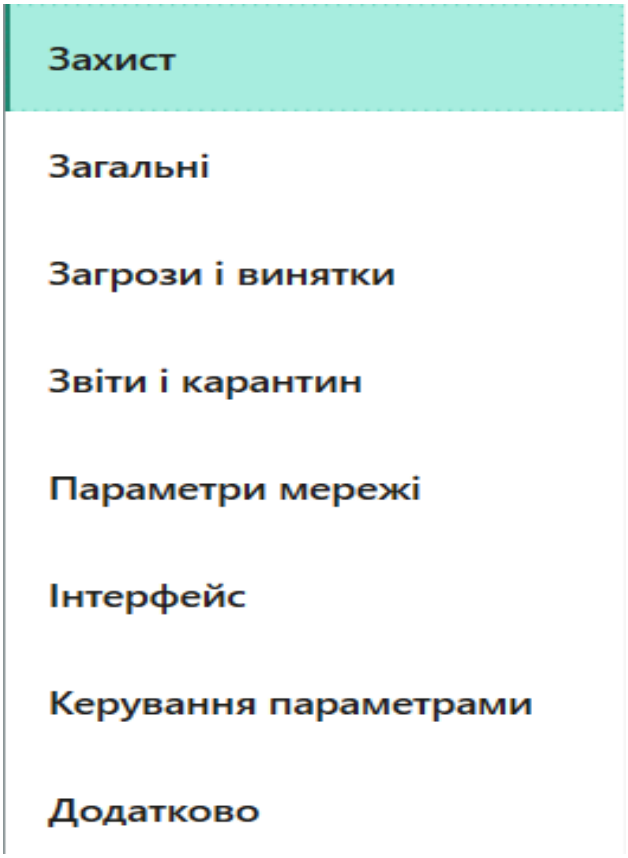



Рисунок 3.2.7 - Панель керування

Панель керування  поділяється на такі відділи:

1. “Загальні”. Відділ в якому можна налштувати режим роботи антивіруса. Та змога використовувати функції які дозволяють зменшувати роботу антивіруса для підвищення продуктивності комп’ютера. Наприклад під час гри, тоді вимикається перевірка та оновлення, також не показуються сповіщення, можна й відкладати виконання завдань на центральний процесор у разі високого навантаження.

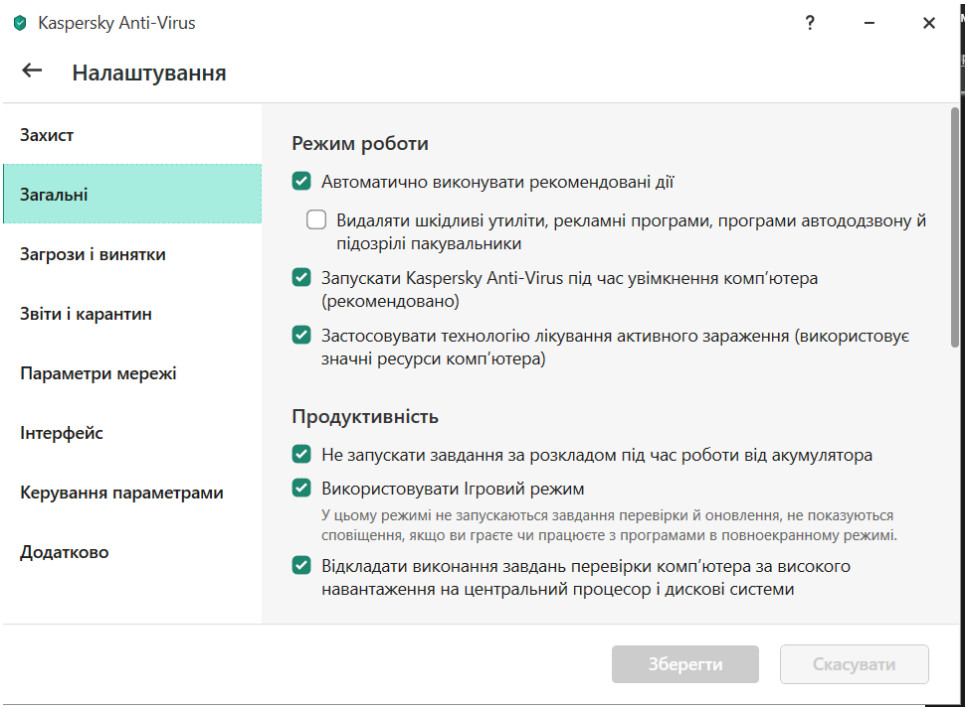



Рисунок 3.2.8. - Загальні налаштування

Існує й функція самозахисту. Дання функція допомагає знешкоджувати спроби вірусів, які здатні проникати в саму програму, й за допомогою її імені змінювати важливі процеси або здійснювати шкідливі дії.

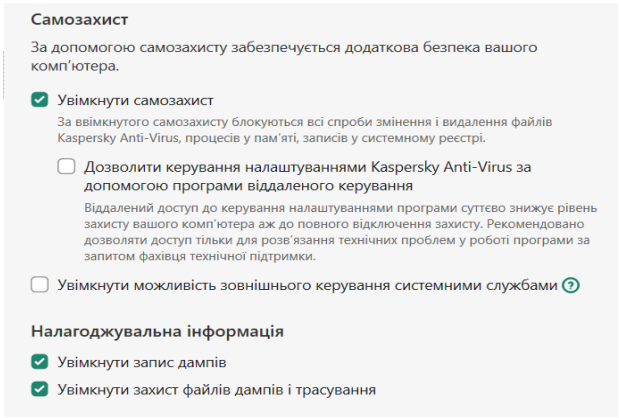



Рисунок 3.2.9. - Функція самозахисту

2. Загрози та винятки. В даному розділі показують, що саме може виявляти даний антивірус. Може виявляти віруси та черв'яки,

троянські програми, шкідливі утиліти, рекламні програми, програми автодозволу.

3. Звіти і карантин. Даний відділ дозволяє налаштовувати параметри карантину, а саме дні проведені в карантині, та розміри файлів-звітів які можуть там перебувати.

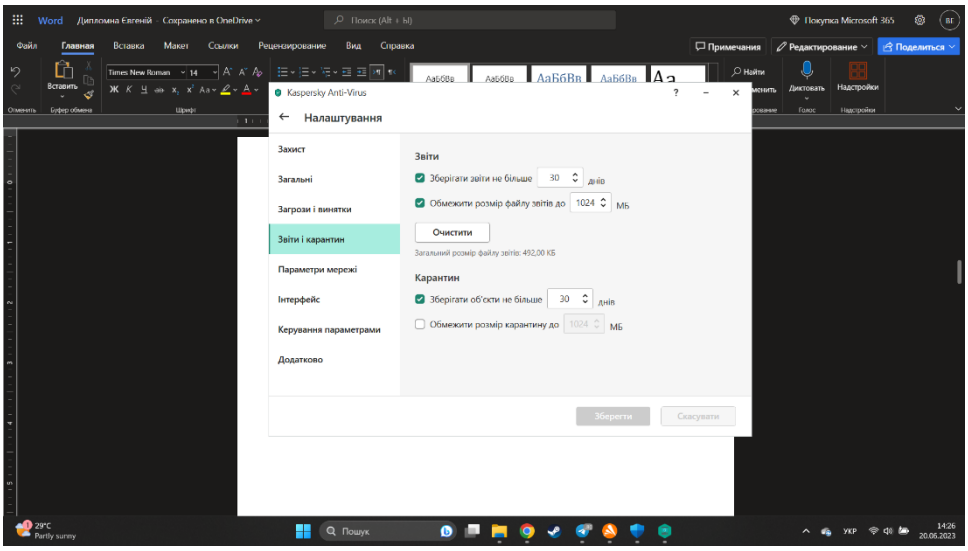
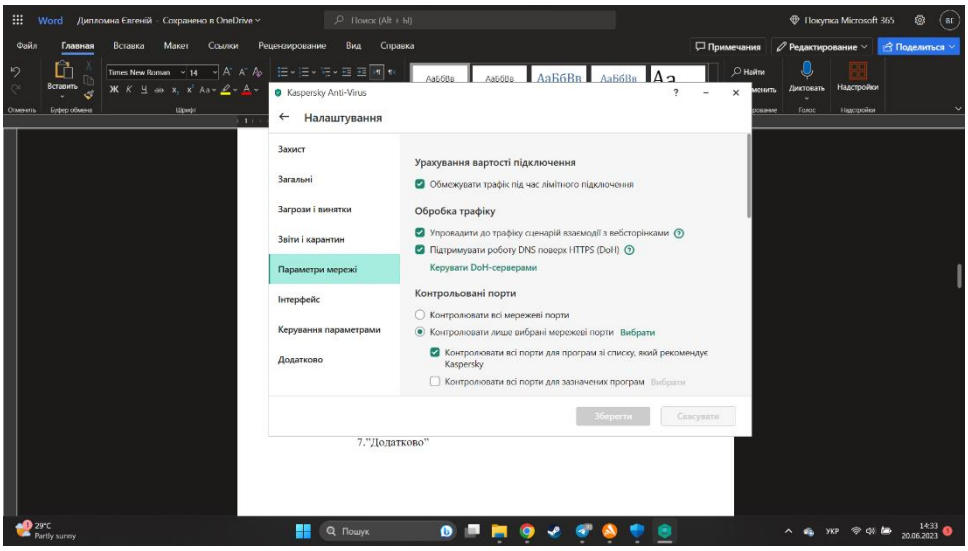



Рисунок 3.2.10. - Налаштування карантину

4. Параметри мережі. Доступні функції контролю портів, заощадження трафіку, якщо ваша мережа має лімітний трафік, обробка трафіку




7."Додатково"

5. Інтерфейс. Тут звичайні налаштування інтерфейсу, його мови, налаштування сповіщень.
6. Керування параметрами. Тут можна зберігати налаштування антивіруса в файлі
7. Додатково. Тут можна додати захист за допомогою адаптивної віртуалізації.

4. Bitdefender Antivirus Plus: Bitdefender Antivirus Plus є ще одним потужним антивірусним рішенням, яке забезпечує високий рівень захисту від шкідливих програм. Він включає в себе функції, такі як антивірусний захист в реальному часі, контроль веб-камери, фаєрвол і захист від фішингу. Bitdefender Antivirus Plus також має мінімальний вплив на продуктивність системи і простий інтерфейс.

Початковий інтерфейс виглядає так:

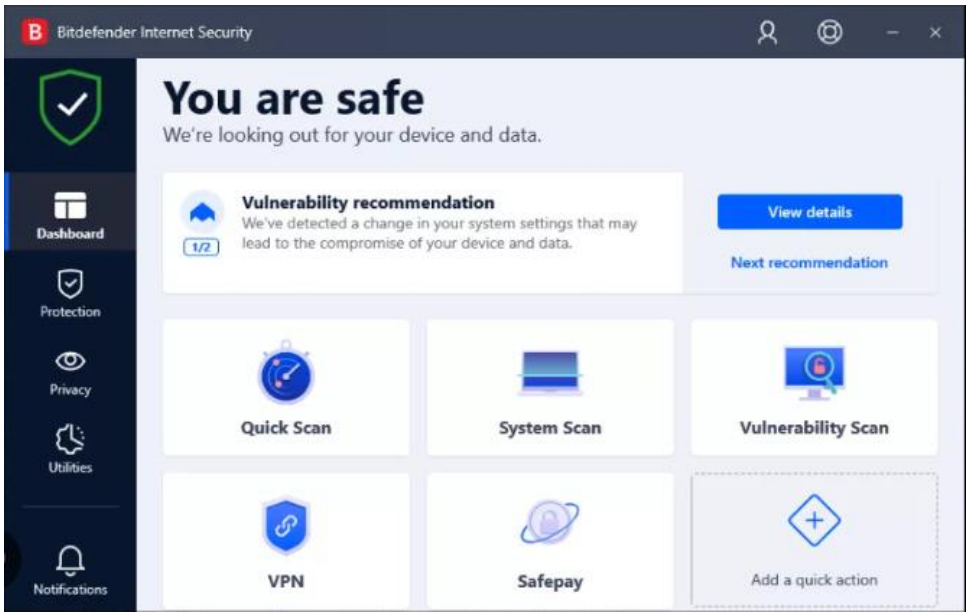



Рисунок 3.2.12. - Інтерфейс Bitdefender

5. Avast Antivirus: Avast Antivirus є безкоштовним антивірусним продуктом з великою кількістю функцій для базового захисту. Він виявляє й блокує шкідливі програми, має функцію аналізу пошти на наявність спаму і

фішингу, а також включає в себе фаєрвол для контролю мережевого з'єднання. Avast Antivirus також пропонує простий у використанні інтерфейс та можливість сканування системи на вимогу користувача [3].

Початковий інтерфейс виглядає так:

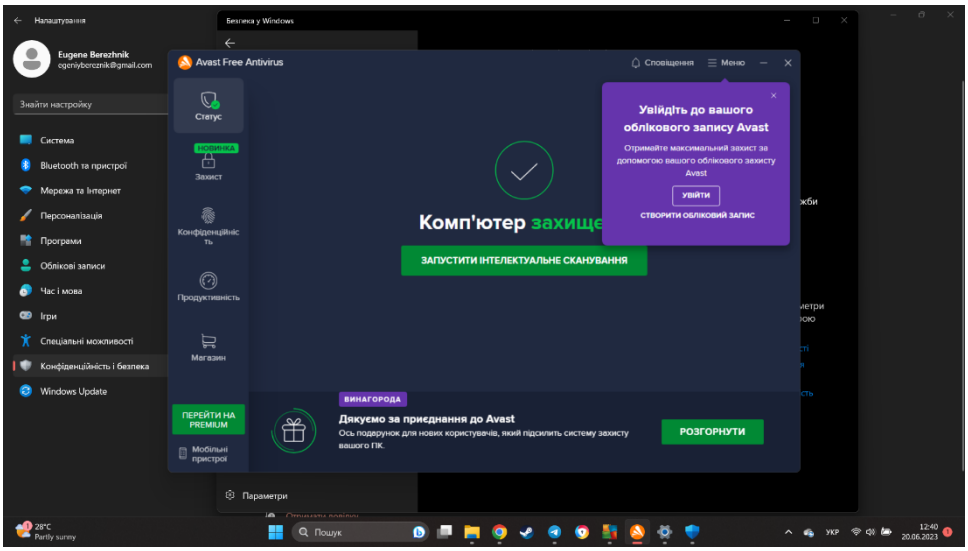



Рисунок 3.2.13. - Початковий інтерфейс Avast

На початку зображений статус комп’ютера, зліва знаходиться панель керування у верхньому правому кутику є кнопка “Меню” в якій можна налаштувати свій профіль в антивірусі та налаштувати сам антивірус.

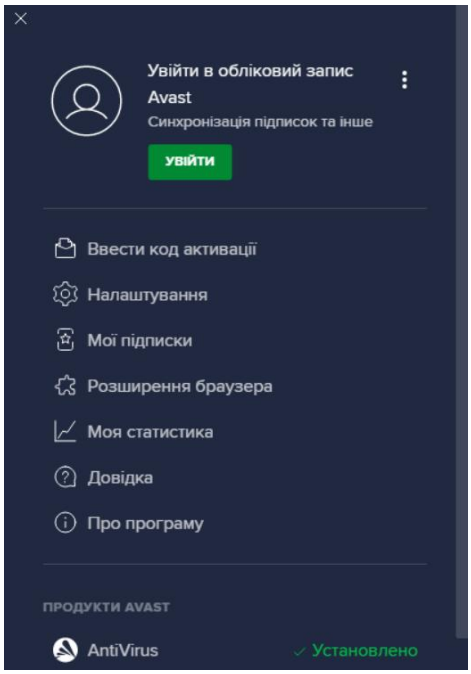


Рисунок 3.2.14. - Меню Avast

В відділі “Захист” показує функції захисту. Можливість запустити перевірку вірусів, переглянути стан карантину та файли які в ньому знаходяться, сканувати мережу.

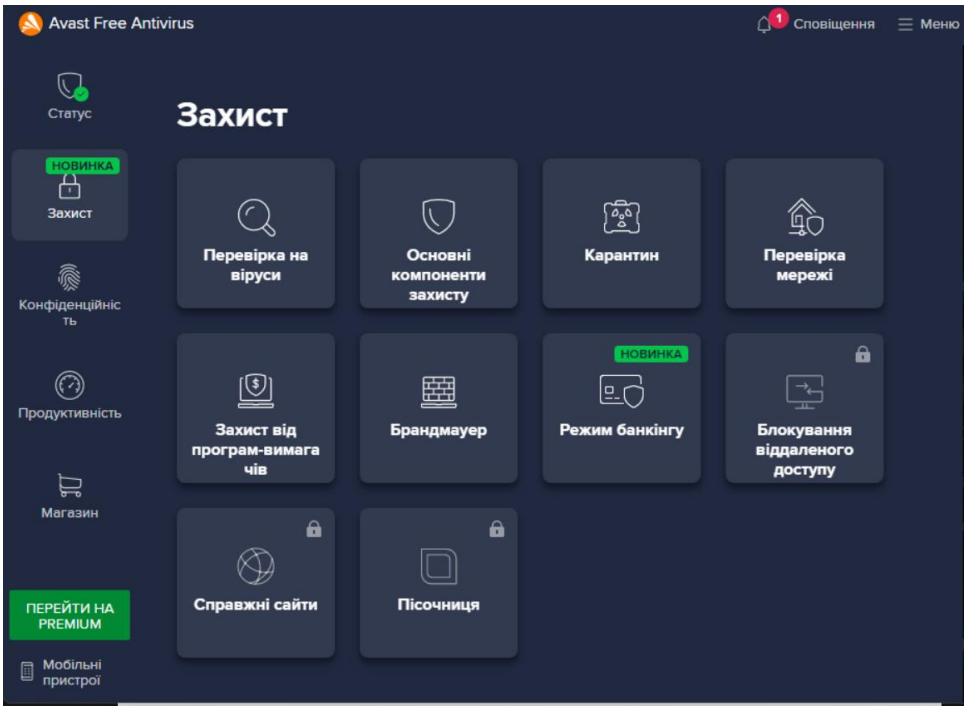



Рисунок 3.2.15. -Відділ “Захист”

В відділі “Конфіденційність” можна захистити свою веб камеру, Захистити конфіденційність даних, захистити паролі та не дозволити витоку в мережу.

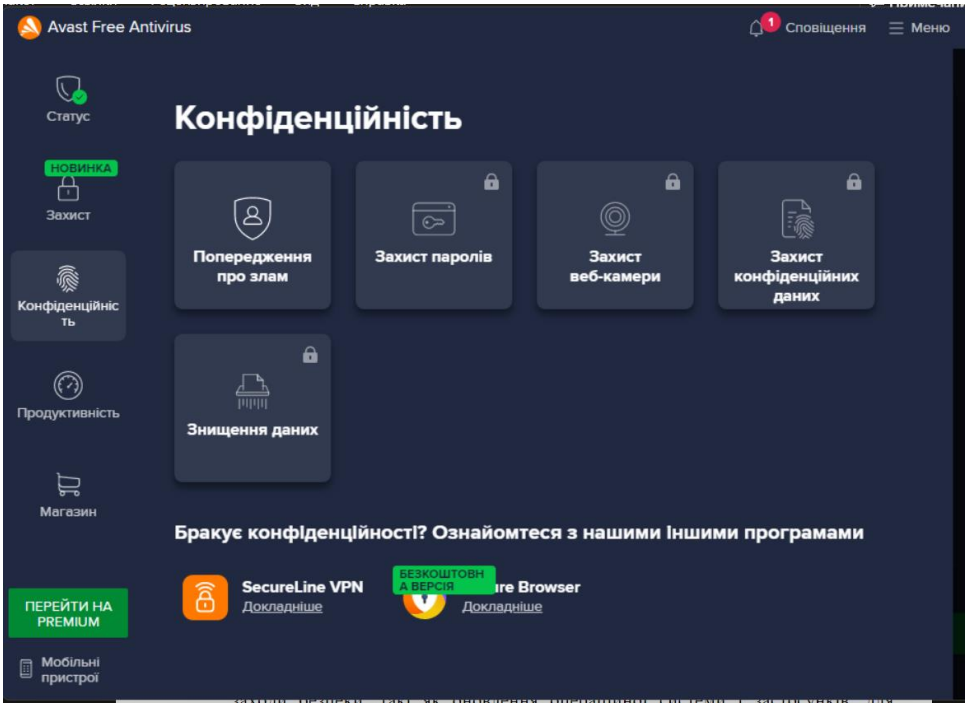



Рисунок 3.2.16. - Відділ “Конфіденційність”

Якщо ж перейти в налаштування Avast першим що ми побачимо це таку картину.

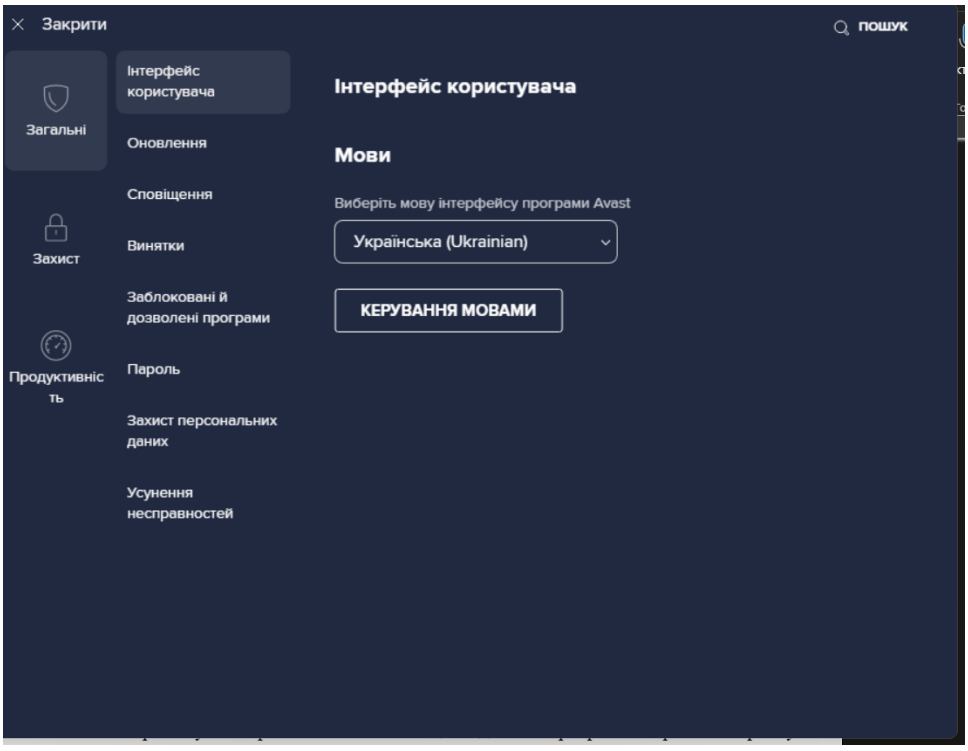



Рисунок 3.2.17. - Загальні налаштування

В налаштуваннях є три відділи. У першому відділі можна налаштувати загальні параметри. Такі як інтерфейс (змінити мову), керувати оновленнями програми та сповіщеннями. Можна добавити виняткові файли, сайти де програма не буде застосовувати ніяких дій.

Відділ “Захист” це той самий відділ, який знаходиться на початковому інтерфейсі, тільки трошки обрізаний та налаштований конкретно на захист без не потрібних моментів

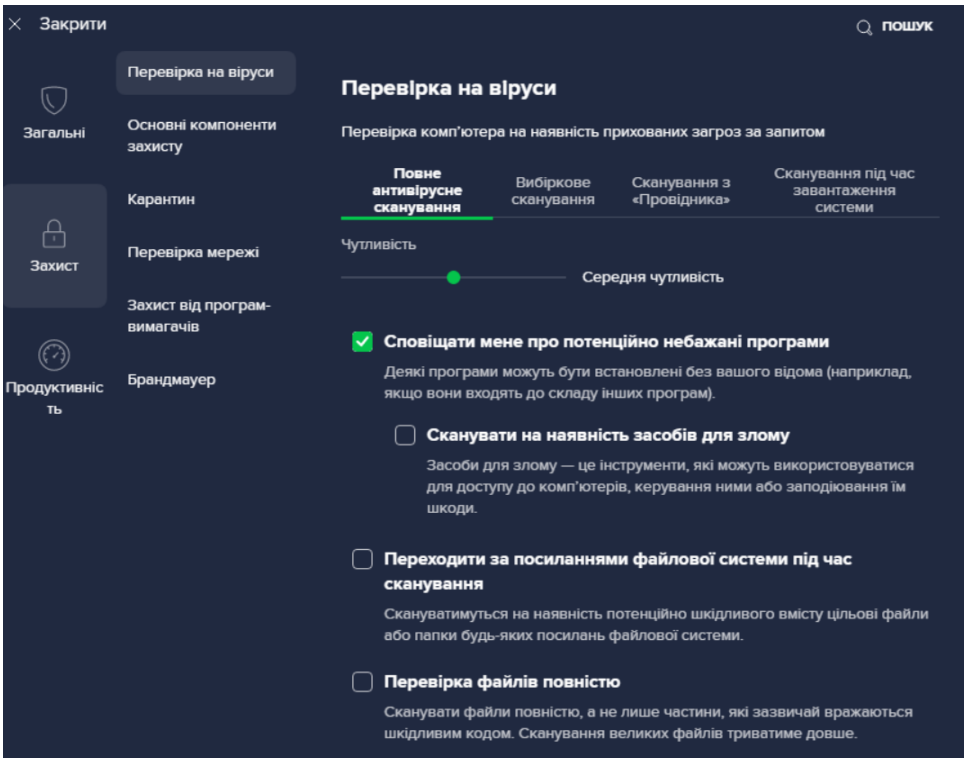



Рисунок 3.2.18. - Налаштування захисту

В відділі “Продуктивність” можна підвищити продуктивність комп’ютера шляхом призупинення функцій антивірусу під час гри тощо.

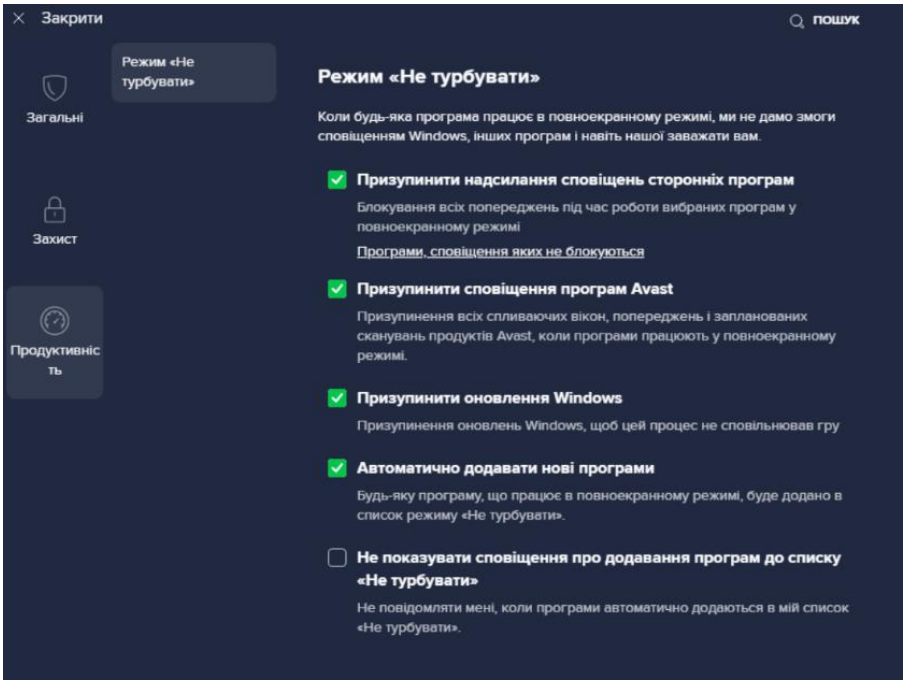



Рисунок 3.2.19. - Налаштування продуктивності

6. Windows Defender - це вбудована антивірусна програма, розроблена компанією Microsoft. Вона надає повноцінний захист від більшості сучасних загроз і включає різні модулі безпеки для виявлення підозрілих змін в реальному часі [11].

Так виглядає інтерфейс Windows Defender

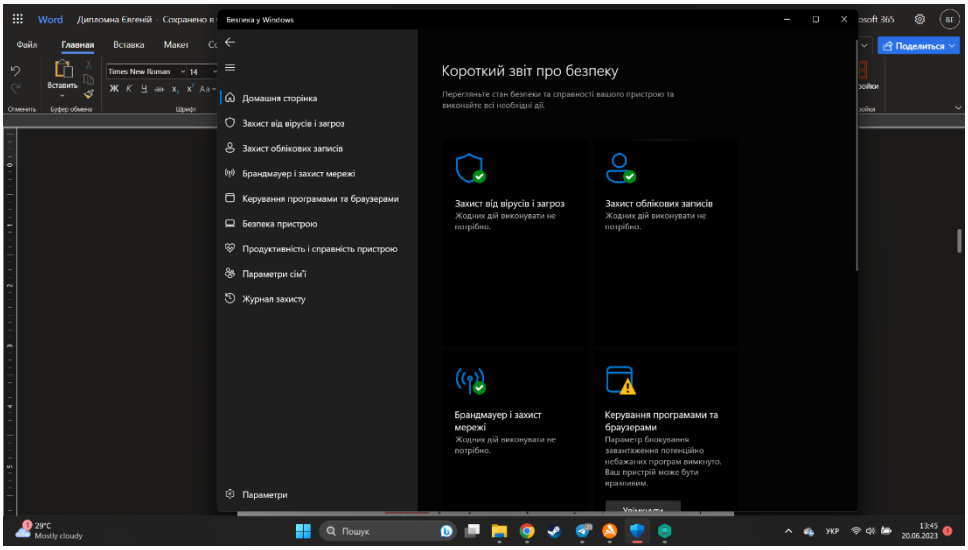



Рисунок 3.2.20. - Початковий інтерфейс Windows Defender

З приходу нас вітає “Короткий звіт про безпеку”. Тут показано коротко про стан комп’ютера та активні функції, показує також і не активні.

Зліва від короткого звіту в нас є панель керування

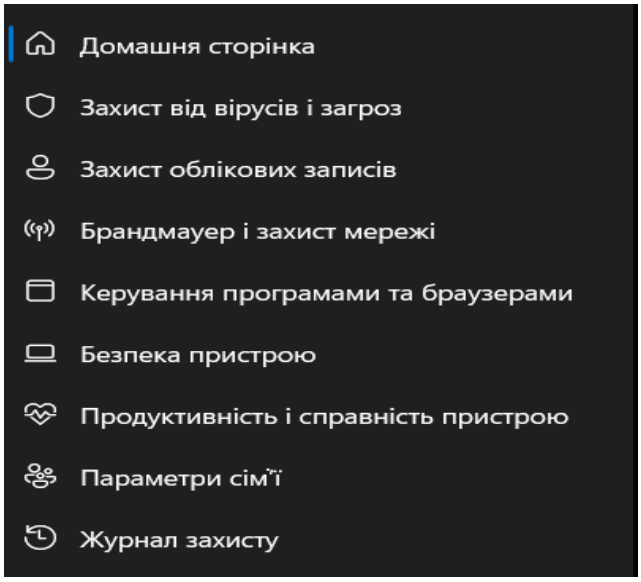



Рисунок 3.2.21. - Панель керування Windows Defender

Windows Defender може виконувати сканування системи для пошуку шкідливих програм, планувати регулярні перевірки і автоматично видаляти або поміщати підозрілі програми в карантин. Він використовує сигнатури для виявлення шкідливих програм і автоматично оновлює їх через Центр оновлення Windows.

Щоб активувати Windows Defender, необхідно видалити антивірусну програму стороннього розробника, якщо вона встановлена на комп'ютері. Включення Windows Defender можна здійснити через "Панель управління".

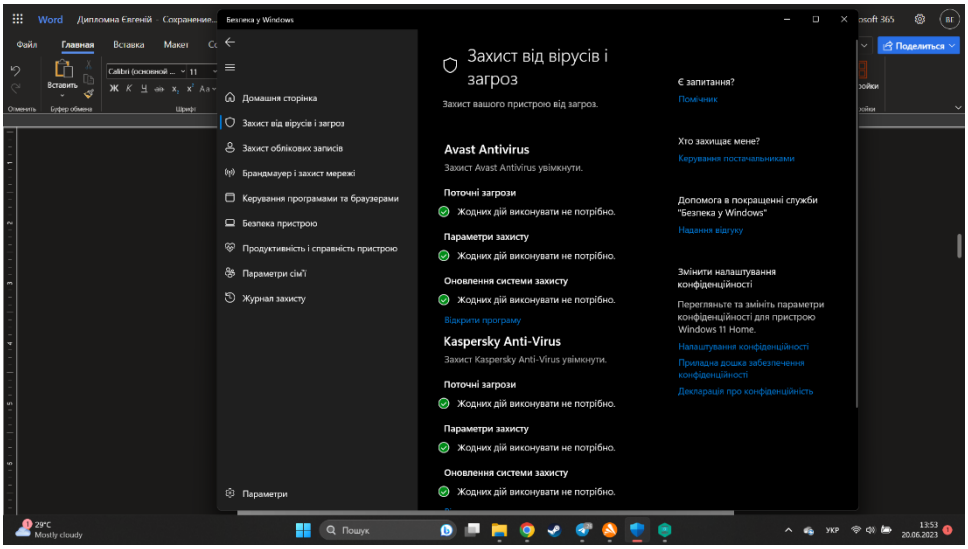



Рисунок 3.2.22. - Керування захистом від вірусів і загроз

Windows Defender пропонує захист в реальному часі, що сповіщає вас про спроби шкідливих програм виконати установку або змінити важливі параметри операційної системи. Також можна налаштувати та переглянути стан захисту мережі та сам стан брандмауера.

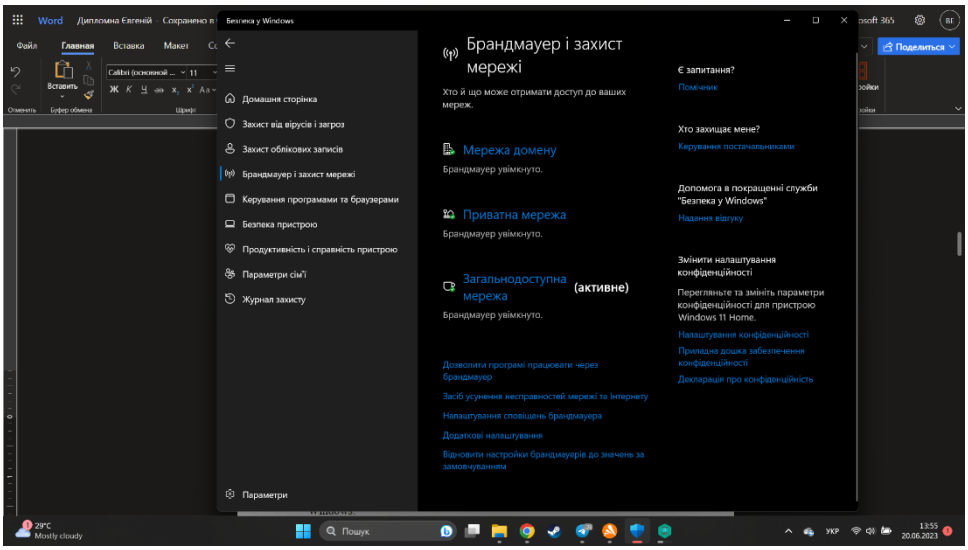



Рисунок 3.2.23. - Брандмауер Windows Defender

Програма Windows Defender має різні варіанти перевірки комп'ютера, включаючи швидку, повну і особливу перевірку, яку можна запустити з додатку або через панель управління.

Загалом, Windows Defender є повноцінним антивірусом, який може надати ефективний захист від загроз без необхідності установки додаткових програм сторонніх розробників.

Антивірусні програмні продукти грають важливу роль у захисті ПК від шкідливого програмного забезпечення та онлайн-загроз. Вони забезпечують виявлення, блокування та нейтралізацію вірусів та інших шкідливих програм у режимі реального часу. Завдяки постійному оновленню вірусних баз даних, вони здатні розпізнавати нові загрози та надавати надійний захист. Додаткові функції дозволяють підвищити рівень безпеки ПК і захистити користувачів від широкого спектру загроз в онлайн-середовищі. Отже, використання надійних антивірусних програмних продуктів є необхідним елементом безпеки в цифровому світі [10].

Функції різних антивірусів - різні. В таблиці (Таблиця 3.1), представлено функції вище описаних антивірусів

Таблиця 3.1 Порівняльний аналіз антивірусних програм

| Функції | Avast | Windows Defender | Kaspersky | AvgAntivirus | Bitdefender | Norton 360 |
|---|---|---|---|---|---|---|
| Перевірка на наявність вірусів | є | є | є | є | є | є |
| Брандмауер | є | є | є | є | є | є |
| Карантин | є | є | є | є | є | є |
| Батьківський контроль | є | є | є | немає | | є |
| Захист веб-камери | є | немає | немає | немає | немає | є |
| Самозахист | немає | немає | є | немає | немає | є |
| Підвищення продуктивності | є | є | є | є | є | є |

| | | | | | | |
|---|---|---|---|---|---|---|
| комп’ютера | | | | | | |

Переваги та недоліки обєднанні у таблиці (Таблиця 3.2)

Таблиця 3.2 Перваги та недоліки антивірусів

| Назва | Переваги | Недоліки |
|---|---|---|
| Avast | • Швидко працююча резидентна частина.<br>• Веб-антивірус, який контролює вихідні і вхідні пакети даних, скануючи все, що завантажується за допомогою браузера, поштового клієнта і клієнтів миттєвих повідомлень.<br>• Простий і зрозумілий інтерфейс.<br>• Незначне споживання системних ресурсів і висока швидкість сканування. | • Збільшення зростання споживання системних ресурсів при виставленні максимальних налаштувань безпеки;<br>• Не дуже гарні сигнатурні бази (при найнижчих установках евристики можливі помилкові спрацьовування);<br>• Сканер антивіруса не працює із запакованими і виконавчими файлами;<br>• Для роботи зі статистикою додатки потрібно встановити Flash Player, який дуже активно використовують для атак на браузер, що, звичайно ж, робить систему більш вразливою. |
| Windows Defender | • Швидко працююча резидентна частина;<br>• Рівень глибини сканування системи краще, ніж у більшості стороніх програм.<br>• Мінімальні системні вимоги до апартного забещпечення.<br>• невеликий процент хибних спрацювань; | • Іноді пропускає шкідливі програми.<br>• Відстає в цілому по потужності\надійності від лідерів сегмента.<br>• Відсутні додаткові функції, які не часто оновлюються. |

| | | |
|---|---|---|
| | • Повна відсутність реклами і додаткових сервісів;<br>• Автоматична активація.<br>• Відсутність збірки конфіденційної інформації для комерційного використання (вже все є в основній системі). | |
| Kaspeysky | • Захист від усіх видів інтернет-загроз.<br>• Повноцінний захист від усіх видів вірусів та атак, який включає евристичний аналіз, поведінкове блокування, перевірку по всіх базах.<br>• Перевірка трафіку, поштових повідомлень і файлів, що завантажуються в режимі реального часу.<br>• Батьківський контроль. | • Відсутній міжмережевий екран «FireWall».<br>• Батьківський контроль низької якості.<br>• Підвищене споживання ресурсів комп'ютера |
| AvgAntivirus | • Перевірка файлів перед завантаженням (компонент Online Shield), що підвищує рівень безпеки, блокуючи шкідливі програми до потрапляння на комп'ютер користувача;<br>• Перевірка безпеки посилань, що передаються у повідомленнях (компонент Online Shield);<br>• Пріоритетні оновлення (ці оновлення включають, крім антивірусних баз, оновлення модулів антивірусу);<br>• Доступ до технічних експертів для отримання підтримки та допомоги. | • Відсутність нормальної техпідтримки;<br>• Повільна робота на слабому ПК.<br>• Складні та заплутані налаштування.<br>• Немає Української мови. |

| | | |
|---|---|---|
| Bitdefender | • Постійно сканує комп'ютер на наявність шкідливого програмного забезпечення.<br>• Інформує користувача про виниклу загрозу.<br>• Видаляє і попереджує небезпечне ПЗ. | • Базовий рівень захисту і обмежений набір дій, які вживаються для безпеки.<br>• Безкоштовні версії можуть супроводжуватися постійним показом реклами. Найчастіше – закликає купити ліцензійний антивірус того ж розробника. |
| Norton 360 | • Високорівневий захист. Програма відрізняється наявністю сучасних модулів безпеки, які дозволяють швидко і точно виявляти загрози різного типу.<br>• Гнучкі налаштування. Ви можете вибрати спосіб сканування, папки та жорсткі диски, що перевіряються, налаштувати графік роботи та ступінь навантаження.<br>• Зрозумілий та наочний інтерфейс.<br>• Якісна підтримка.<br>• Доступність. Якщо ви поки що сумніваєтеся у покупці, то можете активувати пробну версію на 30-90 днів та оцінити всі можливості антивірусу. | • Висока ціна платної версії. Незважаючи на наявність деморежиму, після закінчення пробного періоду вам доведеться сплатити повну суму передплати.<br>• Вимоги до ПК. Norton вимагає багато системних ресурсів для повноцінної роботи. Особливо це помітно за повного сканування. Якщо у вас малопотужний ПК або ноутбук, доведеться попередньо налаштувати програму, щоб забезпечити швидкодію системи. |

Після проведення порівняльного аналізу антивірусних програм, варто зазначити що кращим з платних антивірусів це Norton 360, на даний момент це один з ефективних антивірусів, більшість людей дає йому перевагу за гарну технічну підтримку, за споживання меншої кількості ресурсів комп'ютера ніж безкоштовні антивіруси, також варто відмітити зручний інтерфейс.

З безплатних антивірусів кращою альтернативою є Avast, який має зручний інтерфейс, доступна також платна версія, яка відкриває багато можливостей для користування та більш детального захисту як комп'ютера, так і мережевої інформації (захист паролів, конфіденційність даних). У якості безкоштовного антивіруса він добре захищає від вірусів різних типів, починаючи від червяків та певних незначних шкідливих програм, до більш тяжких та серйозних - троянів. До ще однієї перевагою даного антивіруса є наявність фаєрвола який моніторить стан мережі та сканує в режимі реального часу всі мережеві процеси що відбуваються на комп'ютері, присутня постійна підтримка оновлень.

# 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

## 4.1. Психологічні причини нещасних випадків і травматизму

Нещасні випадки і травматизм є серйозною проблемою, що становить загрозу для громадського здоров'я і безпеки. Хоча фізичні фактори, такі як небезпечні умови праці, недосконаліть обладнання або небезпека дорожнього руху, часто визнаються як основні причини травматизму, психологічні аспекти також відіграють значну роль у виникненні нещасних випадків. Розглянемо психологічні причини, які можуть сприяти травмуванню і виявити важливість розуміння цих факторів для розробки стратегій активної безпеки [10].

1. Відволікання Однією з головних психологічних причин нещасних випадків є відволікання. Недостатня увага або зосередженість на інших завданнях може призвести до необережного поводження та неправильних рішень. Наприклад, використання мобільних пристроїв під час водіння є серйозним джерелом відволікання, що може призвести до аварій.
2. Стрес та емоції Стресові ситуації та емоції можуть впливати на нашу здатність приймати рішення та реагувати на небезпеку. Наприклад, люди, які перебувають під впливом значного стресу, можуть бути менш уважними та більш схильними до необережних дій, що збільшує ризик нещасних випадків.
3. Помилки при прийнятті рішень Психологічні процеси, пов'язані з прийняттям рішень, також можуть бути важливими факторами, які сприяють травматизму. Недостатнє оцінювання ризику, неправильне вирішення проблеми або погане планування можуть призвести до ситуацій, де людина опиняється в небезпеці.
4. Вплив оточення та соціального середовища Соціальне середовище і оточення також можуть мати значний вплив на безпеку. Наприклад, групова динаміка або вплив товаришів можуть спонукати до ризикованої

поведінки або приводити до безпечних вчинків. Також, психологічний тиск, включаючи соціальну конформність, може змушувати людей приймати ризиковані рішення, незалежно від власних переконань.

5. Стан свідомості Вживання алкоголю, наркотиків або недосипання можуть впливати на наш стан свідомості, знижуючи наші рефлекси, увагу та здатність приймати рішення. Це може призвести до необережного поводження і збільшити ризик нещасних випадків та травм.

Рівень травматизму в виробничій сфері тісно пов'язаний з технологічними процесами, обладнанням, організацією виробництва та ергономічною організацією робочого місця. В цьому контексті розглядаються організаційні, психофізіологічні та технічні причини, а також техногенні, природні, екологічні та соціальні причини [11].

Згідно з даними Фонду соціального страхування України, у 2020 році найбільш поширеними причинами страхових нещасних випадків були організаційні причини, які становили 52,7% від загальної кількості нещасних випадків. Інші причини спричинили 21,7% випадків, психофізіологічні причини — 16,6%, технічні причини — 7,4%, а причини, пов'язані з техногенними, природними, екологічними та соціальними факторами, склали 1,6% випадків.

Давайте розглянемо кожен з цих видів причин виробничого травматизму більш детально [17].

1. Організаційні причини: Ці причини пов'язані з організацією роботи та умовами праці. Сюди входять неправильна організація робочого процесу, недостатня підготовка працівників, відсутність необхідних інструкцій і заходів безпеки, недостатня комунікація між робочими, а також незадовільний стан обладнання і засобів праці.
2. Психофізіологічні причини: Ці причини пов'язані з психологічним станом працівників, їх емоційним станом, стресом, втомою і недосипанням. Негативні емоції та стрес можуть впливати на увагу та концентрацію, що збільшує ризик виникнення нещасних випадків.

3. Технічні причини: Ці причини пов'язані з технічним станом обладнання, його неправильним використанням, дефектами і несправностями. Недостатня безпека на робочому місці, неправильно встановлені заходи безпеки, відсутність необхідних пристроїв захисту також можуть сприяти виникненню травм.
4. Техногенні, природні, екологічні та соціальні причини: Ці причини пов'язані зі специфічними умовами праці, які можуть бути зумовлені природними факторами (погодні умови, природні катастрофи), техногенними аваріями, екологічним забрудненням або соціальними проблемами, такими як конфлікти на робочому місці або небезпека, пов'язана з взаємодією з публікою.

Вивчення цих причин та вживання відповідних заходів безпеки може допомогти покращити умови праці та зменшити ризик виробничого травматизму [14].

Розуміння психологічних причин нещасних випадків і травматизму є важливим кроком у розробці стратегій активного захисту. Звернення уваги на фактори, такі як відволікання, стрес та емоції, помилки при прийнятті рішень, вплив оточення та соціального середовища, а також стан свідомості, може допомогти визначити пріоритетні напрямки роботи щодо запобігання нещасним випадкам і зменшення ризику травматизму. Необхідно розробляти і впроваджувати програми попередження, спрямовані на підвищення свідомості та навичок безпеки серед населення.

## 4.2. Соціальне значення охорони праці

Охорона праці є важливим аспектом суспільної діяльності, який має значення не тільки для працівників, але й для суспільства в цілому. Недостатня увага до охорони праці може призвести до серйозних наслідків, таких як нещасні випадки на роботі, професійні захворювання та загрози для здоров'я та безпеки

працівників. Тому важливо розуміти соціальне значення охорони праці і вплив, який вона має на суспільство [8].

1. Безпека та здоров'я працівників.

Одним із основних аспектів охорони праці є забезпечення безпечних та здорових умов праці. Це охоплює впровадження заходів щодо попередження нещасних випадків на роботі, виявлення та контроль небезпечних факторів, надання необхідного захисту та навчання працівників правилам безпеки. Забезпечення безпеки працівників сприяє зменшенню травматизму, покращує їхнє фізичне та психічне здоров'я та підвищує загальний рівень безпеки суспільства.

2. Профілактика професійних захворювань.

Охорона праці також має на меті запобігання професійним захворюванням, які можуть виникати внаслідок впливу шкідливих факторів на робочому місці. Це можуть бути хімічні речовини, шум, вібрація, довготривале напруження тощо. Шляхом впровадження відповідних заходів профілактики, таких як використання захисного обладнання, контроль рівня шкідливих речовин, регулярні медичні огляди та навчання працівників, можна значно знизити поширеність професійних захворювань та покращити загальний стан здоров'я населення.

3. Економічні та соціальні переваги.

Ефективна система охорони праці має значні економічні та соціальні переваги для суспільства. По-перше, зниження кількості нещасних випадків та професійних захворювань призводить до зменшення витрат на лікування та компенсації, що сприяє економічному зростанню. По-друге, покращення умов праці, зменшення фізичного та психічного перевантаження, та створення безпечного та здорового робочого середовища сприяють підвищенню продуктивності праці, творчості та задоволеності працівників. Крім того, збереження здоров'я та безпеки працівників має позитивний вплив на їхню якість життя та загальний соціальний статус.

Основоположним документом, що регулює охорону праці в Україні, є Закон України "Про охорону праці". Він визначає два основних завдання охорони праці: інженерно-технічне та соціальне. Інженерно-технічне завдання полягає у запобіганні небезпечним подіям під час трудового процесу, а соціальне завдання забезпечує відшкодування матеріальної, моральної та соціальної шкоди, завданої внаслідок нещасного випадку або професійного захворювання, забезпечуючи захист працівників та їхні права.

Охорона праці базується на правових та організаційних основах. Правові основи включають закони, нормативно-правові акти, соціально-економічні та організаційні заходи, спрямовані на безпечну організацію праці, забезпечення працівників засобами захисту, компенсацію за важку роботу та роботу в шкідливих умовах, навчання працівників безпечним роботам, регламентацію відповідальності та відшкодування збитків у разі ушкодження здоров'я або смерті працівника [10].

Українське законодавство про охорону праці складається з таких взаємопов'язаних нормативно-правових актів, як Закон України "Про охорону праці", Кодекс законів про працю України, Закон України "Про загальнообов'язкове державне соціальне страхування" та інші нормативні акти, що прийняті відповідно до них.

Охорона праці має велике соціальне значення для суспільства. Вона сприяє забезпеченню безпеки та здоров'я працівників, запобігає професійним захворюванням та нещасним випадкам на роботі. Ефективна система охорони праці забезпечує економічні та соціальні переваги, включаючи зменшення витрат, підвищення продуктивності та покращення якості життя працівників. Для досягнення цих переваг необхідно постійно розвивати та впроваджувати ефективні стратегії охорони праці, сприяти підвищенню свідомості та освіті в галузі безпеки та здоров'я працівників, а також забезпечувати ефективний контроль та впровадження нормативних актів у сфері охорони праці. Тільки таким чином ми зможемо створити безпечне та здорове робоче середовище для всіх громадян та підвищити загальне соціальне благополуччя [11].

# ВИСНОВКИ

У ході проведеного порівняльного аналізу превентивного та активного захисту ПК від вірусів за допомогою сучасних антивірусних програмних продуктів було встановлено наступне.

Превентивний захист є ефективним і важливим компонентом безпеки ПК. Він дозволяє запобігати вторгненням інфекційних програм, шкідливих вірусів і троянських коней на ПК, шляхом використання антивірусних програм і фаєрволів. Такий захист передбачає регулярне оновлення антивірусних баз даних та виявлення відомих загроз, що дозволяє надійно захищати систему від відомих вразливостей і атак.

Активний захист, в свою чергу, виявляє і реагує на нові і невідомі загрози. Використання інтелектуальних систем виявлення загроз дозволяє аналізувати поведінку програм і виявляти аномальну активність, що може свідчити про наявність шкідливих програм. Цей підхід надає додатковий рівень захисту від невідомих загроз і забезпечує більш високу ефективність захисту ПК.

Слід зазначити, що обидва підходи до захисту ПК мають свої переваги та обмеження. Превентивний захист надійно захищає від відомих загроз, але може бути менш ефективним проти нових і невідомих вразливостей. Активний захист забезпечує виявлення нових загроз, але може супроводжуватися помилковими спрацюваннями і підвищеним навантаженням на систему.

З урахуванням потреб користувача рекомендується комбінування превентивного та активного захисту для найбільш ефективного захисту ПК від вірусів. Використання актуального антивірусного програмного забезпечення, фаєрволів, систем виявлення вторгнень та інтелектуальних систем виявлення загроз дозволить забезпечити комплексний захист і зменшити ризик інфікування ПК шкідливими програмами.

Для подальшого розвитку даної теми рекомендується проведення додаткових досліджень щодо оцінки ефективності різних антивірусних

програмних продуктів, вивчення нових технологій і методів інтелектуального виявлення загроз, а також врахування специфіки сучасних вірусних загроз та інноваційних підходів до захисту ПК.

Додатковою рекомендацією є проведення тестування різних антивірусних програмних продуктів з метою оцінки їх ефективності, швидкодії та навантаження на систему. Це дозволить користувачам обрати оптимальний антивірусний продукт, який задовольнить їхні потреби з точки зору безпеки та продуктивності.

Також важливим аспектом є регулярне оновлення антивірусних баз даних і програмного забезпечення. Виробники антивірусних програм надають регулярні оновлення для боротьби з новими вірусами і загрозами. Користувачі повинні пам'ятати про важливість оновлення своєї антивірусної програми, а також про активування автоматичного оновлення, яке дозволяє отримувати найсвіжіші визначення вірусів і заходи проти загроз.

Крім того, рекомендується зберігати резервні копії важливих файлів і даних. Це може бути корисно в разі випадкового видалення файлів або інфікування системи вірусом. Регулярне створення резервних копій допоможе відновити важливу інформацію в разі потреби.

У зв'язку зі зростаючими загрозами вірусів і кібератаками, користувачам ПК слід також зосередитися на освіті і підвищенні своєї кібербезпеки. Знання про основні принципи безпеки, такі як уникання небезпечних веб-сайтів, непідтверджених посилань і прикріплених файлів, допоможуть уникнути потенційних загроз і зберегти безпеку своїх ПК.

Нарешті, регулярне технічне обслуговування ПК, таке як встановлення оновлень операційної системи, перевірка наявності оновлень для встановлених програм і видалення застарілих або непотрібних програм, також є важливим елементом підтримки безпеки ПК. Застосування цих запобіжних заходів допоможе зменшити вразливості системи і підвищити її стійкість до потенційних загроз.

У висновку, превентивний та активний захист ПК є невід'ємною складовою кібербезпеки. Використання сучасних антивірусних програмних продуктів, актуальних антивірусних баз даних, фаєрволів, систем виявлення вторгнень та інтелектуальних систем виявлення загроз дозволяє забезпечити комплексний захист ПК і зменшити ризик інфікування вірусами та іншими шкідливими програмами. Однак, важливо пам'ятати, що жодна система захисту не є абсолютною, тому користувачам ПК також слід дотримуватись правил кібербезпеки, регулярно оновлювати програмне забезпечення та робити резервні копії даних. Тільки комплексний підхід забезпечить ефективний захист ПК і збереже цінну інформацію в безпеці.

Загалом, використання комплексного підходу до захисту ПК, поєднуючи превентивний та активний захист, є ключовим для забезпечення надійності, безпеки та захисту інформації у цифровому світі.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Законодавчі та нормативні документи України у сфері інформації, видавничої та бібліотечної справи: Тематична добірка: У 2-х ч. Ч.
2. Container security requires more than securing your images [Електронний ресурс] : https://developer.ibm.com/solutions/security/.
3. Snort instaling on Windows [Електронний ресурс] : https://www.snort.org/.

Steinberg J. Cybersecurity For Dummies / Joseph Steinberg., 2019. – 368 с. – (1st edition).

4. Ozkaya E. Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity / Erdal Ozkaya., 2019. – 396 с. – (Packt Publishing).
5. Mitnick K. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data / Kevin Mitnick., 2019. – 320 с.
6. Mining E. Kali Linux Hacking: A Complete Step by Step Guide to Learn the Fundamentals of Cyber Security, Hacking, and Penetration Testing. Includes Valuable Basic Networking Concepts. / Ethem Mining., 2019. – 175
7. Антивірусні програми світови брендів. [Електронний ресурс] : https://core.ac.uk/reader/47229590
8. Сучасні технології комп’ютерної безпеки .О.М. Черкун 2012 -91с.
9. Методи захисту. Захист від зовнішніх вторгнень. Навчальний посібник для вузів. С. Н. Никифоров. 2023. 94с.