Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувач кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«_____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 «Кібербезпека»
(код і назва спеціальності)
освітній ступінь бакалавр
освітня програма Кібербезпека
(назва освітньої програми)
на тему: Засоби захисту інформаційних ресурсів від шкідливого програмного забезпечення

Виконавець: студент IV курсу, групи КБ-42

_____ **Василь ПЛИСЮК**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник роботи	Микола БРАІЛОВСЬКИЙ	

Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-42** (група) **Плисюку Василю Миколайовичу** (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Засоби захисту інформаційних ресурсів від шкідливого програмного забезпечення

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Аналіз інфраструктури, ідентифікація потенційних загроз, оцінка вразливостей вибір захисних заходів, оцінка поточного стану інфраструктури

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Основні поняття інформаційного ресурсу, визначення та класифікація шкідливого програмного забезпечення, Методи та технології протидії шкідливому програмному забезпеченню, Огляд сучасних антивірусних програм, Вибір підходів та технологій для розробки системи захисту, Розробка архітектури системи захисту інформаційних ресурсів

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність полягає у розробці та впровадженні ефективних стратегій, методів та інструментів для захисту інформаційних ресурсів

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Василь ПЛИСЮК
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 28.01.2023	*виконано*
2	Аналіз літератури	29.01.2023 – 11.02.2023	*виконано*
3	Обґрунтування вибору рішення	12.02.2023 – 15.02.2023	*виконано*
4	Класифікація шкідливого програмного забезпечення	16.02.2023 – 04.03.2023	*виконано*
5	Аналіз проблем інформаційної безпеки в інформаційних ресурсах	05.03.2023 – 21.03.2023	*виконано*
6	Дослідження особливостей і вразливостей інформаційних ресурсів	22.03.2023 – 08.04.2023	*виконано*
7	Розробка системи захисту від шкідливого програмного забезпечення	09.04.2023 – 10.05.2023	*виконано*
8	Оформлення пояснювальної записки	11.05.2023 – 27.05.2023	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2020 – 12.06.2023	*виконано*

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Василь ПЛИСЮК
(підпис) (ім'я, прізвище)

Термін подання дипломної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел. Основний текст займає 62 сторінок, включає в себе зміст, вступ, три розділи дипломної роботи, висновки та список джерел. У пояснювальній записці дипломної роботи міститься 17 рисунків і 3 таблиці. Список використаних джерел містить 39 посилань та займає 4 сторінки.

Метою роботи є розробка системи захисту інформаційних ресурсів від шкідливого програмного забезпечення.

Об'єктом дослідження є процес захисту інформаційних ресурсів в комп'ютерних системах.

Предметом дослідження **є** засоби захисту інформаційних ресурсів від шкідливого програмного забезпечення.

Методи дослідження:

- аналіз відкритих джерел;
- порівняння методів захисту;
- створення системи захисту;

Практичною цінність полягає у розробці та впровадженні ефективних стратегій, методів та інструментів для захисту інформаційних ресурсів від шкідливого програмного забезпечення.

Ключові слова: шкідливе програмне забезпечення, віруси, шпигунське ПЗ, кібербезпека, засоби захисту, антивірусні програми, брандмауер, криптографічний захист, біометрична ідентифікація, мережева безпека, резервне копіювання, аутентифікація.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕННЬ

ШПЗ	–	Шкідливе Програмне Забезпечення
ПЗ	–	Програмне Забезпечення
AI	–	Штучний Інтелект
IoT	–	Інтернет Речей
IT	–	Інформаційні Технології
IP	–	Інформаційний Ресурс
КС	–	Комп’ютерна Система
ОС	–	Операційна Система
CIA	–	Конфіденційність, Цілісність, Доступність

ВСТУП

Захист інформації є однією з найбільш актуальних проблем на сучасному етапі розвитку інформаційного суспільства. Інформація стає все більш цінним ресурсом, який потрібно захищати від зовнішніх та внутрішніх загроз. Особливо актуальним є захист інформаційних ресурсів від шкідливого програмного забезпечення (ШПЗ).

Шкідливе програмне забезпечення є однією з найбільш поширених загроз в інформаційній безпеці. Воно може призвести до виходу інформації з-під контролю, порушення конфіденційності, цілісності та доступності інформаційних ресурсів. Тому розробка та вдосконалення засобів захисту від шкідливого програмного забезпечення є надзвичайно важливою задачею.

Метою даної дипломної роботи є вивчення основних видів шкідливого програмного забезпечення та методів їх поширення, огляд технологій та засобів захисту від шкідливого програмного забезпечення, аналіз стану безпеки інформаційних ресурсів та розробка системи захисту. Для досягнення цієї мети в роботі будуть вирішуватись такі завдання:

1. Дослідити поняття шкідливого програмного забезпечення та визначити його основні види.
2. Розглянути методи поширення шкідливого програмного забезпечення та визначити основні принципи його роботи.
3. Оглянути методи захисту від шкідливих програм та технології і засоби захисту від шкідливого програмного забезпечення.
4. Проаналізувати стан безпеки інформаційних ресурсів та виявити слабкі місця систем захисту.
5. Розробити та випробувати власні засоби захисту від шкідливих програм.
6. Порівняти ефективність різних методів та засобів захисту від шкідливого програмного забезпечення.

У розділі 1 "ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ " досліджено основні поняття та види шкідливого програмного забезпечення, методи його

поширення, методи захисту від шкідливих програм, технології та засоби захисту від шкідливого програмного забезпечення.

У розділі 2 "АНАЛІЗ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ " проаналізовано проблеми безпеки інформаційних ресурсів, порівняні різні методи та засоби захисту, виявлені слабкі місця систем захисту.

У розділі 3 «РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ» представлена практична частина, де описуються методи тестування та валідації засобів захисту від шкідливого програмного забезпечення, та розробка системи захисту інофрмації.

РОЗДІЛ 1
ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1 Основні поняття інформаційного ресурсу

Інформаційний ресурс так як у [1] — це сукупність відомостей, що знаходяться в організації або за її межами, і можуть бути використані для досягнення її цілей. Інформаційні ресурси можуть представляти собою дані, інформацію, знання та інші види цінностей, які можуть бути використані в бізнес-процесах.

Дані: Це сировина, з якої формується інформація. Дані - це факти, статистика, числа, слова, без конкретного контексту чи обробки.

Інформація: Це дані, які були оброблені таким чином, що вони мають значення для користувача. Інформація має контекст і може бути використана для прийняття рішень.

Знання: Це інформація, яку людина або організація використовує для дій або рішень. Знання базуються на інформації, досвіді, інтуїції та навчанні.

Інформаційна система: Це система, яка збирає, обробляє, зберігає та поширює інформацію. Інформаційна система може бути технологічною (наприклад, комп'ютерна система) або не технологічною (наприклад, бібліотека).

Безпека інформації: Це захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, зміни, знищення або переривання.

Конфіденційність, цілісність та доступність (CIA): Це три основні цілі безпеки інформації.

Конфіденційність — це запобігання несанкціонованого доступу до інформації. Це означає, що інформація доступна лише для тих, хто має на це право.

Цілісність — це забезпечення точності та повноти інформації. Це означає, що інформація захищена від несанкціонованих змін, будь-то випадкових або навмисних.

Доступність — це забезпечення надійного та своєчасного доступу до інформації для тих, хто має на це право. Системи та сервіси мають бути доступні для використання при потребі.

Інформаційні активи: Це специфічні елементи інформації, які мають цінність для організації. Це може включати документи, бази даних, програмне забезпечення, інтелектуальну власність, персональні дані клієнтів та інше.

Інформаційний ризик: Це потенційна загроза для безпеки інформаційних активів, яка може призвести до втрати цілісності, доступності або конфіденційності.

Інформаційна політика: Це набір правил та процедур, що визначають, як організація повинна керувати, зберігати, передавати та захищати свою інформацію.

1.2 Визначення та класифікація шкідливого програмного забезпечення

Шкідливе програмне забезпечення (ШПЗ) так як у [10] - це програми або коди, розроблені з метою несанкціонованого доступу, завдання шкоди або крадіжки інформації з комп'ютерних систем і мереж. ШПЗ може мати різні форми та функції, але усі вони створюють загрозу для безпеки інформаційних ресурсів.

Класифікація шкідливого програмного забезпечення так як [11]:

• Віруси - програми, які здатні самостійно розмножуватися, вбудовуючись в інші програми або файлі. Вони можуть завдавати шкоди системам, змінюючи або видаляючи файли, сповільнюючи роботу комп'ютера та перешкоджаючи роботі користувача.

• Мережевий хробак - відрізняються від вірусів тим, що не потребують вбудовування в інші програми для розмноження. Вони самостійно розповсюджуються через мережі, використовуючи їхні недоліки та уразливості.

• Троянські коні - програми, які маскуються під корисне програмне забезпечення, але насправді забезпечують зловмисникам несанкціонований доступ до комп'ютера або мережі.

• Руткіти - програми, які дозволяють зловмисникам приховано контролювати систему, захищаючи себе від виявлення антивірусними програмами та іншими засобами захисту.

• Рекламне ПЗ (Adware) - програми, які автоматично відображають небажану рекламу на комп'ютері користувача. Вони можуть уповільнювати роботу системи та збільшувати ризик інфікування іншими видами ШПЗ.

• Шпигунське ПЗ (Spyware) - програми, які без відома користувача збирають інформацію про користувача, його дії та звички в Інтернеті. Шпигунське ПЗ може передавати ці дані зловмисникам, які використовують їх для крадіжки ідентифікаційних даних, шахрайства або інших злочинних дій.

• Програма вимагач (Ransomware) - шкідливе програмне забезпечення, яке шифрує дані на комп'ютері користувача та вимагає від нього відшкодування (найчастіше у вигляді криптовалюти) за їх розшифровку. Відмова від оплати може призвести до втрати даних.

• Криптомайнери (Crypto-miners) - програми, які використовують ресурси комп'ютера користувача для видобутку криптовалюти без його відома та згоди. Криптомайнери можуть значно сповільнити роботу системи та зносити обладнання.

• Ботнети (Botnets) - мережі заражених комп'ютерів, які контролюються зловмисниками на відстані. За допомогою ботнетів зловмисники можуть проводити DDoS-атаки, розсилати спам або інфікувати інші системи.

• Фішинг (Phishing) - техніка, що використовується зловмисниками для отримання конфіденційних даних користувачів, таких як паролі, номери кредитних карт та інші особисті дані. Зазвичай відбувається через фальшиві електронні листи або повідомлення, які виглядають надійними.

Ця класифікація шкідливого програмного забезпечення допомагає краще розуміти потенційні загрози та розробляти ефективні стратегії захисту інформаційних ресурсів. Важливо пам'ятати, що нові види ШПЗ постійно з'являються, тому регулярне оновлення безпекових програм та систем, а також розширення знань і навичок в галузі кібербезпеки є ключовими факторами у захисті від потенційних кібератак.

Важливо відмітити, що кожен вид шкідливого програмного забезпечення вимагає відповідного підходу до його виявлення та нейтралізації. Наприклад, віруси та хробаки можуть бути виявлені та видалені за допомогою антивірусних програм, тоді як виявлення руткітів часто вимагає спеціалізованих інструментів.

Також важливо зауважити, що шкідливе програмне забезпечення часто використовує комбіновані тактики, включаючи одночасне використання різних видів шкідливого ПЗ для забезпечення максимальної шкоди або вигоди для зловмисника. Тому комплексний підхід до кібербезпеки, який включає в себе антивірусні програми, файрволи, системи виявлення вторгнень, а також регулярне навчання та освіту користувачів, є важливим для захисту від шкідливого програмного забезпечення.

Враховуючи швидкий розвиток технологій та постійне зростання кількості та складності кіберзагроз, важливість розуміння та захисту від шкідливого програмного забезпечення не може бути переоцінена. Тому ця тема продовжує бути актуальною для наукових досліджень та практичної роботи в галузі кібербезпеки.

1.3 Методи та технології протидії шкідливому програмному забезпеченню

Методи та технології протидії шкідливому програмному забезпеченню так як у [12] складаються з різних заходів, що спрямовані на запобігання, виявлення та реагування на кібератаки. Ось декілька з них:

• Антивірусне програмне забезпечення: Сучасні антивіруси використовують різні технології для виявлення та блокування шкідливого ПЗ, включаючи сигнатурне сканування, поведінковий аналіз, евристичне сканування, та аналіз у хмарі.

• Оновлення та виправлення помилок ПЗ (patching): Регулярне оновлення всього програмного забезпечення, включаючи операційні системи, додатки та антивірусні програми, допомагає захистити від шкідливого ПЗ, яке може використовувати відомі уразливості.

• Системи виявлення та попередження вторгнень (IDS/IPS): Ці системи моніторять мережевий трафік на наявність підозрілих активностей або відомих загроз та можуть автоматично блокувати або повідомляти про такі дії.

• Пісочниці: Це ізольовані середовища, де можна безпечно виконувати підозрілі або невідомі програми, щоб побачити, що вони роблять, без ризику пошкодження основної системи.

• Програми контролю за застосунками (Application Control): Ці програми дозволяють тільки відомим та довіреним програмам виконуватися на системі, що значно обмежує можливість виконання шкідливого ПЗ.

• Фільтрація веб-трафіку та електронної пошти: Ці технології блокують доступ до відомих шкідливих веб-сайтів та автоматично сканують електронну пошту на наявність шкідливих вкладень та посилань.

• Множинні рівні захисту (Defense in Depth): Цей підхід передбачає використання декількох шарів захисних заходів для забезпечення безпеки, так що, якщо один з них не вдається, інші продовжують забезпечувати захист.

• Блокування виконання скриптів: Багато шкідливого ПЗ використовує скрипти для своєї роботи. Налаштування системи на блокування автоматичного виконання скриптів може допомогти в захисті.

• Кібергігієна: Прості кроки, такі як регулярна зміна паролів, обережне поводження з електронною поштою та використання двофакторної автентифікації, можуть допомогти в захисті від шкідливого ПЗ.

• Шифрування даних: Шифрування важливих даних може допомогти захистити їх в разі інфікування шкідливим ПЗ, особливо програмою вимагачем.

• Прогнозування та аналіз шкідливого ПЗ: Із застосуванням методів машинного навчання та штучного інтелекту можна аналізувати патерни поведінки шкідливого ПЗ та прогнозувати його подальший розвиток.

• Розробка нових антивірусних алгоритмів: Нові методи виявлення та блокування шкідливого ПЗ постійно розробляються для протистояння новим загрозам.

• Дослідження в області кіберінтелекту: Шкідливе ПЗ часто використовує дедалі більш складні та хитромудрі методи атаки. Дослідження в цій області можуть допомогти розробити ефективніші методи захисту.

• Створення ефективних стратегій реагування на інциденти: Якщо атака все ж таки відбулася, важливо мати чіткий план дій для мінімізації шкоди та відновлення роботи систем.

Найбільш ефективним підходом до захисту від шкідливого програмного забезпечення є поєднання технологічних заходів зі здоровим глуздом і обережністю. Регулярне навчання та освіта користувачів також є важливими для забезпечення їхнього розуміння потенційних загроз та того, як їх уникнути.

Враховуючи наведені вище методи та технології, слід пам'ятати, що шкідливе програмне забезпечення постійно розвивається, а зловмисники намагаються відшукати нові способи обходу захисних механізмів. Тому важливою складовою боротьби з шкідливим ПЗ є наукові дослідження та розробка нових технологій захисту.

Отже, забезпечення захисту від шкідливого програмного забезпечення вимагає постійних зусиль, які включають в себе не лише використання існуючих технологій та методів, але й проведення постійних досліджень та розробку нових рішень.

1.4 Основні підходи до захисту інформаційних ресурсів

Захист інформаційних ресурсів вимагає комплексного підходу, який включає різноманітні стратегії та технології. Деякі з основних підходів включають:

• Фізичний захист: Це охоплює заходи для забезпечення фізичного захисту обладнання та носіїв даних, включаючи контроль доступу, системи відеоспостереження, захист від пожежі та інших надзвичайних ситуацій.

• Технологічний захист: Захист від кіберзагроз, таких як шкідливе програмне забезпечення, вторгнення в мережі, атаки типу "відмова в обслуговуванні" (DoS або DDoS), і т.д. Використовуються різноманітні технології, включаючи антивіруси, брандмауери, системи виявлення та попередження вторгнень (IDS/IPS), шифрування даних, двофакторна автентифікація, і т.д.

• Адміністративний захист: Це охоплює політики та процедури, які регулюють доступ до інформаційних ресурсів. Такі політики можуть включати контроль доступу на основі ролей (RBAC), політику мінімальних привілеїв, політику паролів, і т.д.

• Правовий захист: Законодавство та нормативні акти можуть надавати основу для захисту інформаційних ресурсів. Це може включати закони про захист даних, кіберзлочини, авторські права.

• Освітні та навчальні програми: Освіта користувачів та персоналу є важливим елементом захисту інформаційних ресурсів. Це може включати навчання з кібербезпеки, з безпечного користування Інтернетом, інформування про актуальні загрози та способи їх уникнення, і так далі.

• Регулярний моніторинг та аудит: Важливо постійно моніторити стан інформаційних систем, проводити аудити безпеки для виявлення потенційних слабких місць та проводити корективні заходи, коли це потрібно.

• Планування відновлення після аварії: Незважаючи на всі заходи захисту, можливість аварії або серйозного інциденту безпеки не може бути повністю виключена. Ефективне планування відновлення після аварії допомагає забезпечити, що організація може відновити свою діяльність з мінімальними збитками.

• Застосування принципу мінімуму довіри: Цей принцип полягає у наданні обмеженого доступу до ресурсів лише тим особам, яким це дійсно необхідно для виконання їх обов'язків. Це допомагає зменшити ризик недозволеного доступу або витоку інформації.

• Використання сучасних технологій захисту: Такі технології, як штучний інтелект та машинне навчання, можуть бути використані для виявлення аномалій та потенційних загроз.

Отже, захист інформаційних ресурсів вимагає комплексного підходу, який об'єднує різні методи та технології, а також включає в себе адміністративні, технологічні та освітні аспекти.

1.5 Компоненти системи захисту інформації

Система захисту інформації є складною і багатокомпонентною, оскільки вона повинна забезпечувати захист на різних рівнях і протистояти різноманітним видам загроз. Основні компоненти системи захисту інформації включають:

• Антивірусне програмне забезпечення: Воно забезпечує захист від шкідливого програмного забезпечення, такого як віруси, троянські програми, шпигунське програмне забезпечення та інше.

• Брандмауери (Firewalls): Вони контролюють вхідний та вихідний мережевий трафік і блокують потенційно шкідливі пакети даних.

• Системи виявлення та попередження вторгнень (IDS/IPS): Ці системи постійно моніторять мережевий трафік і виявляють підозрілу активність, яка може вказувати на спробу вторгнення.

• Шифрування: Шифрування даних може забезпечити захист від несанкціонованого доступу, навіть якщо дані були перехоплені або викрадені.

• Контроль доступу: Включає в себе різні механізми, такі як автентифікація користувачів, контроль доступу на основі ролей (RBAC), політику мінімальних привілеїв, і т.д.

• Резервне копіювання та відновлення даних: Ці компоненти забезпечують можливість відновлення даних після втрати або пошкодження в результаті атаки або технічної несправності.

• Політики безпеки: Це включає в себе різні процедури та політики, розроблені для підтримки безпечної експлуатації системи, включаючи політики паролів, політики використання інтернету, політики обробки даних та інші.

• Фізичний захист: Включає в себе заходи для захисту фізичного обладнання, включаючи сервери, мережеве обладнання, робочі станції та пристрої зберігання даних, від несанкціонованого доступу, пошкоджень або крадіжки.

• Освітні програми: Освіта користувачів є критично важливою частиною будь-якої системи захисту інформації. Користувачі повинні знати про потенційні загрози і як їм потрібно діяти для запобігання витоку або втраті даних.

• Регулярний аудит та оцінка безпеки: Це означає проведення періодичних перевірок та оцінок системи безпеки з метою ідентифікації потенційних слабких місць та вдосконалення заходів безпеки.

Всі ці компоненти взаємодіють між собою, щоб створити цілісну систему захисту інформації, яка може протистояти широкому спектру загроз і забезпечити надійний захист інформаційних ресурсів.

Висновки за розділом 1

Вивчення теоретичних основ захисту інформаційних ресурсів відбувається в контексті широкого спектра понять, що включає в себе аспекти інформаційної безпеки, кібербезпеки, шкідливого програмного забезпечення та протидії йому. Ця область є важливою для оцінки сучасних викликів та загроз, з якими стикається цифрове суспільство.

Інформаційні ресурси представляють собою активи, які потребують захисту. Вони можуть включати дані, програмне забезпечення, апаратне забезпечення, мережі та людський капітал. Теоретичні основи захисту інформаційних ресурсів включають розуміння природи цих ресурсів та способів їх захисту від різних видів загроз.

Шкідливе програмне забезпечення є однією з ключових загроз для інформаційних ресурсів. Воно включає в себе віруси, хробаки, троянські програми, руткіти, шпигунське ПЗ та інше. Важливо розуміти характеристики цих загроз, їх способи поширення та потенційні наслідки для інформаційних ресурсів.

Захист від шкідливого програмного забезпечення включає в себе ряд стратегій та технологій, включаючи антивірусні програми, брандмауери, системи виявлення вторгнень, криптографічні механізми, попереднє виявлення вразливостей, обмеження доступу та інше.

Також включають розуміння людського фактору в інформаційній безпеці. Навчання та освіта користувачів, створення культури безпеки, впровадження політик і процедур безпеки – все це важливі складові захисту інформаційних ресурсів.

Також важливим є впровадження проактивного підходу до інформаційної безпеки, який передбачає не лише реагування на інциденти безпеки, а й їхнє попередження. Це може включати моніторинг мережі на предмет аномалій, регулярні оцінки безпеки, тестування на проникнення та ін.

Розробка політики інформаційної безпеки, яка включає в себе як технологічні, так і організаційні аспекти, є важливою складовою основ захисту. Організаційні аспекти можуть включати розподіл обов'язків та відповідальності, аудити безпеки, розробку планів відновлення після аварійних ситуацій та ін.

Використання міжнародних стандартів та нормативів, таких як ISO 27001, може допомогти організаціям встановити ефективні системи управління безпекою інформації.

У цілому, основи захисту інформаційних ресурсів надають фундамент для розуміння, як виявляти, запобігати, реагувати та відновлювати системи від шкідливого програмного забезпечення та інших загроз інформаційній безпеці.

РОЗДІЛ 2
АНАЛІЗ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1 Огляд сучасних антивірусних програм

Антивірусна програма - це програмне забезпечення, що використовується для запобігання, виявлення і видалення зловмисного програмного забезпечення, зокрема вірусів, троянів, шпигунського програмного забезпечення та рекламного ПЗ.

Основні функції антивірусних програм включають:

• Сканування файлів для виявлення та видалення зловмисного програмного забезпечення

• Веб-захист, який блокує доступ до зловмисних веб-сайтів

• Захист від шпигунського програмного забезпечення, що використовується для крадіжки особистої інформації

• Захист електронної пошти, що перевіряє отримані та відправлені повідомлення на наявність шкідливих приєднаних файлів або посилань

• Фаєрвол для контролю мережевого трафіку та запобігання несанкціонованому доступу до комп'ютера

Деякі з антивірусних програм пропонують безкоштовні версії, але повнофункціональні платні версії зазвичай надають більше захисту.

Norton 360 Deluxe: відомий своєю сильною захистною спроможністю та широким спектром функцій, включаючи VPN, менеджер паролів, резервне копіювання в хмарі та багато іншого.

Bitdefender Antivirus Plus: надає надійний захист проти вірусів та шкідливого програмного забезпечення, а також надає корисні додаткові функції, такі як VPN, захист від шахрайства, захист від трекінгу в браузері та інше.

Webroot SecureAnywhere AntiVirus: є легким антивірусним рішенням, яке використовує хмарні технології для швидкого виявлення та видалення загроз. Воно також включає функції, такі як файрвол, захист від фішингу та менеджер паролів.

McAfee Total Protection надає широкий спектр функцій, включаючи антивірус, файрвол, захист від шахрайства, VPN, менеджер паролів, резервне копіювання в хмарі та багато іншого.

Avast Free Antivirus: є одним з найпопулярніших безкоштовних антивірусів, який надає базовий захист від вірусів та шкідливого ПЗ. Він також включає додаткові функції, такі як захист від шахрайства і захист від шпигунського ПЗ.

AVG AntiVirus Free: також є популярним безкоштовним антивірусом, який надає надійний базовий захист та додаткові функції, включаючи файрвол, захист від шахрайства, веб-захист та інше.

Sophos Home: є простим у використанні антивірусом, який надає захист від вірусів, шкідливого ПЗ, шахрайства та інших загроз. Особливістю цього продукту є можливість керування захистом кількох пристроїв з одного онлайн-інтерфейсу.

Malwarebytes: є потужним інструментом для видалення шкідливого ПЗ. Хоча це не є повноцінним антивірусом, воно може бути використане як додатковий шар захисту поряд із традиційним антивірусом.

Ці антивіруси мають різні функції, рівні захисту та ціни, тому користувачам слід вибирати на основі своїх індивідуальних потреб та бюджету.

2.2 Оцінка ефективності різних засобів захисту

Оцінка ефективності різних засобів захисту від шкідливого програмного забезпечення складається з таких аспектів:

Рівень захисту: Як ефективно засіб захисту виявляє та блокує шкідливе програмне забезпечення? Це може бути оцінено за допомогою тестів на виявлення, які проводять незалежні лабораторії, такі як AV-TEST або AV-Comparatives.

Вплив на продуктивність системи: Чи знижує засіб захисту продуктивність комп'ютера або мобільного пристрою? Деякі засоби захисту можуть використовувати

багато системних ресурсів, що може призвести до зниження швидкості роботи системи.

Користувацький інтерфейс та легкість використання: Чи легко встановити та налаштувати засіб захисту? Чи є його інтерфейс зрозумілим та зручним для користувача?

Додаткові функції: Чи пропонує засіб захисту додаткові функції, такі як файрвол, захист від шахрайства, VPN, менеджер паролів тощо?

Ціна: Чи відповідає ціна засобу захисту його якості та набору функцій?

Підтримка користувачів: Чи пропонує виробник якісну підтримку користувачів? Це може включати в себе телефонну підтримку, підтримку через електронну пошту, чат у реальному часі, базу знань, відеоуроки тощо.

Враховуючи ці фактори, можна зробити більш обгрунтований вибір засобу захисту. Однак важливо зазначити, що немає "найкращого" засобу захисту для всіх ситуацій. Різні користувачі можуть мати різні потреби, тому те, що добре працює для одного користувача, може не бути оптимальним для іншого.

Більше того, ефективність засобів захисту може змінюватися з часом, оскільки виробники постійно оновлюють свої продукти, щоб протистояти новим загрозам. Тому важливо регулярно оновлювати своє програмне забезпечення та стежити за останніми оновленнями в області безпеки.

Крім того, важливо пам'ятати, що навіть найкращий засіб захисту не може надати 100% захисту від всіх шкідливих програм. Користувачі повинні також зберігати здоровий глузд та обережність при використанні інтернету, наприклад, не відкривати підозрілі електронні листи або завантажувати програмне забезпечення з ненадійних джерел.

Останнім, але не менш важливим, є те, що захист від шкідливого програмного забезпечення - це лише один аспект загальної стратегії безпеки. До інших важливих елементів можуть належати захист від витоку даних, захист від взлому, фізичний захист обладнання, надійне резервне копіювання даних та ін.

2.3 Порівняльний аналіз захисту від шкідливого програмного забезпечення на різних платформах

Щоб розглянути захист від шкідливого програмного забезпечення на різних платформах, варто розглянути кілька основних : Windows, macOS, Linux, Android та iOS. Кожна з цих платформ має свої особливості, які впливають на їхню схильність до атак і на здатність користувачів захищатися.

Windows: Microsoft Windows - це найпоширеніша операційна система в світі, що робить її основною мішенню для багатьох видів шкідливого програмного забезпечення. Microsoft працює над постійним вдосконаленням своїх засобів захисту. Вбудований антивірусний інструмент, Windows Defender, надає базовий рівень захисту. Однак багато користувачів вибирають додаткові сторонні антивірусні програми для підвищення захисту.

macOS: Ця система від Apple має репутацію більш безпечної системи, порівняно з Windows, через свою Unix-подібну структуру і більш обмежену користувацьку базу. Apple включає в систему macOS інструменти безпеки, такі як Gatekeeper, який перевіряє завантажені програми на наявність шкідливого програмного забезпечення, і XProtect, який надає антивірусний захист на рівні системи. Тим не менш, атаки на macOS зростають, і користувачам рекомендується використовувати додаткове антивірусне ПЗ.

Linux: Хоча Linux не так поширений, як Windows або macOS в ролі основної системи для особистого використання, його часто використовують для серверів та вбудованих систем. Linux відомий своєю високою безпекою, зокрема через модель відкритого вихідного коду, що дозволяє широкому колу розробників виявляти та виправляти уразливості.

Android: Операційна система Android від Google - це найпопулярніша мобільна платформа в світі. Її відкритість та розповсюдженість роблять її привабливою мішенню для шкідливого ПЗ. Google включає в систему Android набір заходів безпеки, включаючи Google Play Protect, який автоматично перевіряє додатки в Google Play Store на наявність шкідливого ПЗ. Однак, користувачі все ще можуть

стикатися з ризиком інфекції, особливо коли вони встановлюють додатки з неофіційних джерел. З цієї причини рекомендується використовувати додаткове антивірусне програмне забезпечення для Android.

iOS: iOS від Apple відрізняється високим рівнем безпеки, наданим строгою контрольованою екосистемою. Всі додатки в App Store проходять строгу перевірку на наявність шкідливого ПЗ перед тим, як стати доступними для користувачів. Крім того, система iOS має ряд вбудованих заходів безпеки, щоб запобігти виконанню шкідливого коду.

Підсумовуючи, можна сказати, що хоча різні платформи вимагають різних підходів до безпеки, основні принципи залишаються такими ж для всіх: користувачі повинні оновлювати свої системи та програми вчасно, використовувати надійне антивірусне програмне забезпечення, а також бути обережними при відкритті незнайомих файлів або посилань.

2.4 Проблеми та виклики в області захисту інформаційних ресурсів

У захисту інформаційних ресурсів в сучасному світі існує не мала кількість проблем. Розглянемо наступні:

Швидкий розвиток технологій: Нові технології, як-то штучний інтелект (AI), хмарні обчислення, Інтернет речей (IoT), блокчейн та інше, відкривають безмежні можливості для розвитку. Але з іншого боку, ці ж технології створюють нові вектори атак та уразливості, з якими слід вміти боротися. Хмарні обчислення, наприклад, можуть посилити ризик порушення безпеки даних, особливо у випадку мультитенантної архітектури. IoT-пристрої часто стають легкою мішенню через погано забезпечені протоколи зв'язку та недостатнє оновлення програмного забезпечення.

Шкідливе програмне забезпечення: Шкідливе ПЗ постійно розвивається та стає все складнішим. Нові види шкідливого ПЗ, такі як програма вимагач або криптоджекінг, з'являються і розвиваються зі швидкістю, що випереджає можливість

захисту від них. Це поставило безпеку даних на перший план і потребує постійного розвитку антивірусних технологій.

Інсайдерські загрози: Ці загрози походять від людей зсередини організації - співробітників, контрактників або партнерів, які мають допуск до системи. Інсайдери можуть навмисно або випадково завдати шкоди, і їх важко виявити, оскільки вони використовують легітимний доступ до системи.

Соціальна інженерія та фішинг: Соціальна інженерія це техніка, яка маніпулює людьми для отримання конфіденційної інформації. Фішинг є популярною формою соціальної інженерії, де атакуючий використовує підроблені електронні повідомлення, щоб викрасти облікові дані користувачів. Незважаючи на всі технологічні заходи безпеки, людський фактор залишається найбільш вразливим елементом в системах безпеки.

Недостатній рівень освіченості у сфері кібербезпеки: Важливо, щоб всі користувачі розуміли основи кібербезпеки, оскільки багато атак використовують прості помилки користувачів. Організації повинні зосередитися на навчанні своїх співробітників впізнавати і уникати потенційних загроз.

Проблеми з приватністю: Сучасні технології дозволяють збирати та аналізувати величезні обсяги даних. З одного боку, це може призвести до значних поліпшень в продуктивності і персоналізації послуг. З іншого боку, це створює величезні ризики для приватності. Без належного захисту, персональні дані можуть бути викрадені або зловживані.

Відстаюче законодавство: Технології розвиваються набагато швидше, ніж законодавство, яке регулює їх використання. Це означає, що багато потенційних уразливостей і проблем з приватністю можуть не бути належним чином регульовані, а тому – не захищені.

Складність управління ідентифікацією та доступом: Ідентифікація та контроль доступу є важливими аспектами інформаційної безпеки. Однак, з ростом кількості користувачів, пристроїв, додатків і сервісів, управління цими елементами стає все складнішим. Крім того, змішані IT-середовища подальше ускладнюють це завдання.

Витоки даних: Витоки даних можуть бути результатом атак або просто випадкових помилок. Вони можуть включати фінансову інформацію, персональні дані, інтелектуальну власність та інше. Витоки даних можуть призвести до значних фінансових втрат, а також до втрати довіри до компанії.

Недостатня координація між сторонами: Інформаційна безпека вимагає координації між різними сторонами, включаючи IT-відділ, керівництво, співробітників та постачальників. Без ефективної координації, можуть виникнути прогалини в безпеці.

Кібервійна: Країни використовують кіберпростір для здійснення шпигунства, кібервійни та інформаційних операцій. Ці дії можуть призвести до значних пошкоджень інфраструктури і їх може бути важко виявити або протистояти.

З усіх вищезазначених причин, захист інформаційних ресурсів є великою проблемою. Важливо, щоб організації розробляли і впроваджували всеоб'ємні стратегії безпеки, що враховують ці виклики та ефективно їм протидіють.

Висновки за розділом 2

Вивчення та аналіз засобів захисту інформаційних ресурсів від шкідливого програмного забезпечення дали нам глибоке розуміння викликів, з якими стикається сфера інформаційної безпеки в сучасному цифровому середовищі.

Шкідливе програмне забезпечення стає все більш розумним і складним, використовуючи нові вектори атак та експлуатуючи уразливості, що з'являються у результаті швидкого технологічного розвитку. Визначення та класифікація шкідливого програмного забезпечення, розробка стратегій та технологій протидії ньому відіграють важливу роль у створенні ефективних систем захисту.

Антивіруси, брандмауери, системи виявлення інтрузій, системи управління доступом і інші компоненти безпеки, включаючи криптографічні інструменти, використовуються для захисту інформаційних ресурсів. Однак, незважаючи на їхню

важливість, вони можуть бути недостатніми, якщо не врахувати людський фактор, оскільки багато кібератак вдаються внаслідок помилок користувачів.

Огляд сучасних антивірусних програм та аналіз ефективності різних засобів захисту виявили, що немає єдиного рішення, яке підходить всім. Ефективність засобів захисту залежить від конкретного середовища, видів потенційних загроз та способів їх використання.

Порівняльний аналіз захисту від шкідливого програмного забезпечення на різних платформах вказує на важливість врахування специфіки платформи при виборі засобів захисту.

Виявлено, що в сучасному світі існує багато проблем та викликів в області захисту інформаційних ресурсів, включаючи недостатнє розуміння користувачами питань кібербезпеки, проблеми з приватністю, відстаюче законодавство, складність управління ідентифікацією та доступом, витоки даних, а також кібервійну.

Всі ці фактори вимагають уваги і постійного розвитку нових підходів до захисту інформаційних ресурсів від шкідливого програмного забезпечення. Дієвий захист передбачає не лише застосування передових технологій, але і розвиток культури кібербезпеки серед користувачів, посилення законодавчої бази, зміцнення міжнародного співробітництва та інтеграція різних засобів захисту в єдину цілісну систему.

Бачимо, що в області захисту від шкідливого програмного забезпечення є великий простір для наукових досліджень та практичних застосувань. У майбутньому слід зосередити увагу на розробці нових стратегій та технологій, спрямованих на попередження шкідливого програмного забезпечення, замість реагування на нього.

Вивчення та аналіз засобів захисту інформаційних ресурсів від шкідливого програмного забезпечення є важливим етапом у створенні ефективних систем інформаційної безпеки, які можуть захистити організації від широкого спектра кіберзагроз.

РОЗДІЛ 3
РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

3.1 Вибір підходів та технологій для розробки системи захисту

Для початку розглянемо засіб автентифікації і авторизації користувачів.

Засіб автентифікації і авторизації користувачів — це інструменти, які використовуються для перевірки ідентифікації користувача та надання відповідних дозволів на доступ до ресурсів.

Автентифікація — це процес визначення ідентичності користувача. Це зазвичай включає введення імені користувача та пароля. Однак існують і більш складні форми автентифікації, такі як двофакторна автентифікація, яка вимагає від користувача подання двох видів доказів їхньої ідентичності, наприклад, щось, що вони знають (пароль), і щось, що вони мають (токен або код, що надіслано на їхній мобільний телефон).

Авторизація — це процес надання дозволів автентифікованому користувачу. Після того, як користувач був успішно автентифікований, система визначає, до яких ресурсів у нього є доступ, і які операції він може виконувати. Наприклад, деякі користувачі можуть мати доступ тільки для читання даних, в той час як іншим дозволено змінювати дані.

Типи систем автентифікації та авторизації включають:

Ідентифікація на основі паролів: Найпоширеніша форма автентифікації, яка вимагає від користувача введення імені користувача та пароля.

Двофакторна автентифікація: Ця форма автентифікації вимагає два види доказів ідентичності, що збільшує рівень безпеки.

Біометрична автентифікація: Використовує унікальні біологічні ознаки, такі як відбитки пальців, сканування сітківки ока або розпізнавання обличчя для

ідентифікації користувача. Ці системи є досить надійними, але також вимагають додаткового обладнання та можуть бути дорогими.

Автентифікація на основі токенів: В цьому випадку користувачу надається токен, наприклад, віртуальний або фізичний ключ безпеки, який генерує унікальний код для використання при вході в систему.

Автентифікація на основі сертифікатів: Використовує цифрові сертифікати, які можуть бути встановлені на комп'ютер користувача. Ці сертифікати містять унікальний ключ, який відповідає публічному ключу на сервері.

Щодо авторизації, основні технології та методики включають:

Access Control Lists (ACLs): Це списки, що визначають, хто або що має дозвіл на доступ до ресурсу.

Role-Based Access Control (RBAC): Замість того, щоб керувати дозволами на рівні окремих користувачів, RBAC працює на основі ролей, які відповідають різним обов'язкам в організації.

Attribute-Based Access Control (ABAC): ABAC, також відомий як політика-керована доступом, використовує ряд атрибутів, включаючи атрибути користувача, атрибути ресурсу, атрибути дій і атрибути оточення, для визначення доступу.

Mandatory Access Control (MAC): MAC - це метод керування доступом, в якому організація встановлює центральну політику безпеки, яка автоматично контролює доступ користувачів до ресурсів.

Federated Identity: Цей підхід дозволяє користувачам використовувати ті ж самі облікові дані для доступу до ресурсів різних мереж і систем, які об'єднані в федерацію. Це полегшує процес автентифікації для користувачів і зменшує кількість паролів, які вони повинні пам'ятати.

Single Sign-On (SSO): SSO дозволяє користувачам використовувати одну пару ім'я користувача/пароль для доступу до всіх своїх систем і програм. Це зручно для користувачів і може покращити безпеку, зменшивши кількість паролів, які вони повинні пам'ятати і які потенційно можуть бути вкрадені.

Privileged Access Management (PAM): PAM допомагає захищати доступ до найважливіших систем і даних організації, контролюючи доступ користувачів із

привілейованими правами (тобто користувачів, які мають можливість змінювати систему або мати доступ до конфіденційних даних).

Identity Governance and Administration (IGA): IGA - це комплексний набір процесів і технологій, що забезпечують управління цифровими ідентичностями та відповідними правами доступу до ресурсів.

Існує набір систем для автентифікації та авторизації користувачів, які включають Fido, Sidway, Google Authenticator і RSA SecurID. Визначаючись з вибором, найефективнішою є RSA SecurID, яка має найкраще співвідношення робочих принципів до якості. Ця система вирізняється наявністю спеціалізованого програмного забезпечення як для серверу, щоб відстежувати активність, так і для особистого комп'ютера, що не характерно для інших. Google Authenticator базується на принципі підключення до Інтернету. Однак, для надання більшої безпеки, потрібно програмне забезпечення, яке може працювати автономно і не потребує постійного підключення до Інтернету.

2) Наступним пунктом системи захисту є антивірусне забезпечення

Антивірус є інструментом, розробленим для забезпечення безпеки інформаційних активів так як у [13]. Це зазвичай є комбінованим програмно-апаратним рішенням, що створює інтегрований комплекс для надійного антивірусного захисту інформаційного контенту в локальній мережі. Повний спектр застосування такого інструменту передбачає організацію управління всіма потоками інформації, що проходять через захищену локальну мережу. Для забезпечення ефективного функціонування системи, що гарантує відмінний захист від негативного впливу вірусів на всі компоненти інфраструктури, потрібна висока ступінь взаємодії між методами та інструментами. Переглядаючи ринок популярних антивірусних продуктів, можна виділити такі відомі бренди, як Avast, Avira, ESET, AVG, Comodo, Symantec та інші. Надамо порівняльну статистику на рис.3.1 та рис.3.2.

Рисунок 3.1 - Кількість користувачів

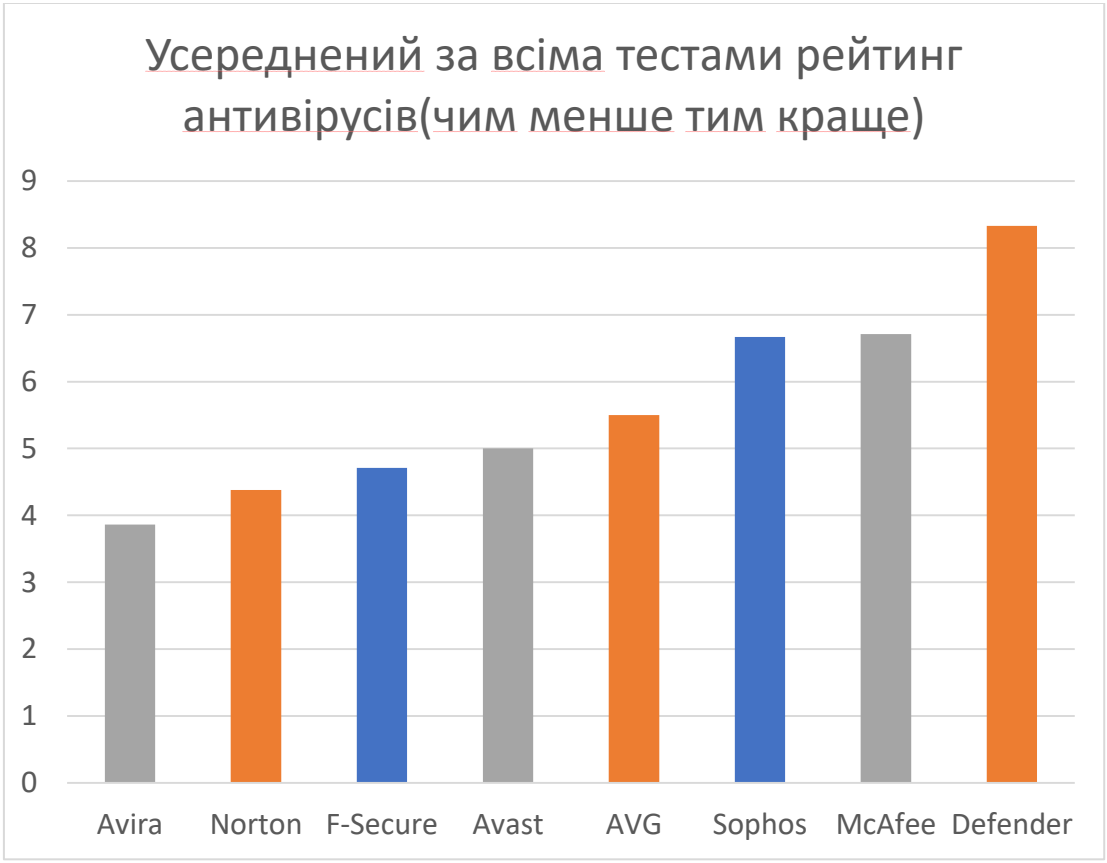

Рисунок 3.2 - Порівняльна статистика

Після проведення аналізу, Avast виявився найкращим варіантом за рахунок простого керування робочими станціями в антивірусній мережі через механізм

групування, швидкого та ефективного розповсюдження оновлень бази даних вірусів. Додаткові переваги включають зменшення мережевого трафіку локальних мереж, побудованих на протоколах TCP / IP, IPX, завдяки використанню спеціальних алгоритмів стиснення, ізолювання інфікованих об'єктів у карантин замість негайного видалення, можливість вибрати тип об'єктів для сканування. Аналіз тестування показав, що Avast є найкращим вибором як антивірусного засобу для системи захисту.

3) Міжмережевий екран — це спеціальний засіб, що використовується для контролю і обмеження вхідного та вихідного мережевого трафіку. Він базується на попередньо визначених правилах безпеки і служить як перший рівень захисту в інформаційних системах. Його основна мета — відокремити надійну мережу від ненадійних мереж, таких як Інтернет.

Сучасні міжмережеві екрани можуть бути апаратними, програмними або поєднанням обох типів.

Апаратний міжмережевий екран — це фізичний пристрій, що з'єднує мережу з Інтернетом і забезпечує контроль трафіку між двома точками через застосування набору правил фільтрації. Вони часто використовуються в корпоративних мережах для захисту внутрішньої інфраструктури від зовнішніх загроз.

Програмний міжмережевий екран встановлюється на комп'ютері та контролює весь вхідний та вихідний трафік цього комп'ютера. Вони дозволяють забезпечити більш детальний контроль трафіку, ніж апаратні екрани, оскільки вони можуть визначати, які програми можуть надсилати і приймати дані.

Міжмережеві екрани можуть працювати на різних рівнях моделі OSI, використовуючи різні методи фільтрації:

Фільтрація пакетів: Фільтрація на рівні мережі, базується на параметрах, таких як IP-адреси, порти та протоколи.

Фільтрація на рівні застосувань: Фільтрація на рівні додатків, що використовує більш високий рівень контролю, аналізуючи деталі конкретних додатків, які надходять через міжмережевий екран. Вона впроваджує глибокий аналіз пакетів для визначення того, чи допускається трафік, який входить або виходить, на основі детального перегляду даних застосунків.

Цей тип фільтрації дозволяє системі безпеки краще розуміти, що відбувається на рівні застосування. Наприклад, хоча протокол HTTP може бути допустимим, фільтрація на рівні застосувань може блокувати конкретні HTTP-запити або відповіді, які містять потенційно шкідливий вміст.

Веб-фільтрація: Фільтрація веб-контенту, що проходить через міжмережевий екран, яка може включати в себе блокування конкретних веб-сайтів або різних типів веб-сайтів.

Перевірка стану сеансу (Stateful inspection): Це підхід до фільтрації, який не просто перевіряє властивості пакетів, а й враховує контекст сеансу. Такий підхід включає в себе перевірку стану та інформації, пов'язаної з кожною активною сеансовою з'єднаністю.

Проксі-сервери: Вони діють як посередники між двома кінцевими точками, перевіряючи всю вхідну та вихідну інформацію. Коли ви відправляєте запит до інтернет-ресурсу, проксі-сервер спочатку обробляє ваш запит, а потім передає його до вказаного сервера. Відповідь сервера потім проходить через проксі-сервер, перш ніж повертатися до вас

Міжмережеві екрани відіграють важливу роль в системі захисту інформації, вони не тільки забезпечують контроль трафіку, але і можуть відслідковувати спроби вторгнення та забезпечувати захист від певних видів атак. Однак вони повинні використовуватись разом з іншими засобами захисту, такими як антивірусні програми, системи виявлення вторгнень (IDS) та системи захисту від вторгнень (IPS), адже міжмережеві екрани не здатні виявляти або блокувати всі типи загроз.

Розглянуто та порівняно одні з найвідоміших апаратних міжмережевих екранів які є на ринку у таблиці 3.1.

Такі як Cisco ASA 5515-X, Juniper SRX 220 та Checkpoint 421. При порівнянні звернули увагу на такі характеристики як: Пропускна здатність, VPN підтримка, кількість портів, фаєрвол, наявність IDS/IPS, SSL інспекція та масштабованість

Таблиця 3.1

Порівняння мережевих екранів

Модель екрану	Cisco ASA 5515-X	Juniper SRX 220	Checkpoint 4210
Пропускна здатність	1 Гбіт/с	950 Мбіт/с	2.5 Гбіт/с
VPN підтримка	Так	Так	Так
Кількість портів	6 портів	8 портів	8 портів
Фаєрвол	Так	Так	Так
IDS/IPS	Так	Так	Так
SSL інспекція	Так	Так	Так
Масштабованість	Середня	Висока	Висока

Отже серед наведених варіантів, найкращим вибором є Checkpoint 4210. Він має найвищу пропускну здатність, 8 портів Ethernet та ні в чому не програє своїм конкурентам.

4) Засоби криптографічного захисту інформації є ключовими компонентами в системі інформаційної безпеки. Їх головне призначення - забезпечити конфіденційність, цілісність, автентичність даних.

Шифрування: Шифрування перетворює зрозумілу інформацію в незрозумілу форму за допомогою криптографічного ключа. Є два основні типи шифрування: симетричне і асиметричне. Симетричне шифрування використовує один і той самий ключ для шифрування та розшифрування даних, тоді як асиметричне шифрування використовує різні ключі: приватний для розшифрування та публічний для шифрування.

Цифровий підпис: це технологія, яка підтверджує автентичність та цілісність даних. Він гарантує, що дані не були змінені під час трансляції, і підтверджує ідентичність відправника.

Хеш-функції: Хеш-функції використовуються для перетворення даних в унікальний хеш-код, який служить "цифровим відбитком" даних. Якщо дані змінюються, хеш-код також змінюється, що свідчить про те, що дані були змінені.

Протоколи безпеки: Протоколи безпеки, такі як SSL (Secure Sockets Layer) та TLS (Transport Layer Security), використовують криптографічні методи для забезпечення безпеки комунікації між двома кінцевими точками.

Безпека електронної пошти: S/MIME (Secure/Multipurpose Internet Mail Extensions) та PGP (Pretty Good Privacy) - це два стандарти для забезпечення конфіденційності.

Криптографічне зберігання даних: Для зберігання даних в зашифрованому вигляді можна використовувати різні технології, включаючи дискове шифрування - це технологія шифрування, яка конвертує всю інформацію, збережену на диску, в зашифровану форму.

Системи управління ключами: це важливий аспект криптографії. Вони включають в себе генерування, зберігання, розподіл, використання, оновлення та знищення ключів.

Криптографія з відкритим ключем: використовує пару ключів - публічний і приватний - для шифрування і розшифрування даних. Публічний ключ відкритий для всіх, але приватний ключ зберігається в таємниці.

Квантова криптографія: Це новий підхід до криптографії, який використовує закони квантової механіки для створення абсолютно незламного коду.

Серед програм для криптографічного захисту інформації можна виділити BestCrypt Volume Encryption, Windows BitLocker та Knox. Відмінність Windows BitLocker від інших полягає в тому, що вона не підтримує шифрування динамічних дисків.. Що стосується Knox, то вона розроблена спеціально для Mac OS і несумісна з Windows. Таким чином, найбільш вдалим вибором є BestCrypt Volume Encryption.

5) Засоби фізичного захисту інформаційних ресурсів – це засоби, призначені для відвертання безпосередніх фізичних загроз до інфраструктури, що зберігає та обробляє дані. Вони важливі, оскільки навіть найбільш суворі мережеві та програмні заходи безпеки можуть стати недієвими, якщо зловмисник має безпосередній

фізичний доступ до обладнання. Нижче наведено деякі основні засоби фізичного захисту:

Контроль доступу: Закриті двері, ключові картки, біометричні сканери, охорона – всі ці засоби використовуються для обмеження доступу до об'єктів, де знаходяться важливі IT-ресурси.

Відеоспостереження: Відеокамери та системи запису відео можуть слідкувати за тим, хто має доступ до приміщень та їх діями всередині.

Захист від пожежі та води: Спеціальні вогнегасники, водонепроникні заходи, а також системи виявлення пожежі та витоку води можуть захистити обладнання від пошкоджень.

Замки на серверних шафах: Це ще один рівень захисту, що перешкоджає несанкціонованому доступу до серверів та іншого обладнання.

Управління живленням: Захист від перебоїв у живленні та захист від перенапруги є важливими для забезпечення стабільності роботи обладнання.

Клімат-контроль: Правильне охолодження та вологість критично важливі для збереження серверів та іншого IT-обладнання в робочому стані.

Розглянемо та порівняємо засоби біометричної ідентифікації які можемо використати при побудові системи захисту у таблиці 3.2.

Сканери відбитку пальця:

VeriFinger Portable: Це сканер відбитків пальців високої роздільної здатності, який можна використовувати для застосунків, які вимагають високої рівня безпеки.

DigitalPersona U.are.U: Це портативний сканер відбитків пальців, який працює з різними операційними системами, включаючи Windows і macOS.

Сканер обличчя:

FaceStation 2: Цей портативний пристрій використовує технологію розпізнавання обличчя для ідентифікації особи.

Сканер райдужної оболонки:

IrisAccess iCAM 7S: Цей пристрій використовує технологію розпізнавання райдужної оболонки для ідентифікації особи.

Таблиця 3.2

Порівняння фізичних методів захисту

Модель сканера	Біометричний метод ідентифікації	Інтерфейс підключення	Підтримка платформ	Розмір	Особливі функції
VeriFinger Portable	Відбиток пальця	USB	Windows, Android	Портативний	Автономний режим роботи, висока точність
FaceStation 2	Розпізнавання обличчя	TCP/IP, RS485	Windows, Android	Середній	Технологія Anti-Spoofing, широкий кут огляду
IrisAccess iCAM 7S	Розпізнавання райдужної оболонки	USB	Windows, Linux	Портативний	Висока швидкість зчитування, висока точність
DigitalPersona U.are.U	Відбиток пальця	USB	Windows, Linux, Mac OS	Портативний	Висока швидкість зчитування

Для системи захисту обрано DigitalPersona U.are.U.

6) Резервне копіювання є важливим елементом стратегії захисту інформаційних ресурсів. Воно дозволяє зберегти копії даних і відновити їх у випадку втрати або пошкодження.

Засоби резервного копіювання можуть бути апаратними або програмними:

Апаратні засоби резервного копіювання: це фізичні пристрої, які використовуються для збереження даних. Вони включають зовнішні жорсткі диски, мережеві сховища (NAS), та стрічкові приводи. Вони забезпечують високу місткість та надійність, але вони можуть бути вразливими до фізичних пошкоджень та зносу.

Програмні засоби резервного копіювання: це програми, які використовуються для створення копій даних та їх збереження на різних носіях. Вони можуть використовувати різні стратегії резервного копіювання, такі як повне резервне копіювання, диференціальне або інкрементне резервне копіювання. Популярні програмні засоби включають Acronis True Image, Veeam Backup, Norton Ghost та інші.

Хмарні сервіси резервного копіювання:

Google Drive: Безкоштовний сервіс від Google, який дозволяє зберігати файлі та папки в інтернеті.

Dropbox: Це комерційний сервіс, який дозволяє зберігати файлі та папки в інтернеті і має багато додаткових можливостей.

Microsoft OneDrive: Це сервіс від Microsoft, який інтегрований з Windows 10 і Office 365.

Apple iCloud: Це хмарний сервіс від Apple, що інтегрований з iOS і macOS.

Незалежно від вибору засобу, важливо врахувати такі фактори, як частота резервного копіювання, ємність зберігання, швидкість відновлення даних та безпека даних під час зберігання та передачі. Для додаткового захисту, рекомендується зберігати резервні копії на різних місцях або використовувати послуги хмарного зберігання. Порівняємо програмні засоби у таблиці 3.3.

Таблиця 3.3

Порівняння засобів резервного копіювання

Програма	Acronis True Image	Veeam Backup	Norton Ghost
Операційна система	Windows, Mac, Linux	Windows	Windows
Тип резервного копіювання	Повне, інкрементне, диференційне	Повне, інкрементне	Повне, інкрементне
Зберігання у хмарі	Так	Так	Ні

Відновлення на рівні файлів та образів	Так	Так	Так
Відновлення на різних апаратних конфігураціях	Так	Так	Ні
Планування резервного копіювання	Так	Так	Так

Доцільно буде використовувати Acronis True Image, це популярний інструмент для резервного копіювання, яке надає повне рішення для резервного копіювання та відновлення даних для індивідуальних користувачів і малого бізнесу. Він пропонує широкий спектр функцій, які покривають потреби в резервному копіюванні, включаючи резервне копіювання на місцевому рівні та в хмарі, а також відновлення системи.

3.2 Розробка архітектури системи захисту інформаційних ресурсів

1) При розгляді антивірусного забезпечення вибір ліг на Avast Antivirus.

• Для початку потрібно скачати та встановити його. Avast є популярним антивірусним програмним забезпеченням, який пропонує багато різних налаштувань для задовільнення ваших потреб. Ось основні кроки для налаштування Avast:

• Після встановлення Avast, можете відкрити його, двічі натиснувши на іконку Avast на робочому столі або в меню "Пуск".

• Оновлення бази даних вірусів: Оновіть базу даних вірусів, натиснувши на кнопку "Оновити" в головному вікні Avast. Це забезпечить, що ваша програма Avast може виявляти останні загрози (рис.3.3).

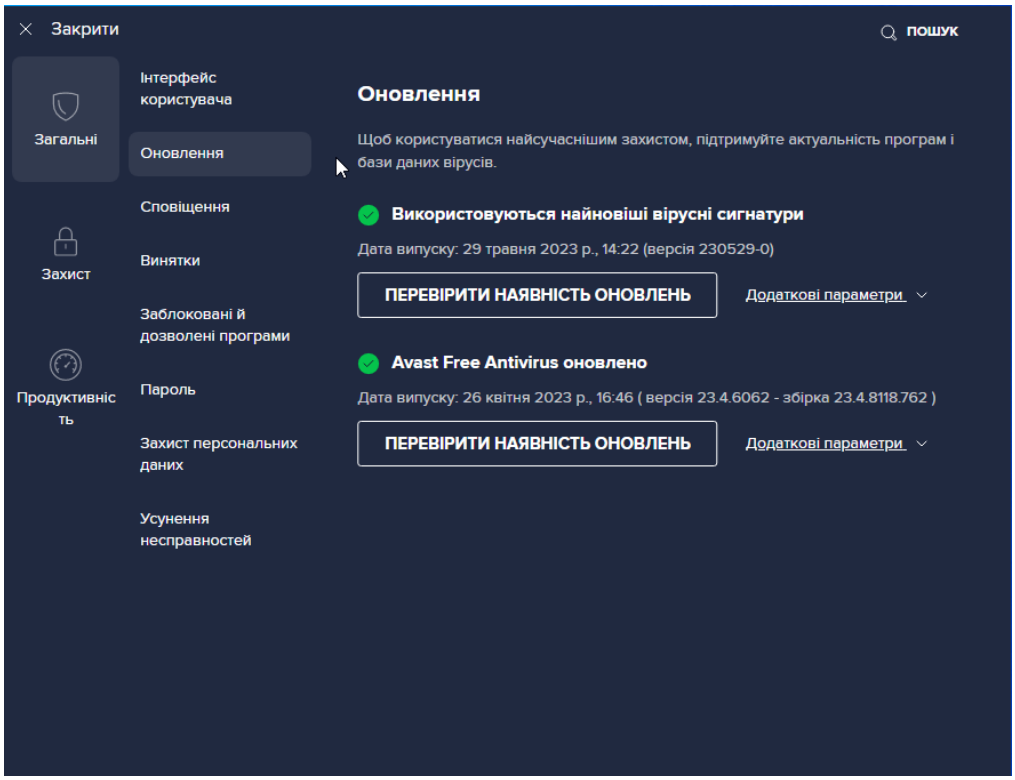

Рисунок 3.3 - Оновлення бази даних вірусів

• Налаштування захисту: Avast включає кілька заходів, які захищають вас від різних типів загроз. Можна вибрати, які заходи увімкнені, натиснувши на вкладку "Захист" в меню налаштувань. Зазвичай рекомендується увімкнути всі, але це може сповільнити систему .

• Налаштування планування сканування: є можлтвість налаштувати автоматичне сканування на конкретний час або день. Це можна зробити в меню "Планувальник сканування".

• Налаштування сповіщень: Avast може відправляти вам повідомлення, коли виявляє загрози або потребує оновлення. Можна налаштувати ці повідомлення в меню "Сповіщення" в налаштуваннях Avast.

• Налаштування захисту від шкідливих сайтів: Avast може блокувати шкідливі веб-сайти. Налаштовуємо цю функцію в меню "Захист від шкідливих сайтів" .

• Оновлення програми: Регулярно перевіряйте наявність оновлень для програми Avast. Це забезпечить, що у вас є останні засоби захисту від загроз. Щоб перевірити наявність оновлень, перейдіть до налаштувань програми і виберіть "Оновлення".

• Керування винятками: додавайте конкретні файли, папки або веб-сайти до списку винятків Avast, якщо ви впевнені, що вони безпечні. Це можна зробити в меню "Винятки".

• Налаштування приватності: В Avast є налаштування, які дозволяють контролювати, як програма збирає та використовує ваші дані. Ви можете переглянути ці налаштування в меню "Захист персональних даних".

• Використання додаткових інструментів: Avast пропонує ряд додаткових інструментів, таких як VPN для анонімного веб-серфінгу, засоби очищення для видалення небажаних файлів та інструменти оптимізації для прискорення роботи вашого комп'ютера. Ці інструменти можна увімкнути та налаштувати в меню "Додатково".

2)Використано міжмережевий екран Checkpoint 4210

Виконайте початкове налаштування пристрою Check Point 4210 за допомогою майстра першого налаштування так як у [29]

Щоб запустити майстер першої конфігурації:

1. Підключіть стандартний мережевий кабель до інтерфейсу керування пристроєм і до мережі керування. Інтерфейс керування має позначку MGMT. Для цього інтерфейсу попередньо налаштовано IP-адресу 192.168.1.1.

2. Підключіться до інтерфейсу керування, підключившись з комп’ютера в тій самій підмережі, що й інтерфейс керування (наприклад, з IP-адресою 192.168.1.x і маскою мережі 255.255.255.0). Це можна змінити пізніше через WebUI.

3. Щоб отримати доступ до інтерфейсу адміністрування, ініціюйте підключення з браузера до IP-адреси адміністрування за замовчуванням: https://192.168.1.1.

4. Увійдіть у систему, використовуючи ім’я користувача/пароль за замовчуванням: admin/admin, і натисніть «Увійти».

5. Змініть пароль адміністратора. Стандартний пароль надає вам доступ до пристрою. З міркувань безпеки ви повинні змінити його на більш безпечний пароль. У розділі «Маркер входу для відновлення пароля» можна завантажити маркер входу, який можна використовувати, якщо ви забудете пароль. Рекомендується зберегти та безпечно зберігати файл маркерів входу для відновлення пароля.

6.Майстер першої конфігурації представляє вікна, які допоможуть вам налаштувати пристрій.

• Налаштуйте дату й час на сторінці налаштування дати й часу. Натисніть Застосувати.

• Мережеві підключення: Налаштуйте мережеві підключення на сторінці «Мережеві підключення» (рис3.4)

• Щоб змінити IP-адресу керування, і підключення збережеться. Додатковий інтерфейс створюється автоматично для збереження з’єднання. Цей інтерфейс можна видалити після завершення роботи майстра на сторінці «Мережа > Мережеві підключення» після завершення роботи майстра.

• Налаштуйте параметри маршрутизації на сторінці «Таблиця маршрутизації».

Рисунок 3.4 - Мережеві підключення

• Налаштуйте хост, домен і DNS-сервери на сторінці хоста, параметрів домену та DNS-серверів. Ім’я хоста має починатися з літери і не може мати назву com1, com2....com9. У розділі DNS встановіть DNS-сервери для пристрою.

• Налаштовуємо спосіб керування пристроєм на сторінці типу керування. Розгортання з локальним керуванням: пристрій є шлюзом безпеки та сервером керування безпекою. Сервер керування безпекою керує політикою безпеки, яка виконується шлюзом безпеки.

• Розгортання з централізованим керуванням: пристрій є шлюзом безпеки без сервера керування безпекою. Шлюзом безпеки керує віддалений сервер керування безпекою.

• Визначаємо клієнтів, яким дозволено підключатися до пристрою за допомогою веб-браузера або клієнта SSH. Ці клієнти можуть керувати пристроєм за допомогою веб-з’єднання або підключення SSH. Ви можете визначити хост відповідно до імені хоста або IP-адреси. Введіть розділений комами список IP-адрес, з яких ви керуєте пристроєм. Після того, як ви завершите роботу майстра першого налаштування, у меню WebUI доступні додаткові параметри.

Для налаштування політики безпеки потрібно встановити програми SmartConsole.

Налаштовуємо тип шлюзу для пристрою з централізованим керуванням. Виберіть один із:

• Стандартний шлюз

• Шлюз є членом кластера

• Шлюз використовує динамічно призначену IP-адресу

Визнаємо клієнтів, яким дозволено підключатися до пристрою за допомогою веб-браузера або клієнта SSH. Ці клієнти можуть керувати пристроєм за допомогою веб-з’єднання або підключення SSH. Ви можете визначити хост відповідно до імені хоста або IP-адреси. Введіть розділений комами список IP-адрес, з яких ви керуєте пристроєм.

Процедура налаштування Windows Firewall:

Для початку треба зайти у панель керування (рис.3.5) та з усіх параметрів, що доступні, потрібно вибрати "Брандмауер захисника Windows" (рис.3.6). Вбудований механізм безпеки брандмауера Windows активно збирає IP-адреси та пов'язані з підключеннями дані, які виникають в домашніх та корпоративних мережах, а також під час використання Інтернету. Це дозволяє реєструвати як успішні підключення, так і втрачені пакети. Отже, ви зможете відслідковувати моменти підключення комп'ютера в мережі, наприклад, до конкретного веб-сайту.

Windows Firewall дозволяє встановлювати специфічні правила для кожної програми на вашому комп'ютері. Наприклад, ви можете дозволити або заборонити певній програмі доступ до інтернету. Також має здатність блокувати весь вхідний трафік. Це може бути корисно, якщо ви хочете тимчасово захистити свій комп'ютер від можливих загроз з інтернету.

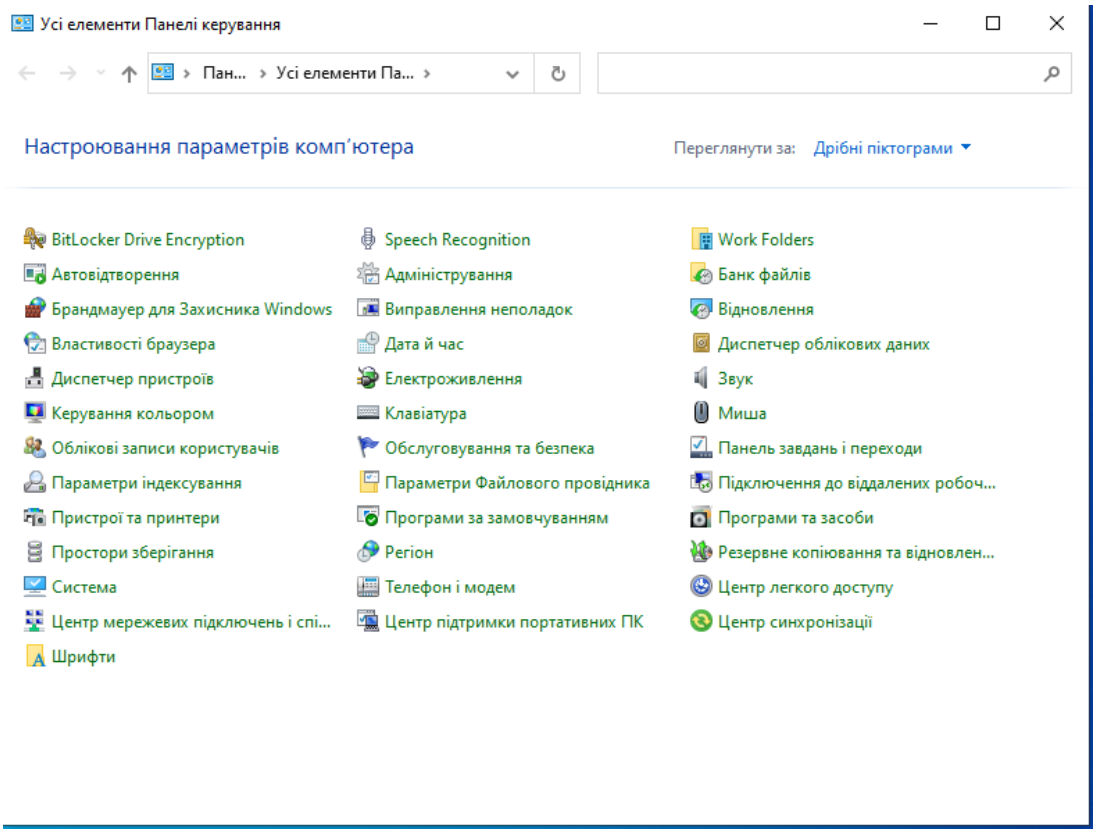

Рисунок 3.5 - Панель керування

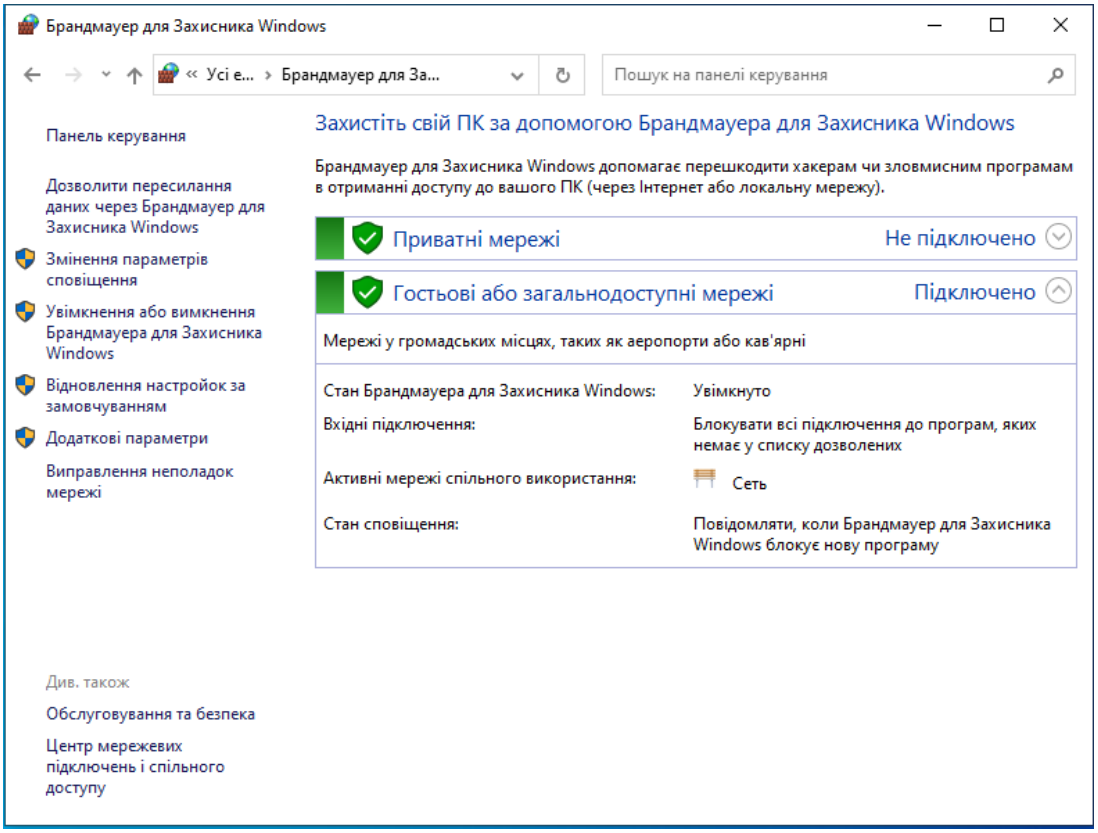

Рисунок 3.6 - Брандмауер Windows

Переходимо до меню «Додаткові параметри» (Рис.3.7).Тут бачимо поточний стан захисника та його налаштування.

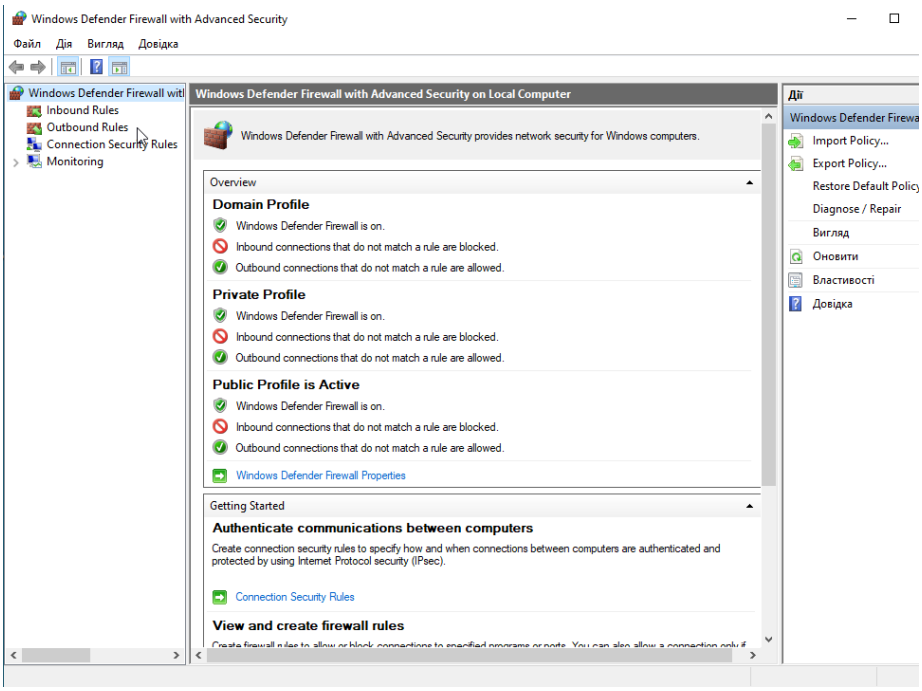

Рисунок 3.7 - Додаткові параметри

Щоб створити блокування певних програм, потрібно скористатися стовпцем "Правила для вихідних з'єднань", де слід обрати "Створити правило" (рис.3.8).

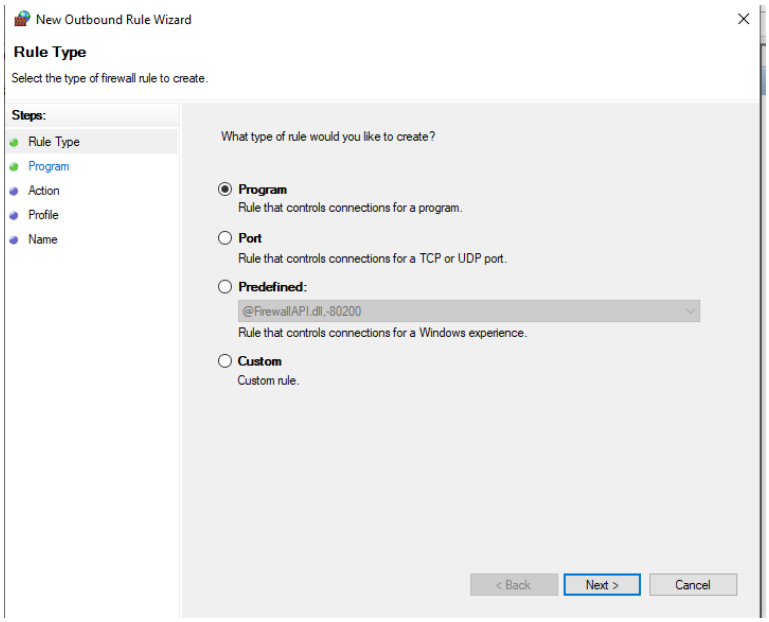

Рисунок 3.8 Створити правило

Спробуємо виконати блокування вихідних з’єднань для програми Microsoft Edge. Для цього потрібно вказати шлях до програми (рис.3.9).

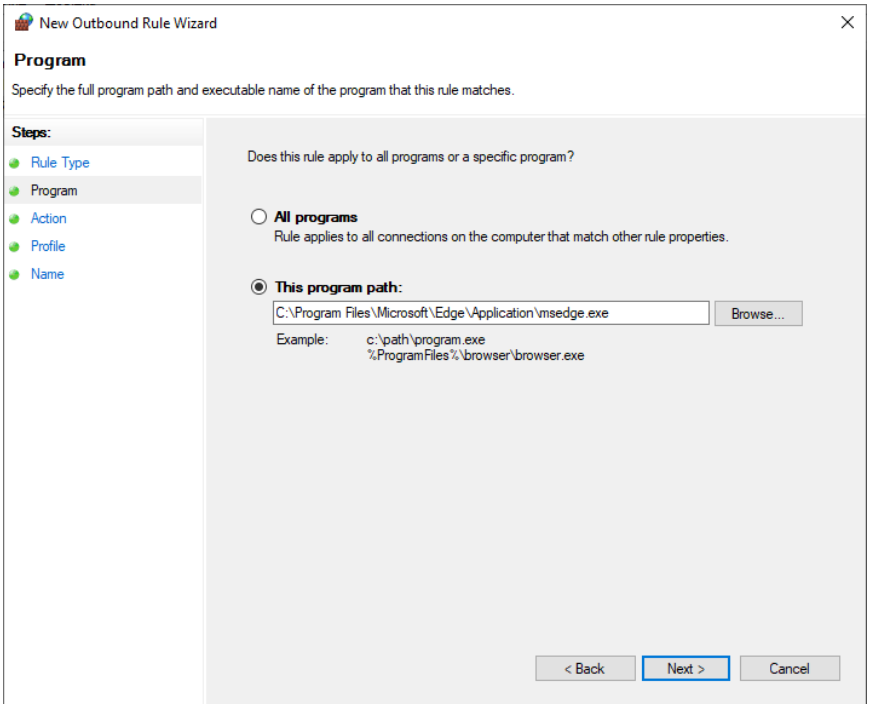

Рисунок 3.9 - Блокування вихідних з’єднань

Далі обрати «Блокувати підключення» (рис.3.10).

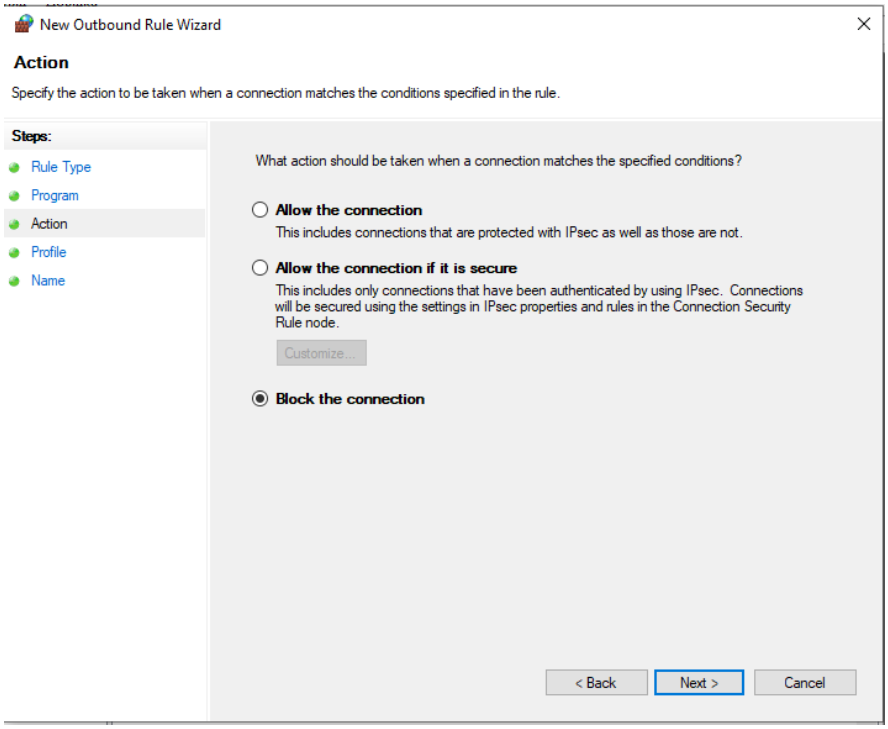

Рисунок 3.10 - Блокування підключення

Обрати профілі до яких застосовується правило (рис.3.11)

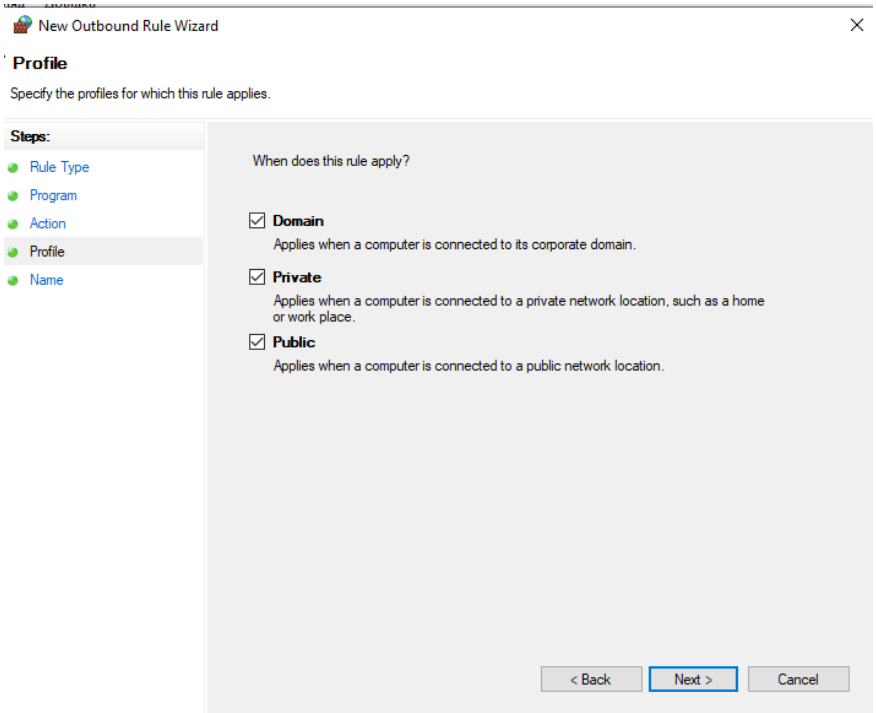

Рисунок 3.11 - Профілі

Та ввести ім’я правила (рис.3.12)

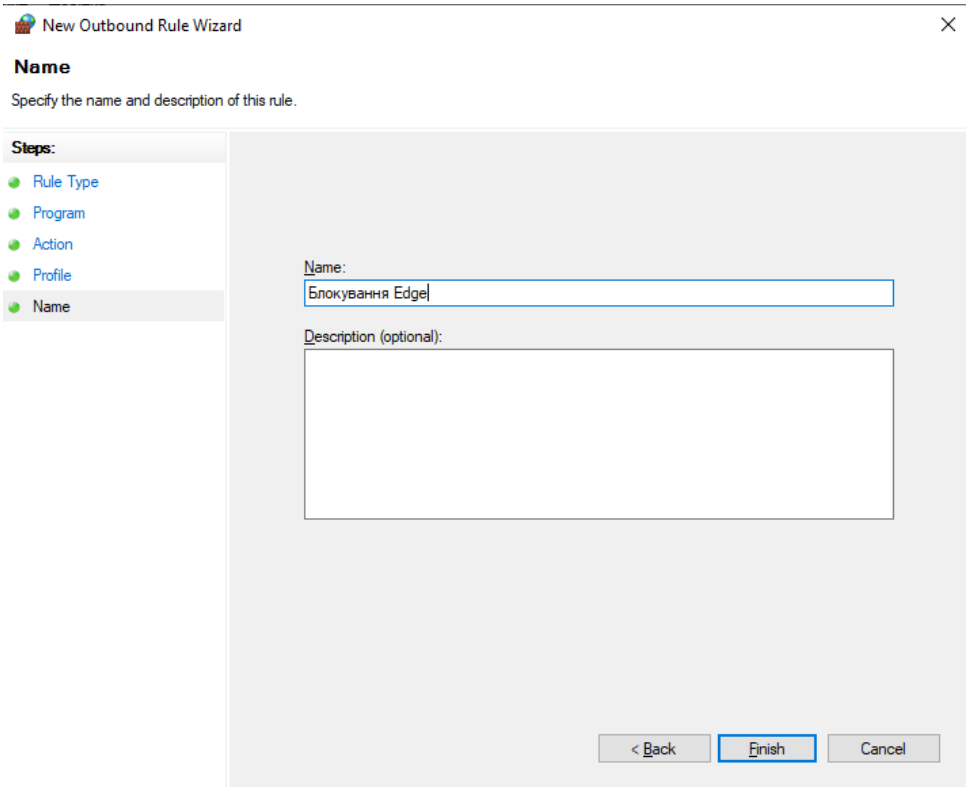

Рисунок 3.12 - Ім’я правила

Після виконаних дій, всі вихідні підключення для даної програми будуть блокуватися.

3) Засоби криптографічного захисту інформації

Для системи захисту обрано програмне забезпечення BestCrypt Volume Encryption.

BestCrypt Volume Encryption - це програмне забезпечення від компанії Jetico, що використовується для шифрування всіх даних для всіх видів дискових томів - фіксованих, з’ємних та оптичних. З шифруванням відразу на весь диск, а не окремі файли або теки, BestCrypt Volume Encryption забезпечує захист від несанкціонованого доступу до всієї інформації, яка зберігається на диску.

Основні характеристики BestCrypt Volume Encryption включають:

• Шифрування на рівні тому (диска): Шифрує всі види томів, включаючи системні томи з операційною системою, диски з розкладками, та своп-файли.

• Шифрування з’ємних дисків: Включає USB-флешки, карти пам'яті та зовнішні HDD/SSD.

• Підтримка різних алгоритмів шифрування: Програма підтримує декілька сильних алгоритмів шифрування, включаючи AES (Rijndael), Serpent, Twofish, Blowfish, CAST и GOST 28147-89.

• Висока безпека: Шифрування відбувається на низькому рівні, що забезпечує високу безпеку, незалежно від типу файлової системи.

• Автоматичне шифрування: Коли ви вставляєте з’ємний носій даних, програма може автоматично шифрувати його без будь-якої додаткової дії з вашого боку.

• Гнучкі налаштування і зручний інтерфейс: Ви можете вибирати між кількома режимами шифрування, а також визначати свої налаштування для кожного диску окремо.

• Захист від "холодного старту": BestCrypt Volume Encryption захищає ключі від атак типу "холодний старт", використовуючи спеціальні алгоритми що забезпечують безпечне зберігання ключів шифрування в пам'яті комп'ютера.

• Підтримка шифрування UEFI: BestCrypt Volume Encryption підтримує шифрування томів, використовуючи загрузку UEFI для більшої сумісності з сучасними системами.

• Шифрування без перезавантаження системи: Дозволяє шифрувати томи без потреби перезавантажувати систему.

• Захист від зміни паролю: BestCrypt Volume Encryption захищає від несанкціонованої зміни паролю, вимагаючи попередній пароль перед встановленням нового.

• Підтримка великих дисків: Підтримує шифрування дисків обсягом до 128 ТБ.

Усі ці особливості роблять BestCrypt Volume Encryption потужним та гнучким інструментом для захисту даних на рівні диска. Це є особливо важливим для організацій, що повинні захищати конфіденційну інформацію та відповідати вимогам щодо захисту даних

Встановлення і налаштування BestCrypt Volume Encryption включає декілька кроків:

• Встановлення: Завантажте BestCrypt Volume Encryption з офіційного сайту і встановіть його на ваш комп'ютер. Слідуйте інструкціям, що з'являються під час процесу встановлення.

• Вибір томів для шифрування: Після встановлення програми, запустіть BestCrypt Volume Encryption і перейдіть до вкладки "Томи". Тут ви зможете вибрати диски або томи, які ви хочете зашифрувати (рис.3.13).

• Встановлення паролю: Після вибору диску або тому для шифрування, виберіть "Шифрувати том". Вам буде запропоновано ввести пароль. Оберіть надійний пароль, який складно буде зламати.

• Вибір алгоритму шифрування: Ви зможете вибрати алгоритм шифрування, який ви хочете використовувати. BestCrypt Volume Encryption підтримує декілька алгоритмів, включаючи AES, Serpent, Twofish і інші. Виберіть той, який найкраще відповідає вашим потребам.

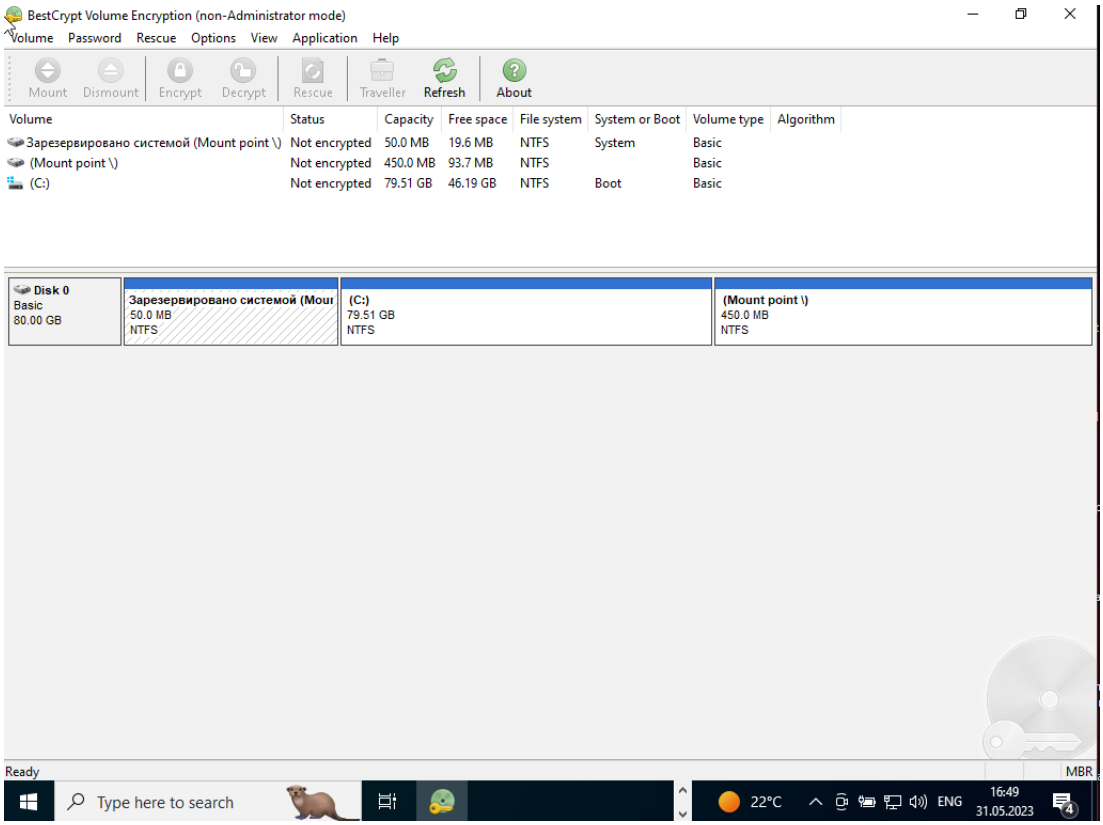

Рисунок 3.13 - Вибір томів

• Завершення процесу шифрування: Після вибору алгоритму і встановлення паролю, програма почне процес шифрування. Це може зайняти деякий час в залежності від обсягу диску.

• Управління зашифрованими дисками: Після завершення процесу шифрування, ви зможете керувати своїми зашифрованими дисками через інтерфейс. Ви можете змінити паролі, додати або видалити зашифровані томи і так далі.

4) Для фізичного захисту обраноми DigitalPersona U.are.U (рис.3.14) — це ряд портативних біометричних сканерів відбитків пальців, що виробляються компанією Crossmatch, що спеціалізується на біометричних рішеннях. Ці сканери відбитків пальців використовуються для управління доступом, автентифікації, цифрового підпису та інших застосувань, де необхідна біометрична перевірка.

Налаштування сканера DigitalPersona U.are.U включає наступні кроки:

Встановлення: Приєднайте сканер U.are.U до вашого комп'ютера за допомогою USB-порту. Ваша операційна система має визначити новий пристрій і автоматично встановити потрібні драйвери. Якщо драйвери не встановлюються автоматично, ви можете завантажити їх з офіційного сайту Crossmatch і встановити вручну.

Налаштування програмного забезпечення: Щоб скористатися всіма перевагами біометричного сканера, вам також потрібно встановити спеціальне програмне забезпечення. Це може бути програмне забезпечення DigitalPersona Pro або інше програмне забезпечення, що підтримує пристрої U.are.U.

Реєстрація відбитків пальців: Після встановлення програмного забезпечення вам потрібно буде зареєструвати свої відбитки пальців. Програмне забезпечення має надати вам інструкції для реєстрації відбитків.

Використання сканера: Після реєстрації відбитків пальців ви зможете використовувати сканер для автентифікації в програмах і сервісах, що підтримують біометричну автентифікацію.

Рисунок 3.14 - Сканер відбитків пальця

5)Засобом резервного відновлення обрано Acronis True Image — це програмне забезпечення для резервного копіювання, створене компанією Acronis. Воно дозволяє користувачам створювати повні копії даних включаючи операційну систему, програми, налаштування, файли тощо і зберігати ці копії на зовнішніх носіях або у хмарному сховищі Acronis.

Встановлення: Спершу вам потрібно завантажити та встановити програму з офіційного сайту Acronis. Під час встановлення слідуйте вказівкам, що відображаються на екрані.

Налаштування резервного копіювання: Після встановлення і запуску програми перейдіть до розділу "Резервне копіювання". Тут ви можете вибрати, які дані ви хочете копіювати (весь комп'ютер, окремі папки та файли тощо), а також куди ви хочете зберігати резервну копію (на зовнішньому пристрої зберігання даних або у хмарному сховищі).

Налаштування графіка резервного копіювання: Acronis True Image дає вам можливість налаштувати автоматичне резервне копіювання за графіком. Ви можете

встановити щоденні, тижневі або місячні резервні копії, щоб впевнитися, що ваші дані завжди захищені.

Відновлення даних: У випадку втрати даних ви можете легко відновити їх із резервної копії. Просто перейдіть до розділу "Відновлення", виберіть потрібну резервну копію і слідуйте вказівкам на екрані

Спробуємо створити резервну копію диску. Для цього спочатку потрібно обрати місце зберігання резервної копії, це може бути місце на хмарі, зовнішній диск або місце на комп’ютері (рис.3.15).

Обрано папку на комп’ютері та розпочато резервне копіювання (рис3.16). Після закінчення створення копії отримаємо відповідне повідомлення (рис.3.17).

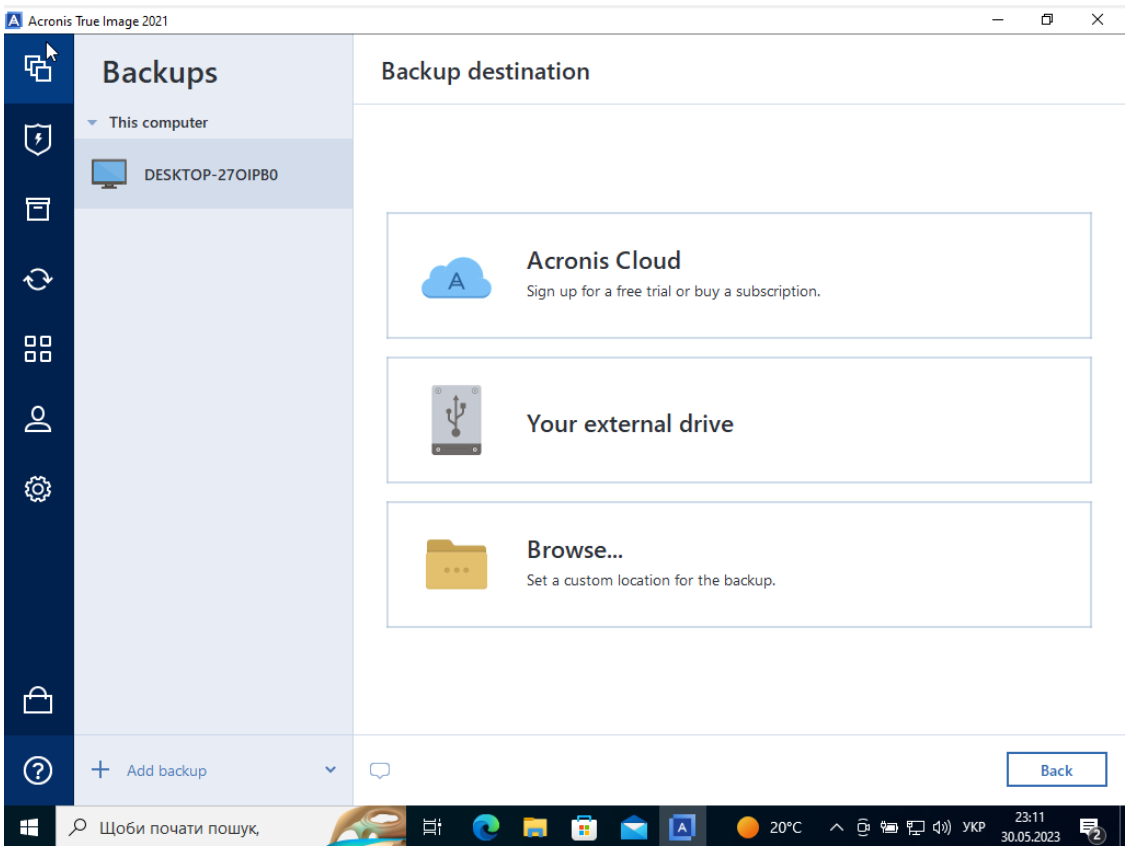

Рисунок 3.15 - Вибір місця

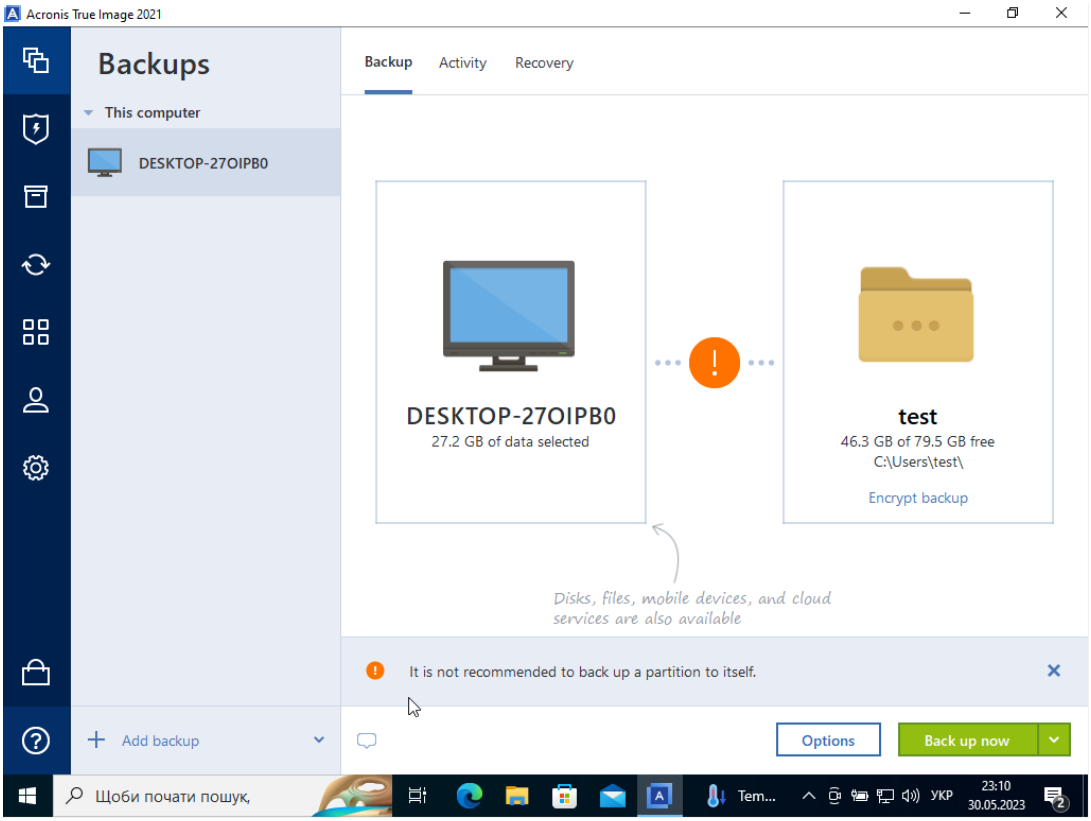

Рисунок 3.16 - Початок копіювання

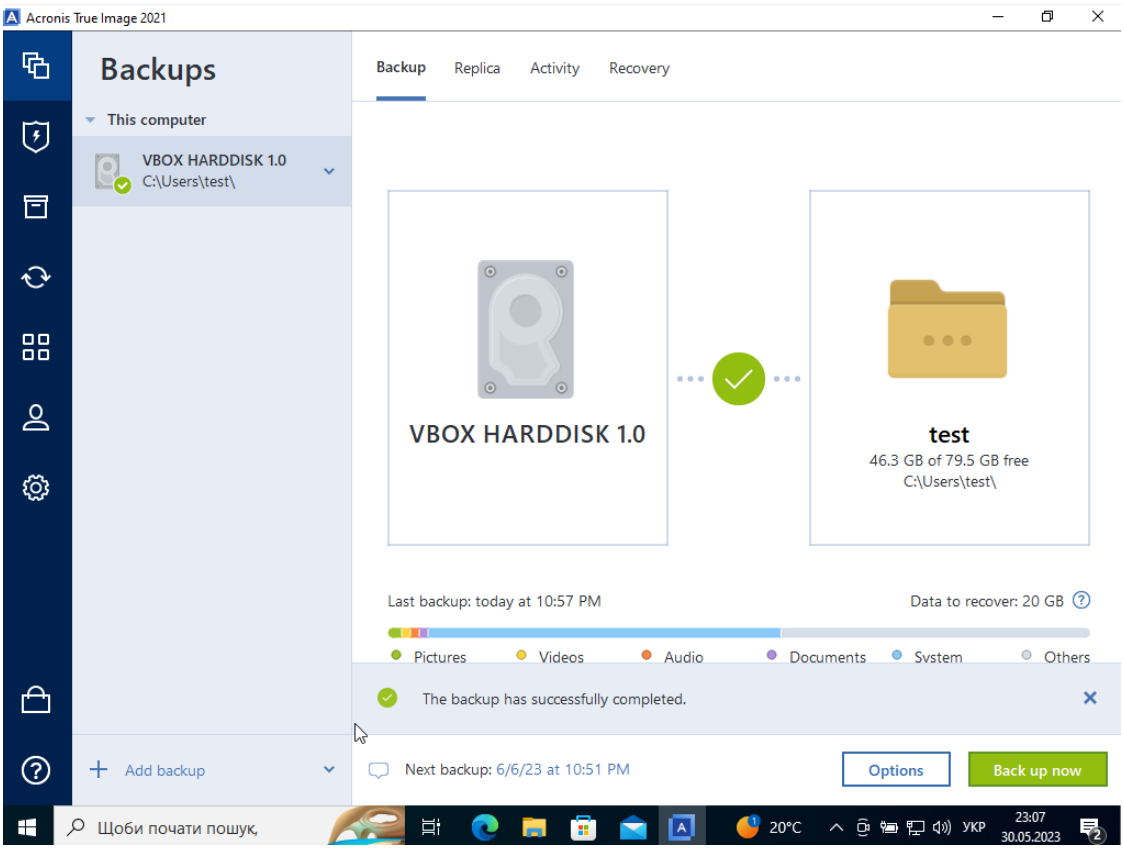

Рисунок 3.17 - Закінчення копіювання

Висновки до розділу 3

В ході розробки системи захисту інформаційних ресурсів від шкідливого програмного забезпечення були вивчені та проаналізовані ключові аспекти безпеки, які включають захист від вірусів та шкідливого програмного забезпечення, автентифікацію та авторизацію користувачів, міжмережеве екранування, криптографічний захист інформації, фізичний захист та резервне копіювання.

В процесі вивчення різних засобів захисту з'ясували, що комплексний підхід є найбільш ефективним. Застосування різних заходів захисту дозволяє створити багаторівневу систему, що забезпечує найкращу захищеність інформаційних ресурсів.

Було вивчено різні засоби автентифікації, включаючи RSA SecurID, Google authenticator та інші, а RSA SecurID було визнано кращим варіантом, з огляду на його властивості та здатність працювати без постійного підключення до інтернету.

Аналіз міжмережевого екранування показав, що використання міжмережевого екрану дозволяє контролювати вхідний та вихідний трафік, а також забезпечує додатковий рівень захисту від потенційно шкідливих дій.

Проаналізували декілька різних програм для шифрування, в результаті було обрано BestCrypt Volume Encryption як найбільш вигідний та безпечний варіант.

Дослідили фізичні засоби захисту, які включають біометричні пристрої для ідентифікації користувачів. Ці технології забезпечують високий рівень захисту і сприяють перешкоджанню несанкціонованого доступу до системи.

Наприкінці, було визнано, що регулярне резервне копіювання є важливою складовою частиною всієї системи захисту. Програма Acronis True Image була визначена як оптимальний інструмент для цієї цілі, враховуючи її потужні функції та надійність.

Таким чином, розробка системи захисту інформаційних ресурсів від шкідливого програмного забезпечення вимагає включення різних засобів і технологій захисту для забезпечення багаторівневого захисту. Така система допоможе забезпечити надійний захист від шкідливих вірусів та програм, захистить важливу

інформацію від несанкціонованого доступу та забезпечить відновлення даних у випадку їх втрати або пошкодження.

ВИСНОВКИ

У ході виконання дипломної роботи було проведено розгорнутий аналіз та розробка системи захисту інформаційних ресурсів від шкідливого програмного забезпечення. Робота включала вивчення різних засобів та методів захисту, а також вибір найкращих інструментів для створення ефективної системи захисту.

Було з'ясовано, що сучасні загрози для інформаційної безпеки вимагають комплексного підходу до захисту. Такий підхід обов'язково повинен включати антивірусний захист, міжмережеві екрани, криптографічний захист інформації, біометричні засоби автентифікації та резервне копіювання даних.

Досліджено програмно-апаратний комплекс захисту, який включає в себе ряд антивірусних програм. Крім того, було виявлено значення міжмережевих екранів у захисті інформаційних ресурсів та розглянуто їх апаратну реалізацію.

У контексті криптографічного захисту було розглянуто застосування програми BestCrypt Volume Encryption. Застосування біометричних засобів для автентифікації та авторизації було виявлено як ефективний метод захисту від несанкціонованого доступу. Зокрема, було визначено ефективність використання портативних сканерів з біометричним методом ідентифікації.

Визначено значення регулярного резервного копіювання як критичного елемента системи захисту інформаційних ресурсів. Acronis True Image було обрано як оптимальний інструмент для цього процесу.

Загалом, виконана робота підтверджує важливість комплексного та багатоаспектного підходу до забезпечення безпеки інформаційних ресурсів. Кожен компонент системи захисту відіграє свою важливу роль у запобіганні, виявленні та відновленні після шкідливих впливів.

Одним з ключових висновків є те, що сучасні технології захисту інформації мають вміти адаптуватися до постійно змінюваних загроз та використовувати розумні, передбачувальні механізми для запобігання можливим атакам.

Також важливо підкреслити значення правильної конфігурації та налаштування системи захисту. Кожен інструмент, чи то антивірусне програмне забезпечення, міжмережевий екран, програми для шифрування, біометричні пристрої автентифікації чи засоби резервного копіювання, вимагає правильного налаштування для забезпечення максимальної ефективності.

Особливо акцентується значення навчання користувачів. Найкраща система захисту може бути недостатньою, якщо користувачі не знають основних принципів безпеки і не здатні виконувати прості, але необхідні процедури, такі як регулярне оновлення програмного забезпечення та використання надійних методів автентифікації.

В цілому, робота підкреслила, що розробка та впровадження ефективної системи захисту є складним, але критично важливим завданням для будь-якої організації, яка зберігає або обробляє важливі інформаційні ресурси.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Поняття інформаційних ресурсів [Електронний ресурс]. – Режим доступу: https://studies.in.ua/inform-pravo-shporu/2518-ponyattya-nformacynih-resursv.html

2. Інформаційні ресурси [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Інформаційні_ресурси

3. Керування доступом на основі ролей [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Керування_доступом_на_основі_ролей

4. Інформаційна безпека [Електронний ресурс]. – Режим доступу: https://naurok.com.ua/informaciyna-bezpeka-247508.html

5. Про інформацію [Електронний ресурс]: Закон України від 21.12.2019 № 2657-XII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12

6. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс]: постанова КМУ від 29.03.2006 №373. – Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%EF#Text

7. Захист інформації [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Захист_інформації

8. Інформаційні ризики [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/5366708/page:4/

9. Шкідливий програмний засіб [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Шкідливий_програмний_засіб

10. Шкідливе програмне забезпечення [Електронний ресурс]. – Режим доступу: https://disted.edu.vn.ua/courses/learn/12421

11. Класифікація шкідливого програмного забезпечення [Електронний ресурс] – Режим доступу: https://studfile.net/preview/5206321/

12. Технології протидії шкідливим програмам [Електронний ресурс]. – Режим доступу: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1486

13. Антивірусна програма [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Антивірусна_програма

14. Антивіруси [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/programnezabezpecenna/sistemne-programne-zabezpecenna/antivirusi

15. Антивірусне програмне забезпечення [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/5610219/page:2/

16. Аналіз сучасних систем виявлення та запобігання вторгнень [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf

17. Система виявлення вторгнень [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Система_виявлення_вторгнень

18. Фільтрування електронної пошти [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Фільтрування_електронної_пошти

19. Основні правила захисту даних[Електронний ресурс]. – Режим доступу:https://www.eset.com/ua/about/newsroom/blog/data-protection/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-internet-polzovatelya/

20. Шифрування [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Шифрування

21. Захист інформації в комп’ютерній системі підприємства [Електронний ресурс]. – Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/rozdil7.html

22. Що таке брандмауер [Електронний ресурс]. – Режим доступу: https://techukraine.net/що-таке-брандмауер-вступний-посібн

23. Рейтинг найкращих антивірусів [Електронний ресурс]. – Режим доступу: https://itc.ua/ua/articles/reityng-antyvirusiv/

24. Що таке шкідливе програмне забезпечення [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-malware

25. Захист інформації в комп’ютерних системах [Електронний ресурс]. – Режим доступу: https://scs.kpi.ua/wp-content/uploads/2021/07/pdf/zahyst-informacziyi-v-kompyuternyh-systemah.pdf

26. Основи інформаційної безпеки та технічного захисту інформації [Електронний ресурс]. – Режим доступу: https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20tzi.pdf

27. Автентифікація (веб) [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Автентифікація_(веб)

28. RSA SecurID [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/RSA_SecurID

29. Check Point 4200 Appliance [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/uc/pdf/datasheets/4200-appliance-datasheet.pdf

30. Аутентифікація і авторизація [Електронний ресурс]. – Режим доступу: https://qagroup.com.ua/publications/autentyfikatciia-i-avtoryzatciia/

31. Що таке двофакторна автентифікація або 2FA? [Електронний ресурс]. – Режим доступу: https://experience.dropbox.com/uk-ua/resources/what-is-2fa

32. Avast [Електронний ресурс]. – Режим доступу: https://www.avast.ua/index#pc

33. Автентифікація за допомогою сертифікатів [Електронний ресурс]. – Режим доступу: https://it.wikireading.ru/59915

34. Що таке фільтрація пакетів [Електронний ресурс]. – Режим доступу: https://uk.theastrologypage.com/packet-filtering

35. Проксі-сервер [Електронний ресурс]. – Режим доступу: https://surfshark.com/uk/blog/proxy-server

36. Що таке протоколи безпеки [Електронний ресурс]. – Режим доступу: https://uk.myservername.com/what-is-ip-security

37. Шифрування даних [Електронний ресурс]. – Режим доступу: https://www.sim-networks.com/ukr/blog/data-encryption-best-practices

38. Атака типу Man-In-The-Middle: що треба знати кожному [Електронний ресурс]. – Режим доступу: https://www.imena.ua/blog/man-in-the-middle/

39. Асиметричне шифрування [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/9094212/page:19/