НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«СУЧАСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ»

Виконав: студент 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Вавілов Микита Богданович

Керівник: доцент, к.ф.-м.н.
Чепурна Олена Євгенівна

Рецензент: професор, д.ф.-м.н.
Василенко Микола Дмитрович

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Вавілову Микиті Богдановичу

1. Тема роботи: «Сучасні системи захисту інформаційних ресурсів від шкідливого програмного забезпечення»
Керівник роботи: доцент, к.ф.-м.н, Чепурна Олена Євгенівна
затверджені наказом НУ ОЮА від 02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 року
3. Дата видачі завдання«15» вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Сучасні системи захисту інформаційних ресурсів від шкідливого програмного забезпечення» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека.

Містить 21 рисунки, 7 таблиць, 20 літературних джерел за переліком посилань. Робота виконана на 52 сторінках загального тексту і 44 сторінках основного тексту.

Метою роботи є розробка та оцінка сучасних систем для захисту інформаційних ресурсів від шкідливого програмного забезпечення.

Об’єктом розробки є системи захисту інформаційних ресурсів, предметом розробки є методи та техніки для виявлення та блокування шкідливих програм. Шляхи досягнення мети включають аналіз існуючих методів захисту, розробку та тестування нових методів, а також їх інтеграцію в існуючі системи захисту.

Робота має високий ступінь реалізації, оскільки розроблені методи були успішно впроваджені у вигляді програмного забезпечення, що дозволяє автоматизовано виявляти та блокувати шкідливі програми.

Результати роботи можуть бути використані при розробці нових та покращенні існуючих систем захисту для виявлення та запобігання кіберзагрозам у різних сферах, включаючи фінансовий сектор, державні установи та комерційні організації.

Можливими напрямками подальших досліджень є покращення алгоритмів для виявлення нових типів загроз, розширення функціональних можливостей систем захисту, а також інтеграція розроблених систем з іншими засобами кібербезпеки для комплексного захисту інформаційних систем.

Ключові слова: КІБЕРБЕЗПЕКА, СУЧАСНІ СИСТЕМИ, ВИЯВЛЕННЯ ЗАГРОЗ, ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, АНАЛІЗ ДАНИХ, АВТОМАТИЗАЦІЯ, ЗАХИСТ ІНФОРМАЦІЇ

ABSTRACT

Qualification work on the topic ‘Modern systems for protecting information resources from malicious software’ for the first (bachelor's) level of higher education in the speciality 125 Cybersecurity, educational programme: Cybersecurity.

Contains 21 figures, 7 tables, 20 references according to the list of references. The work is executed on 52 pages of the general text and 44 pages of the main text.

The purpose of the work is to develop and evaluate modern systems for protecting information resources from malicious software.

The object of development is information resource protection systems, the subject of development is methods and techniques for detecting and blocking malware. Ways to achieve the goal include analysing existing protection methods, developing and testing new methods, and integrating them into existing protection systems.

The work has a high degree of implementation, as the developed methods have been successfully implemented in the form of software that allows automated detection and blocking of malware.

The results of the work can be used to develop new and improve existing security systems to detect and prevent cyber threats in various fields, including the financial sector, government agencies and commercial organisations.

Possible areas for further research include improving algorithms for detecting new types of threats, expanding the functionality of security systems, and integrating the developed systems with other cybersecurity tools for comprehensive protection of information systems.

Keywords: CYBERSECURITY, MODERN SYSTEMS, THREAT DETECTION, MALWARE, DATA ANALYSIS, AUTOMATION, INFORMATION PROTECTION

ЗМІСТ

ВСТУП

Актуальність теми. У епоху, коли інформація стає одним з основних активів організацій, захист даних від незаконного доступу, знищення або зміни є вирішальним для стабільності та довіри в бізнесі та управлінні.

Таке дослідження спрямоване на аналіз ефективності існуючих технологій захисту інформації та виявлення їх слабких місць. Це дозволяє не тільки підвищити захищеність вже існуючих систем, але й сприяє розробці нових, більш ефективних рішень.

Результати такого дослідження важливі для розробки стандартів та протоколів безпеки, що адаптовані до сучасних умов кіберпростору. Ці стандарти можуть бути прийняті на національному чи міжнародному рівнях, забезпечуючи уніфікований підхід до захисту даних.

Освітня складова цього дослідження допомагає підготувати кваліфікованих фахівців у галузі інформаційної безпеки. Воно стимулює розвиток академічних програм та курсів, спрямованих на виховання майбутніх експертів, здатних ефективно протистояти кіберзагрозам.

Четверте, дослідження сприяє співпраці між галузями і відомствами, посилюючи інтеграцію і синергію між різними секторами суспільства. Це підвищує загальну кіберстійкість національних інфраструктур і сприяє формуванню культури безпеки.

В сукупності це дослідження відіграє ключову роль у формуванні міцної та надійної інформаційної інфраструктури, здатної захищати інформаційні активи від сучасних загроз і сприяє створенню безпечного кіберпростору.

Мета дослідження – глибокий аналіз сучасних систем захисту інформаційних ресурсів від шкідливого програмного забезпечення.

Завдання роботи:

- надати основні поняття інформаційної безпеки та класифікація загроз;
- описати архітектуру систем захисту від шкідливого програмного забезпечення;

- охарактеризувати принципи та методи захисту інформації;
- проаналізувати сутність антивірусного захисту та його основні характеристики;
- визначення новітніх технологій розпізнавання та блокування шкідливих програм;
- оцінити методологію оновлення баз даних антивірусних програм;
- зробити тест ефективності антивірусних систем;
- надати аналіз випадків успішного захисту інформаційних ресурсів;
- зпрогнозувати розвиток систем захисту.

Об’єктом роботи є системи захисту інформаційних ресурсів від шкідливого програмного забезпечення.

Предметом роботи є аналіз методів та технік, що застосовуються у сучасних системах захисту для ідентифікації, блокування та усунення шкідливого програмного забезпечення.

Практичне значення отриманих результатів дослідження полягає у значному підвищенні ефективності захисту інформаційних систем від шкідливого програмного забезпечення. Завдяки детальному аналізу сучасних захисних технологій і методик, виявлено можливості для оптимізації існуючих систем безпеки, що дозволить компаніям та організаціям знизити ризики втрати даних та фінансових втрат пов’язаних з кібератаками. Результати дослідження також сприятимуть розвитку нових стратегій захисту, які будуть враховувати найновіші загрози та виклики у сфері кібербезпеки, тим самим підвищуючи загальний рівень безпеки інформаційних технологій. Крім того, ці результати можуть бути використані в освітніх програмах для підготовки фахівців з кібербезпеки, надаючи їм актуальні знання та навички для боротьби з кіберзагрозами.

1 ТЕОРЕТИЧНІ АСПЕКТИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1 Основні поняття інформаційної безпеки та класифікація загроз

Інформаційна безпека є фундаментальною складовою сучасного цифрового світу, що забезпечує захист даних від зовнішніх та внутрішніх загроз. Вона включає заходи для забезпечення конфіденційності, цілісності та доступності інформації. Ці три основні характеристики формують основу для захисту інформації, яка є критично важливою для будь-якої організації. Конфіденційність визначає необхідність захисту інформації від несанкціонованого доступу, тоді як цілісність забезпечує захист інформації від несанкціонованих змін, а доступність гарантує, що інформація залишається доступною для користувачів, коли вона їм потрібна. Захист інформації також охоплює процеси аутентифікації та авторизації, які дозволяють визначати та надавати права доступу до ресурсів [1, с. 291].

На додаток до забезпечення безпеки даних, інформаційна безпека включає заходи для захисту від фізичних і кібернетичних загроз, а також недбалого або шкідливого використання ресурсів. Вона має також важливий аспект контролю та аудиту, який дозволяє організаціям моніторити і аналізувати свої інформаційні системи для виявлення і виправлення потенційних вразливостей. Ці компоненти інформаційної безпеки забезпечують комплексний захист і є критично важливими для забезпечення довіри та надійності в цифровому просторі.

Інформаційна безпека - це сукупність заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, що зберігається, обробляється або передається в системі. Основні принципи, що становлять основу інформаційної безпеки зображені на рисунку 1.1.

Конфіденційність - забезпечення захисту інформації від несанкціонованого доступу. Це означає, що лише авторизовані користувачі мають право доступу до конфіденційної інформації.

Цілісність - гарантування правдивості, повноти та невідмінності інформації під час зберігання, обробки та передачі. Це означає, що інформація не може бути змінена або пошкоджена безповоротно без дозволу.

Рисунок 1.1 – Основні принципи інформаційної безпеки [2, с. 35]

Доступність - забезпечення того, що інформація буде доступною для користувачів у відповідний час. Це означає, що система повинна бути готова працювати в разі потреби та не бути піддається відмовам у обслуговуванні.

Також до основних понять, якими потрібно керуватися у інформаційній безпеці є:

- Аутентифікація - підтвердження ідентичності користувача або суб'єкта системи для надання доступу до ресурсів.
- Авторизація - надання прав користувачеві після успішної аутентифікації для доступу до певних ресурсів або функцій системи.
- Неденежність - захист від несанкціонованого доступу або втрати інформації через злам системи або дії зловмисників.
- Аудит - систематичне моніторинг, запис та аналіз подій та активностей в інформаційній системі для виявлення порушень безпеки та ідентифікації загроз [2, с. 35].

Загрози інформаційній безпеці можуть бути класифіковані за різними критеріями, такими як джерело загрози, методи атак, вплив на систему тощо. Основні класи загроз описані в таблиці 1.1.

Таблиця 1.1 – Класифікація загроз інформаційній безпеці [3, с. 195]

№	Класи	Опис
1.	Кібератаки	несанкціонований доступ, руйнування або викрадення інформації з використанням комп'ютерних мереж та технологій
2.	Віруси та інші шкідливі програми	програмні коди, які можуть завдати шкоди інформаційній системі, включаючи віруси, черви, троянці, шпигунське програмне забезпечення тощо.
3.	Соціальний інжиніринг	використання маніпуляційних технік для отримання конфіденційної інформації від користувачів, таких як ім'я, пароль або інші особисті дані.
4.	Фізичні загрози	загрози безпеці, пов'язані з фізичним доступом до обладнання чи інших інфраструктурних елементів інформаційної системи.
5.	Необережне використання	неналежне використання інформації або технічних засобів, що може призвести до їх втрати або пошкодження.

Забезпечення інформаційної безпеки вимагає комплексного підходу, що включає в себе технічні, організаційні та правові заходи. Розвиток нових технологій та поява нових загроз вимагає постійного вдосконалення заходів забезпечення безпеки для забезпечення захисту інформації у сучасному цифровому світі.

Забезпечення інформаційної безпеки в сучасному світі є складним завданням через швидкий розвиток технологій та зростання кількості загроз. Особливо актуальним є питання захисту інформації у великих корпораціях, де велика кількість даних та їх цінність залучають зловмисників. Захист від кібератак стає більш складним через високий рівень креативності та інноваційності в методах

атак, використання штучного інтелекту та машинного навчання зловмисниками для обходу захисних систем.

Соціальний інжиніринг продовжує бути однією з найбільш ефективних стратегій для злому систем безпеки, оскільки він цілиться на людський фактор — часто найслабшу ланку в захисних механізмах.

Виховання обізнаності та навчання персоналу є критично важливими компонентами інформаційної безпеки, адже вони допомагають зменшити ризики витоку інформації та інших інцидентів.

Фізичний захист та безпека обладнання також відіграють ключову роль. Це включає в себе контроль доступу до приміщень, зберігання серверів у захищених локаціях та використання засобів відеоспостереження для моніторингу потенційних фізичних втручань. Водночас, важливим є забезпечення надійного живлення та адекватних заходів для запобігання втраті даних в результаті технічних неполадок або стихійних лих.

Зростаюча інтеграція мережевих технологій у повсякденне життя також посилює потребу в цілісному підході до інформаційної безпеки, який би включав передові технологічні рішення та стратегії захисту.

Використання шифрування, багаторівневої аутентифікації та постійний аналіз безпеки є невід'ємними складовими ефективної політики безпеки. Крім того, регулярне тестування систем на проникнення та оцінка вразливостей можуть допомогти ідентифікувати потенційні слабкі місця перш, ніж їх буде використано зловмисниками [4, с. 428].

Забезпечення інформаційної безпеки вимагає комплексного підходу, який об'єднує технічні, організаційні та правові заходи. Він також вимагає постійного моніторингу та оновлення стратегій захисту, оскільки загрози постійно еволюціонують.

Організації повинні бути готові до реагування на нові виклики у сфері безпеки та вдосконалювати свої заходи захисту, щоб забезпечити безпеку своєї інформації та інфраструктури.

1.2 Архітектура систем захисту від шкідливого програмного забезпечення

На фоні постійно зростаючих загроз у сфері кібербезпеки, архітектура захисту від шкідливого програмного забезпечення (ШПЗ) стає все більш критичною для забезпечення безпеки інформаційних систем. Вона не лише є необхідною, але й визначає основу ефективного захисту від широкого спектру загроз, починаючи від вірусів та троянців до складних цілеспрямованих кібератак.

Ця архітектура об'єднує різноманітні технологічні та організаційні заходи, щоб створити комплексну систему захисту, яка поєднує в собі запобіжні, виявляючі та реагуючі механізми. Вона включає в себе використання антивірусного програмного забезпечення для виявлення та блокування шкідливих програм, файрволі для контролю трафіку, системи виявлення та запобігання вторгнень для реагування на аномальну активність, а також системи моніторингу та аудиту безпеки для виявлення потенційних загроз та розслідування інцидентів [5, с. 45].

Архітектура сфери захисту інформації та інформаційної безпеки зображено на рисунку 1.2.

Однак ефективність такої архітектури залежить не лише від використання технологічних засобів, але й від організаційних політик та практик. Регулярні оновлення програмного забезпечення, навчання персоналу щодо кібербезпеки, а також строгий контроль доступу до конфіденційної інформації - це лише деякі з ключових аспектів успішної стратегії захисту.

Важливо також підкреслити, що боротьба зі шкідливим програмним забезпеченням - це постійний процес, який потребує постійного моніторингу, аналізу та адаптації до нових загроз і технологій.

Тільки шляхом поєднання технічних і організаційних заходів можна забезпечити надійний рівень захисту від шкідливого програмного забезпечення і зберегти цілісність та конфіденційність важливої інформації.

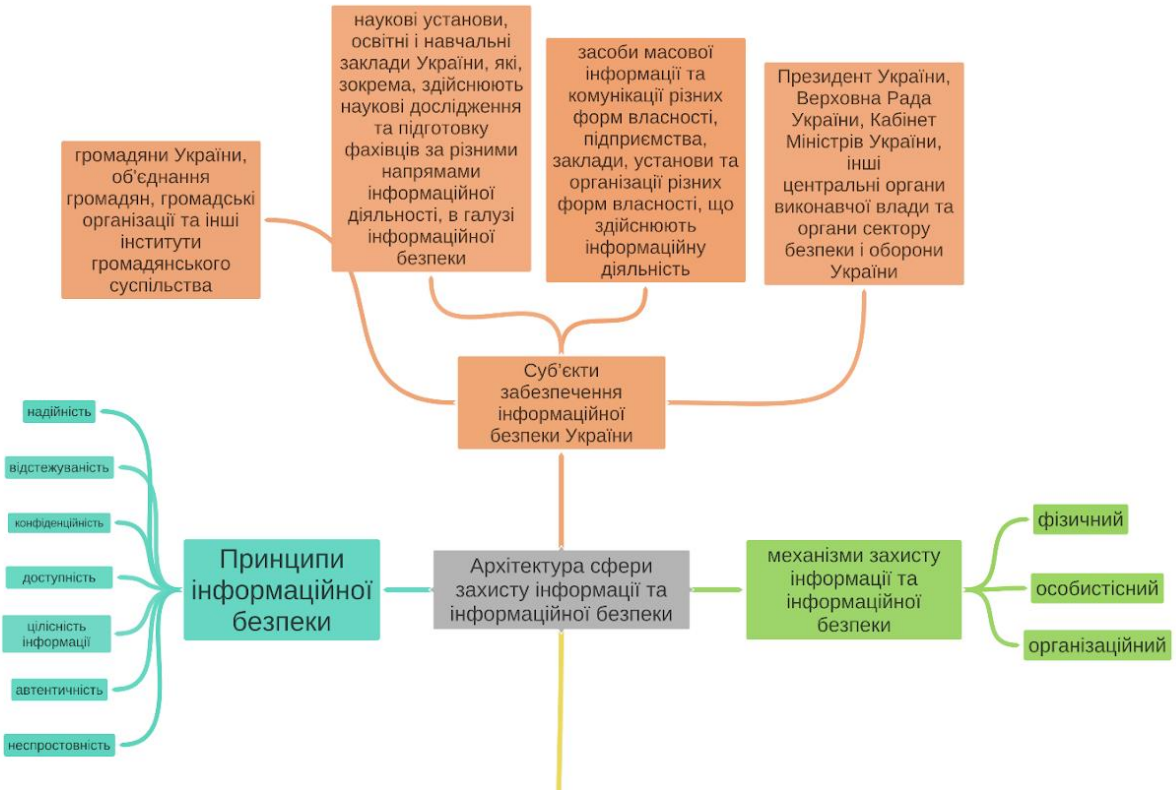

Рисунок 1.2 – Архітектура сфери захисту інформації та інформаційної безпеки [6]

Архітектура систем захисту від шкідливого програмного забезпечення (ШПЗ) є критично важливою для забезпечення безпеки інформаційних систем. Вона охоплює широкий спектр технологічних та організаційних заходів, спрямованих на виявлення, запобігання та вирішення проблем, пов'язаних зі шкідливим програмним забезпеченням. Основні складові архітектури захисту від ШПЗ включають пункти з таблиці 1.2.

Таблиця 1.2 – Архітектура систем захисту від шкідливого програмного забезпечення [7]

№	Складова	Опис	Вплив
1.	Антивірусне програмне забезпечення (АПЗ)	Одна з основних ланок захисту, яка виявляє та блокує віруси, черви, троянці та інші види ШПЗ.	Антивірусні програми сканують систему на предмет шкідливого коду та вживають заходів для його нейтралізації або видалення.
2.	Файрволи	Файрволи контролюють трафік, що проходить через мережу, та блокують небажану або	Вони можуть фільтрувати пакети даних за IP-адресою, портами та

		потенційно шкідливу активність.	іншими характеристиками для запобігання несанкціонованому доступу.
3.	Антишпигунське програмне забезпечення	Тип програм захищає від шпигунства та неправомірного збирання конфіденційної інформації.	Вони виявляють та блокують небажані програми, які можуть намагатися здійснювати перехоплення даних або відправляти конфіденційну інформацію на зовнішні сервери.
4.	Системи виявлення та запобігання вторгнень (СВЗВ)	Системи виявляють та реагують на небажані або агресивні дії у мережі.	Вони аналізують мережевий трафік, спостерігають за незвичайними патернами активності та спрацьовують сигнали тривоги при виявленні потенційно шкідливої активності.
5.	Системи моніторингу та аудиту безпеки	Системи збирають, аналізують та записують дані про безпеку	Дозволяє виявляти потенційні загрози, викривати небажану активність та проводити розслідування інцидентів.
6.	Регулярні оновлення та патчі	Важливо постійно оновлювати програмне забезпечення та встановлювати патчі для вирішення виявлених уразливостей.	Допомагає уникнути використання вразливостей зловмисниками для атак.
7.	Освіта та навчання користувачів	Інформування користувачів про загрози ШПЗ	Навчання їх розпізнавати підозрілу активність та правильно реагувати на потенційні загрози є так само важливим елементом архітектури захисту.
8.	Безпека даних	Захист важливих даних шляхом шифрування, регулярного резервного копіювання	Забезпечення їх цілісності та конфіденційності.
9.	Стратегії управління доступом	Обмеження доступу до чутливої інформації лише авторизованим користувачам	Використання політик доступу та ролей для контролю прав доступу.

Складові взаємодіють між собою, створюючи комплексну систему захисту, яка мінімізує ризики впливу ШПЗ на інформаційну інфраструктуру організації. Важливо регулярно переглядати та оновлювати архітектуру захисту відповідно до змін у загрозах та технологій, щоб забезпечити ефективний рівень захисту. Постійне вдосконалення та адаптація заходів захисту є ключовими аспектами у боротьбі з шкідливим програмним забезпеченням.

Ця комплексна архітектура захисту від ШПЗ не тільки допомагає у виявленні та блокуванні шкідливих програм, але й мінімізує ризики вразливостей і неправомірного доступу до інформації. Вона створює надійну оборонну систему, що включає в себе як технологічні, так і організаційні заходи.

Однак важливо пам'ятати, що безпека інформаційних систем - це постійний процес, а не одноразова подія. Тому необхідно постійно моніторити нові загрози та вдосконалювати стратегії захисту, щоб відповідати зростаючим вимогам безпеки [8].

Архітектура систем захисту від шкідливого програмного забезпечення є життєво важливим компонентом для забезпечення надійності та безпеки інформаційних систем в сучасному цифровому світі. Завдяки стрімкому розвитку технологій та збільшенню кількості кіберзагроз, важливість створення ефективних систем захисту не може бути переоцінена. Основна мета такої архітектури полягає у запобіганні, виявленні та реагуванні на атаки, що можуть завдати шкоди або навіть зруйнувати цілісність і конфіденційність даних.

Завдання захисту від шкідливого програмного забезпечення включає в себе багатошаровий підхід, де кожен шар спрямований на вирішення певних аспектів безпеки. Від антивірусного програмного забезпечення, що сканує та нейтралізує шкідливий код, до файрволів, які контролюють вхідний та вихідний трафік у мережі. Антишпигунське програмне забезпечення забезпечує додатковий рівень захисту від неправомірного збору конфіденційної інформації, тоді як системи виявлення та запобігання вторгнень діють як спостерігачі за будь-якою підозрілою активністю в мережі.

Ключовим аспектом захисту є також системи моніторингу та аудиту безпеки, які не лише виявляють потенційні загрози, але й забезпечують інструменти для аналізу та реагування на безпекові інциденти. Регулярні оновлення програмного забезпечення та оперативне впровадження патчів є невід'ємною частиною захисту, оскільки це допомагає закривати потенційні вразливості перед можливими атаками.

Надзвичайно важливим є освітній аспект - інформування та навчання користувачів. Підвищення обізнаності серед співробітників про потенційні загрози та навчання їх розпізнавати та адекватно реагувати на кібератаки є критично важливим для забезпечення загальної безпеки організації. Ці заходи в комплексі формують міцний фундамент для захисту інформацій

1.3 Принципи та методи захисту інформації

Щоб забезпечити надійний захист конфіденційності, цілісності та доступності даних, необхідно використовувати комплексний підхід, що базується на принципах та методах захисту інформації. Ці принципи, такі як принцип необхідного доступу, мінімальних прав доступу, цілісності, конфіденційності та доступності, формують основу ефективної стратегії інформаційної безпеки. Методи захисту, які включають технологічні, організаційні та процедурні заходи, спрямовані на мінімізацію ризиків інцидентів безпеки та забезпечення стійкості інформаційних систем. Впровадження цих принципів і методів в організаційні процеси дозволяє забезпечити високий рівень захищеності інформації, що є важливим аспектом в управлінні будь-якою сучасною структурою чи системою.

Історія захисту інформації охоплює тисячоліття розвитку, починаючи з простих методів шифрування в античних цивілізаціях, таких як Шпаргалка Цезаря, до сучасних криптографічних систем, які використовують складні математичні алгоритми. Стародавні цивілізації використовували методи, щоб захистити важливі інформаційні дані від несанкціонованого доступу, використовуючи наприклад, шифрування або приховання інформації в складних символах [9].

У середньовіччі шифрування стало ще більш складним і вдосконаленим. Такі методи, як шифр Віженера, дозволяли створювати більш стійкі системи захисту інформації. Проте із розвитком технологій з'явилися і нові методи атак на інформацію, що змусило розвивати більш ефективні системи захисту [10].

У XX столітті з появою комп'ютерів та Інтернету виникла необхідність у складних криптографічних системах. Сучасні методи захисту інформації використовують криптографічні протоколи та алгоритми, такі як RSA, AES та інші, які базуються на складних математичних обчисленнях. Також важливими є методи аутентифікації та авторизації, які дозволяють перевіряти ідентичність користувачів та обмежувати їх доступ до інформації [11].

Завдяки постійному розвитку технологій і зростанню загроз безпеці інформації, методи захисту постійно еволюціонують, шукаючи більш ефективні та надійні способи захисту конфіденційності, цілісності та доступності інформації.

Принципи та методи захисту інформації є важливою складовою сучасного управління інформаційною безпекою. Їх впровадження допомагає забезпечити конфіденційність, цілісність та доступність інформації, що є критичними аспектами для будь-якої організації чи системи.

Основні принципи захисту інформації включають:

1. Принцип необхідного доступу - кожен користувач має мати доступ лише до тієї інформації, яка необхідна для виконання його обов'язків чи завдань.
2. Принцип мінімальних прав доступу - користувачеві надаються лише ті права доступу, які є необхідними для виконання його конкретних завдань, мінімізуючи тим самим ризик несанкціонованого доступу.
3. Принцип цілісності даних - забезпечення того, щоб дані залишалися цілими і не зазнали неправомірних змін або порушень під час передачі, обробки або зберігання.
4. Принцип конфіденційності - забезпечення захищеності конфіденційної інформації від несанкціонованого доступу чи розголошення.
5. Принцип доступності – забезпечення того, щоб інформація була доступною для користувачів, які мають право на неї, у відповідний момент часу [12].

Методи захисту інформації включають в себе технологічні, організаційні та процедурні заходи, такі як шифрування даних, використання багаторівневих систем доступу, автентифікація користувачів, фізичні заходи безпеки (наприклад, захист приміщень і серверних кімнат), а також навчання персоналу з питань інформаційної безпеки та забезпечення їхньої свідомості про потенційні загрози. Комплексне застосування цих принципів та методів допомагає забезпечити надійний рівень захисту інформації в будь-якій організації чи системі.

Захист інформації є критично важливим аспектом для будь-якої сучасної організації чи системи. Це стосується не лише конфіденційних даних, а й усієї інформації, що обробляється, передається та зберігається в системі. Забезпечення безпеки інформації охоплює широкий спектр заходів і стратегій, які починаються з усвідомлення загроз, оцінки ризиків і розробки відповідних заходів захисту.

Один з ключових аспектів цього процесу - це усвідомлення потенційних загроз і вразливостей. Це може включати загрози з боку зловмисників, які намагаються несанкціоновано отримати доступ до інформації, технічні помилки або вразливості систем, а також навмисні або випадкові внутрішні загрози. Після ідентифікації загроз і вразливостей проводиться оцінка ризиків, щоб визначити, які заходи захисту є необхідними і наскільки вони ефективні.

Застосування методів захисту інформації включає в себе впровадження технологічних заходів, таких як шифрування даних, використання захищених мереж та систем доступу, а також встановлення процедур контролю доступу та аутентифікації користувачів. Організаційні заходи, такі як навчання персоналу з питань інформаційної безпеки, розробка політик безпеки та створення ефективної системи управління безпекою, також є важливими складовими захисту інформації.

Загальна мета всіх цих заходів - забезпечити конфіденційність, цілісність та доступність інформації, зменшити ризик втрати або несанкціонованого використання даних, а також забезпечити відповідність регуляторним вимогам та стандартам безпеки. Це потребує постійного моніторингу, оновлення та вдосконалення стратегій і заходів захисту, оскільки загрози і технології розвиваються постійно.

2 ТЕХНОЛОГІЇ ЗАХИСТУ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1 Сутність антивірусного захисту та його основні характеристики

Антивірусний захист є критичним елементом для забезпечення безпеки в динамічному цифровому середовищі сьогодення. Його сутність полягає у захисті інформації та пристроїв від шкідливих програм, які можуть завдати значних збитків як для окремих користувачів, так і для підприємств. Ефективний антивірусний захист має здатність адаптуватися до нових загроз і забезпечувати безпеку в реальному часі без значного сповільнення роботи пристроїв.

Це важливо як для захисту особистої інформації, так і для забезпечення надійності корпоративних мереж і інфраструктури. Постійна інноваційна робота у галузі антивірусного захисту сприяє створенню продуктів, які не тільки реагують на поточні загрози, а й передбачають їхній майбутній розвиток. Тим самим, антивірусний захист залишається важливим і необхідним інструментом для забезпечення безпеки та захисту в світі, що постійно змінюється та динамічно розвивається [13].

На рисунку 2.1 можна побачити приклади сучасних антивірусних програм.

Рисунок 2.1 – Приклади антивірусних програм

Антивірусний захист - це комплекс заходів і програмних засобів, спрямованих на запобігання, виявлення та видалення шкідливого програмного

забезпечення (вірусів, троянів, червів, шпигунського ПЗ тощо) з комп'ютерів та інших пристроїв. Основна сутність антивірусного захисту полягає в забезпеченні безпеки інформації та збереженні пристроїв від небажаних програмних впливів.

Основні характеристики антивірусного захисту включають:

Виявлення інфекцій:

- Антивірусні програми мають механізми для виявлення шкідливих програм. Це може бути на основі сигнатур (у випадку відомих загроз), поведінкового аналізу (виявлення незвичних або підозрілих дій програм), евристичного аналізу (використання загальних характеристик для виявлення потенційно небезпечних програм) тощо.

Видалення інфекцій:

- Після виявлення шкідливої програми, антивірусний захист має здатність видалити її зі системи. Це може включати карантин файлів, щоб вони не завдавали шкоди пристрою.

Оновлення вірусних баз даних:

- Регулярне оновлення баз даних антивірусного програмного забезпечення є необхідним для виявлення нових загроз, оскільки віруси постійно еволюціонують.

Фоновий режим роботи:

- Антивірусні програми часто працюють у фоновому режимі, без перешкоджання нормальній роботі користувача, але все ще забезпечують захист пристрою.

Захист в реальному часі:

- Деякі антивірусні програми забезпечують захист в реальному часі, виявляючи та блокуючи шкідливі програми навіть до їх виконання.

Захист від різних типів загроз:

- Основний антивірусний захист зазвичай включає захист від різних типів загроз, таких як віруси, черви, троянські коні, шпигунське ПЗ, рекламне ПЗ та інше.

Незначний вплив на продуктивність:

- Хороший антивірусний захист має мінімальний вплив на продуктивність пристрою, не сповільнюючи його роботу.

Функція превентивного захисту:

- Деякі сучасні антивірусні програми мають функції превентивного захисту, які спрямовані на запобігання зараження системи ще до того, як шкідливе програмне забезпечення отримає доступ до неї. Це може включати відстеження та блокування потенційно небезпечних веб-сайтів, електронних листів чи завантажень.

Захист від фішингу:

- Деякі антивірусні програми також включають функції захисту від фішингу, що допомагають користувачам уникати потенційно шкідливих веб-сайтів, які намагаються отримати конфіденційну інформацію.

Керування карантином:

- Антивірусні програми часто мають можливість керування карантином, що дозволяє користувачам переглядати та керувати файлами, які були поміщені в карантин для подальшого аналізу або видалення.

Мультисистемний захист:

- У світі, де користувачі часто використовують кілька пристроїв (наприклад, комп'ютери, смартфони, планшети), антивірусний захист може бути розширений для покриття всіх цих пристроїв і забезпечення їхньої безпеки.

Підтримка вирішення проблем:

- Хороші антивірусні програми також надають користувачам можливість отримати підтримку вирішення проблем, таких як видалення вірусів, налаштування програмного забезпечення та інше [14].

Антивірусний захист є невід'ємною складовою сучасного цифрового світу, де загрози від шкідливого програмного забезпечення постійно зростають. Забезпечення безпеки інформації та захисту пристроїв від потенційно небезпечних програм стають ключовими завданнями для користувачів у всіх сферах, від особистих комп'ютерів до корпоративних мереж.

Ефективний антивірусний захист має здатність виявляти, блокувати та видаляти шкідливе програмне забезпечення, забезпечуючи при цьому мінімальний вплив на продуктивність пристроїв. Захист в реальному часі, превентивні заходи, керування карантином і підтримка вирішення проблем - це лише деякі з важливих аспектів, які допомагають створити повноцінний антивірусний захист. Завдяки постійній еволюції технологій, антивірусні програми продовжують удосконалюватися, щоб залишатися ефективними у боротьбі зі зростаючими загрозами для безпеки в Інтернеті.

2.2 Технології розпізнавання та блокування шкідливих програм

Технології розпізнавання та блокування шкідливих програм є критично важливими для забезпечення безпеки в цифровому світі. Антивірусні програми сканують файли та системи, виявляючи віруси та інші загрози на основі відомих сигнатур та аналізуючи поведінку програм для ідентифікації нових шкідливих агентів.

Підписання коду допомагає перевіряти автентичність програм перед їх запуском, запобігаючи виконанню потенційно змінених або шкідливих додатків. Системи виявлення і запобігання вторгненням в мережу активно моніторять і блокують підозрілу активність, в той час як веб-фільтри (рис. 2.2) обмежують доступ до сайтів, які можуть бути небезпечними або містити шкідливий контент [15].

Інша важлива технологія, хеджування, дозволяє запускати програми в контрольованому, ізольованому середовищі для виявлення шкідливих дій, не ставлячи під загрозу основну систему.

Завдяки цим інноваційним технологіям, організації можуть значно знизити ризик кібератак та забезпечити більш надійний захист своїх інформаційних активів.

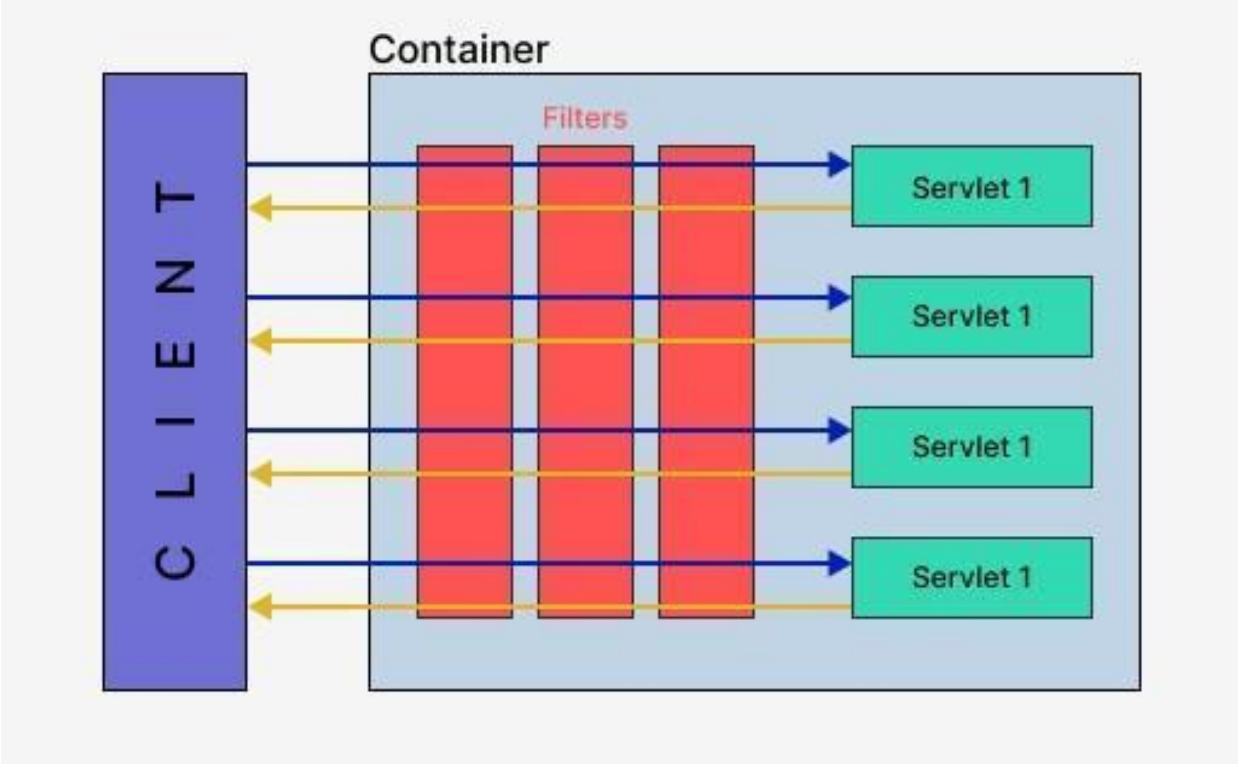

Рисунок 2.2 – Веб-фільтр [16]

Технології розпізнавання та блокування шкідливих програм є важливими складовими для забезпечення кібербезпеки в сучасному інформаційному середовищі. Кілька основних технологій у цій області можна побачити в таблиці 2.1:

Таблиця 2.1 – Основні технології блокування шкідливих програм [17]

№	Вид	Опис
1	Антивірусне програмне забезпечення (Антивіруси)	Це програми, які сканують комп'ютерні файли та систему на наявність шкідливих програм, вірусів, троянських програм, черв'яків тощо. Вони використовують бази даних відомих сигнатур шкідливого коду, а також алгоритми аналізу поведінки для виявлення нових загроз.
2	Підписання програм (Code Signing)	Це процес, за яким програмний код підписується цифровим підписом розробника. Це дозволяє оперативній системі та антивірусним програмам перевірити автентичність та цілісність програми перед її виконанням, запобігаючи виконанню

		непідписаних або модифікованих програм.
3	Аналіз поведінки (Behavioral Analysis)	Технологія, яка вивчає зміни в системі та програмах, що можуть вказувати на наявність шкідливого коду. Вона виявляє аномальну поведінку програм та спроби їх взаємодії з іншими системними компонентами.
4	Інтелектуальна система виявлення загроз (IDS) та системи запобігання вторгнень (IPS)	Ці системи відслідковують та блокують спроби несанкціонованого доступу до мережі або комп'ютерних систем. Вони використовуються для виявлення та блокування шкідливого трафіку та атак на мережеві пристрої.
5	Веб-фільтри	Ці технології використовуються для фільтрації веб-трафіку та блокування доступу до веб-сайтів, які містять шкідливий вміст або представляють потенційні загрози для безпеки користувачів.
6	Хеджування (Sandboxing) (рис. 2.3)	Це техніка, при якій сумісність програм відбувається в ізольованому середовищі, відокремленому від основної системи. Це дозволяє аналізувати поведінку програм та виявляти шкідливі дії без ризику поширення інфекцій.

Технології розпізнавання та блокування шкідливих програм є критично важливими для захисту кібербезпеки. Вони включають в себе антивірусне програмне забезпечення, яке сканує файли та системи на предмет вірусів та іншого шкідливого коду, використовуючи бази даних відомих загроз та алгоритми аналізу поведінки. Підписання коду дозволяє перевіряти автентичність та цілісність програм перед їх виконанням, запобігаючи роботі змінених або неавторизованих застосунків.

Аналіз поведінки допомагає виявляти нестандартні активності в програмах та системі, які можуть свідчити про наявність шкідливих програм.

Рисунок 2.3 – Принцип хеджування [18]

Системи виявлення та запобігання вторгнень (IDS та IPS) захищають від несанкціонованого доступу та атак на мережі, тоді як веб-фільтри блокують доступ до потенційно небезпечних веб-сайтів. Технологія хеджування, або віртуальна пісочниця, дозволяє ізольовано вивчати програми, мінімізуючи ризик інфекції системи. Використання цих технологій, як окремо, так і в комбінації, надає суттєвий захист від широкого спектру кіберзагроз.

2.3 Методи оновлення баз даних антивірусних програм

Антивірусні програми мають велике значення для забезпечення безпеки комп'ютерних систем, особливо в умовах постійного зростання кількості шкідливого програмного забезпечення. Один із ключових аспектів ефективності антивірусів полягає у постійному оновленні баз даних вірусних сигнатур.

Історично методи оновлення баз даних антивірусів пройшли значну еволюцію. Спочатку вони включали ручні оновлення, коли користувачі мусили самостійно завантажувати оновлення з веб-сайтів виробників антивірусного програмного забезпечення. Цей процес був не тільки клопітким, а й створював затримки в реакції на нові загрози.

З розвитком Інтернету та технологій антивірусні компанії почали автоматизувати процес оновлення. Це дозволило системам самостійно завантажувати та інсталювати оновлення без втручання користувача. Такі оновлення могли випускатися декілька разів на день, що забезпечувало більш швидку та ефективну відповідь на загрози [19].

У більш сучасних рішеннях застосовуються ще більш динамічні методи, такі як хмарні технології. Хмарні антивіруси можуть аналізувати дані в реальному часі та отримувати оновлення безпосередньо з хмари, що дозволяє ще більше зменшити час між виявленням нового вірусу та його блокуванням. Такий підхід забезпечує миттєве оновлення інформації та максимально швидку реакцію на вірусні загрози.

Антивірусні програми з часом зазнали значних змін у методах оновлення своїх баз даних, що критично важливо для забезпечення захисту від постійно змінюваних і зростаючих загроз.

1980-ті роки - самі початки антивірусних програм засвідчили еру, коли оновлення баз даних відбувалися рідко і майже виключно вручну. Користувачі мусили фізично отримувати дискети або CD з оновленнями та встановлювати їх вручну. Наприклад, відома антивірусна програма Norton Antivirus (рис. 2.4) вперше була випущена в 1991 році і спочатку оновлювалась через дискети.

Рисунок 2.4 – Перша версія Norton Antivirus

1990-ті роки - з розвитком Інтернету починається епоха автоматизації оновлень. Виробники антивірусного ПЗ, як McAfee і Symantec, запроваджують можливість завантаження оновлень з інтернету, що значно спрощує процес їх отримання і інсталяції.

2000-ті роки - автоматичні оновлення стають стандартом у галузі. Більшість антивірусних програм вже можуть самостійно перевіряти наявність оновлень і встановлювати їх без втручання користувача. Оновлення тепер виходять декілька разів на тиждень, а інколи навіть декілька разів на день.

2010-ті роки до сьогодення - використання хмарних технологій стає новим кроком у розвитку антивірусів. Хмарні антивіруси, такі як Panda Cloud Antivirus, який був випущений у 2009 році, використовують інтернет для того, щоб миттєво аналізувати і реагувати на нові загрози, не потребуючи традиційних оновлень баз даних, завантажених на локальні комп'ютери. Це значно підвищує швидкість відповіді на загрози і зменшує навантаження на ресурси користувача [20].

Кожен з цих етапів показує, як інновації у технологіях та зміна потреб користувачів вплинули на методи оновлення антивірусних програм, що в кінцевому підсумку зробило їх більш ефективними у боротьбі з вірусами та іншими шкідливими програмами.

Оновлення баз даних антивірусних програм є критично важливим для забезпечення ефективного захисту від нових загроз і вразливостей. Існують різні методи, які використовуються для оновлення таких баз даних:

- Оновлення через Інтернет: Більшість сучасних антивірусних програм мають функцію автоматичного оновлення через Інтернет. Програма періодично звертається до серверів виробника для завантаження нових визначень вірусів і оновлень програмного забезпечення.
- Ручне оновлення: Користувачі можуть вручну завантажувати оновлення баз даних антивірусної програми з веб-сайту виробника і встановлювати їх вручну. Цей метод корисний у випадках, коли автоматичне оновлення не працює або коли користувач хоче перевірити оновлення вручну.

- Оновлення через мережу оновлення: Деякі антивірусні програми можуть отримувати оновлення баз даних через локальну мережу в організації. Це дозволяє адміністраторам керувати процесом оновлення централізовано і ефективно.
- Оновлення за допомогою файлів оновлень: Користувачі можуть завантажувати файли оновлень баз даних з веб-сайту виробника антивірусної програми і встановлювати їх вручну. Цей метод корисний у випадках, коли доступ до Інтернету обмежений або коли потрібно оновити декілька комп'ютерів безпосередньо.
- Оновлення через обліковий запис користувача: Деякі антивірусні програми вимагають, щоб користувач мав обліковий запис на веб-сайті виробника для отримання оновлень. Це дозволяє виробникам відстежувати використання своєї програми і надавати користувачам персоналізовану підтримку.

Методи оновлення баз даних антивірусних програм мають критичне значення для забезпечення захисту від нових та еволюціонуючих загроз. Антивірусні програми зазвичай використовують різні підходи до оновлення своїх баз даних, які включають інкрементні та повні оновлення.

Інкрементні оновлення є найбільш поширеними, оскільки вони вимагають меншого обсягу даних для завантаження, що забезпечує швидкість та ефективність процесу. Під час інкрементного оновлення антивірусна програма завантажує тільки ті частини вірусних баз, які змінилися з моменту останнього оновлення. Це дозволяє швидко реагувати на нові загрози без необхідності перевантаження системи великими файлами.

Повні оновлення, хоч і менш часті, також важливі. Вони забезпечують повне переписування бази даних вірусів у програмі. Такий метод застосовується, коли вносяться значні зміни до структури бази даних або коли потрібно виправити помилки попередніх оновлень.

Антивірусні програми також використовують автоматизовані системи для регулярного оновлення баз даних. Ці системи можуть бути налаштовані для автоматичного завантаження та інсталяції оновлень у заданий час, що знижує

втручання користувача та забезпечує, що захисне програмне забезпечення завжди актуальне.

Важливо зазначити, що використання надійних джерел для оновлень є ключовим для запобігання завантаження шкідливих файлів, які можуть бути маскуватися під оновлення антивірусних баз. Тому антивірусні програми часто використовують зашифровані з'єднання для перевірки автентичності та цілісності оновлень перед їх інсталяцією.

3 СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

3.1 Тести ефективності антивірусних систем

Структурна організація системи захисту інформаційних активів від шкідливого програмного забезпечення включає сім елементів і базується виключно на ліцензованому програмному забезпеченні:

Засіб автентифікації та авторизації є вирішальним у обмеженні доступу користувачів. Аутентифікація та ідентифікація користувачів є фундаментальними не тільки для систем безпеки, але й при розробці будь-яких інформаційних систем. У наш час інформаційно-комунікаційний простір розвивається швидкими темпами, системи та послуги стають все більш децентралізованими; разом з тим, зростає значення адекватного вирішення проблеми доступу. Паралельно, у зв'язку з масштабною інформатизацією та прогресом технологій, вимоги до систем доступу стають більш строгими в контексті захисту від дій недобросовісних осіб, зовнішніх чи внутрішніх. Також наростає потреба у надійній ідентифікації користувачів та ресурсів, адже сучасні методи аутентифікації дозволяють персоналізувати дії користувачів, а системи контролю доступу забезпечують достатній рівень надійності для захисту інформаційних ресурсів.

Серед систем автентифікації та авторизації відомі такі рішення, як Fido, Sidway, Рутокен, Google Authenticator, та RSA SecurID. RSA SecurID виділяється серед них кращим балансом принципу роботи та якості, а інші не мають власного програмного забезпечення як для серверів, так і для персональних комп'ютерів. Google Authenticator працює за принципом підключення до інтернету, але для вищого рівня безпеки краще використовувати програмне забезпечення, яке може функціонувати автономно та без підключення до мережі.

Антивірусний засіб, розроблений для захисту інформаційних ресурсів, є програмно-апаратним комплексом, який забезпечує надійний захист інформаційної бази у локальній мережі. Інтегрований підхід до використання цього засобу передбачає управління всіма інформаційними потоками у захищеній

мережі. Ефективна робота системи, яка захи ає від вірусних атак усі компоненти інфраструктури, вимагає високого рівня узгодженості застосованих методів і інструментів. На ринку популярні такі антивіруси як Avira, ESET, AVG, Comodo, Symantec та інші.

В таблиці 3.1 представлене порівняння антивірусних засобів.

Параметри для порівняння включають кількість виявлених загроз, відсоток виявлених загроз, навантаження на центральний процесор і час, необхідний для пошуку загроз.

Таблиця 3.1 – Порівняння антивірусних засобів

Антивірус/ Характеристика	Кількість знайдених загроз	Завантаження центрального процесору	Час на пошук загроз	Відсоток знайдених загроз
Avast	2107	40-50%	10 хв.	81%
AVG	2840	15-30%	9-10 хв.	84%
Comodo	2255	45-55%	7-10 хв.	57%
Symantec	2497	40-50%	8-10 хв.	54%
ESET NOD32	1949	40-50%	5-7 хв.	50%

Брандмауери зазвичай забезпечують захист внутрішніх мереж організації від несанкціонованих доступів із глобальної мережі Інтернет. Однак вони також можуть використовуватися для оборони корпоративних інтрамереж, до яких підключені локальні мережі.

Для вибору фізичного брандмауеру корисно провести аналіз наявних на ринку моделей за допомогою таблиці 3.2.

Таблиця 3.2 Порівняння брандмауерів

Брандмауери	**Cisco ASA 5515 -X**	**Juniper SRX 220**	**Checkpoint 4210**

Пропускна спроможність Мб/сек	1200	950	1300
Пропускна спроможність з використанням IPS	400	100	1150
Підключень в секунду	15000	-	1000
VPN-трафік	250	100	210

Проаналізувавши параметри як-от пропускна спроможність, пропускна спроможність із застосуванням IPS, кількість з'єднань на секунду та VPN-трафік, можна дійти висновку, що найбільш підходящим варіантом для апаратного міжмережевого екрану є модель Cisco ASA 5515 –X. На комп'ютерах користувачів рекомендується використовувати вбудований програмний брандмауер Windows, налаштовуючи його згідно потреб.

Ці засоби криптографічного захисту допомагають забезпечити цілісність, конфіденційність та автентичність критично важливої інформації, а також надають юридичну значимість електронним документам в сфері інформаційної безпеки. Вони інтегровані з системами авторизації та аутентифікації, а управління ключами підтримується субсистемою управління ISS.

Серед криптографічних засобів захисту інформації можна виокремити програми BestCrypt Volume Encryption, Windows BitLocker та Knox. Відмінною рисою Windows BitLocker є відсутність можливості шифрування динамічних дисків, а також висока вартість ліцензії. Knox, розроблена для операційної системи Mac, не сумісна з ОС Windows. Тому найбільш прийнятним варіантом залишається BestCrypt Volume Encryption.

Для написання скриптів використовується мова програмування Lua, яка хоч і має меншу швидкість виконання порівняно з кодом на C, але дозволяє швидше та простіше розробляти програми. Сценарії можна модифікувати без необхідності перекомпілювання сервера, вони будуть автоматично перечитані та скомпільовані LuaJIT при наступному перезавантаженні.

Засоби інженерного та технічного захисту об'єктів базуються на механічних засобах і інженерних спорудах, які перешкоджають фізичному доступу зловмисників до об'єктів захисту. Технічні засоби дозволяють персоналу охорони отримувати інформацію про проникнення непрошених осіб у контрольовані зони та спостерігати за обстановкою.

Проникнення може бути як прихованим, так і з фізичним знищенням інженерних споруд та охоронного обладнання, використовуючи інструменти або вибухові пристрої, а у вкрай рідкісних випадках у вигляді озброєного нападу з нейтралізацією охорони.

Засоби фізичного захисту повинні бути простими у використанні та обслуговуванні, тому для захисту робочих станцій доцільно застосувати портативний сканер з біометричним методом ідентифікації. На ринку представлено кілька таких портативних сканерів (таблиця 3.3).

Таблиця 3.3 – Порівняння портативних сканерів з біометричним методом ідентифікації.

Характеристика	BioLink U-Match 3.5	Secugen Hamster Pro	BioLink U-Match BI
Розширення	508	500	508
Час розпізнавання	1/15 сек.	0,02-0,05 сек.	1/15 сек.
Шанс на помилку	10-9	10-9	10-9
Підтримка Win 10	-	+	+

Аналізуючи такі характеристики сканерів, як роздільна здатність (кількість пікселів на дюйм), швидкість визначення, ймовірність помилки та сумісність з останньою версією операційної системи Windows, можна зробити висновок, що у всіх сканерів однакова ймовірність помилки – одна помилка на мільйон випадків. Найкращі показники швидкості визначення має біометричний сканер Secugen Hamster Pro, який також підтримує останню версію Windows, тому його застосування в системі видається найбільш раціональним.

Щодо ефективних стратегій мінімізації наслідків інформаційних атак,

модифікацій даних та їх втрат, одним із ключових методів є належне впровадження процедур резервного копіювання даних у рамках системи захисту інформаційних активів.

Серед програмних рішень для резервного копіювання та архівування даних можна виділити такі програми, як Acronis True Image, Déjà Dup, Zinstall Backup та Areca Backup. Про Zinstall Backup наведено деталі в таблиці 3.4.

Таблиця 3.4 – Порівняння програмних засобів резервного копіювання та архівування.

Параметр	**Acronis True Image**	**Zinstall Backup**	**Areca Backup**	**Déjà Dup**
Відкритий код	-	-	+	+
Відновлення втрачених даних	+	+	-	+
Клонування дисків	+	-	+	-
Графік створення резервних копій	+	-	-	-

При аналізі програм для резервного копіювання можна дійти висновку, що Areca Backup та Déjà Dup, будучи програмами з відкритим кодом, можуть бути потенційно вразливими, адже зловмисники можуть використати відомості про їхню структуру для проникнення до інформаційних систем. На противагу цьому, Zinstall Backup не має такого обширного набору функцій як Acronis True Image, зокрема таких, як відновлення втраченої інформації, створення додаткових резервних копій, планування часу створення копій, клонування дисків та створення диференційних копій. Отже, для забезпечення надійного захисту інформаційних ресурсів від шкідливого програмного забезпечення рекомендується використовувати Acronis True Image.

3.2 Дослідження системи захисту

Для забезпечення надійного контролю доступу до комп'ютерних систем рекомендується застосування двофакторної автентифікації, заснованої на технології RSA SECURID. Цей метод значно знижує ризики неавторизованого доступу. Технологія складається з трьох основних елементів:

RSA Authentication Manager - це серверний компонент, що встановлюється на окремий комп'ютер і виконує кілька ключових функцій:

- Зберігає базу даних користувачів і журнал подій.
- Обробляє дані, отримані від агентів автентифікації.
- Веде реєстр зареєстрованих токенів.
- Можливість розгортання мережі серверів, кожен з яких захищає визначену зону і може перебрати на себе функції інших у разі їх збою.

RSA Authentication Agents - ці програмні агенти інсталюються на захищені ресурси і замінюють стандартний запит на введення логіна та пароля на вимогу ввести дані SecurID (логін, пін-код та код токена). За відповіддю від сервера, агент надає доступ або блокує його.

Hardware&Software Authenticators - засоби автентифікації у формі фізичних токенів або відповідного програмного забезпечення. Вони постійно перебувають у користувача і показують поточне значення одноразового пароля. Кожен токен містить вбудований акумулятор, який працює протягом усього терміну служби токена (від 2 до 5 років). Токен генерує коди на основі внутрішнього годинника та 128-бітного випадкового числа, що служить стартовим вектором. Сервер може в будь-який момент відновити поточний код, використовуючи той самий алгоритм, завдяки чому забезпечується синхронізація між сервером та токеном.

Рисунок 3.1 – Принцип роботи RSA Authentication Manager та токену.

Ця система двофакторної автентифікації дозволяє значно підвищити безпеку доступу до важливих інформаційних ресурсів, як-от веб-сервери, VPN, поштові сервери, та інші мережеві служби.

Токен в формі брелока для ключів RSA SecurID SID700 зображено на рисунку 3.2.

Рисунок 3.2 – Токен RSA SecurID SID700.

Токен RSA SecurID SD200 За формою аналогічний банківської пластиковій картці. Виконаний з металу, його товщина близько 5 мм. Зображено на рисунку 3.3.

Рисунок 3.3 – Токен RSA SecurID SD200.

Токен RSA SecurID моделі SD520 має розміри, подібні до SD200, проте відрізняється наявністю цифрової панелі. Користувач вводить свій пін-код за допомогою цієї панелі, і в результаті токен показує не тільки код токена, але й комбінацію пін-коду з токен-кодом, яка використовується для аутентифікації. Це дозволяє забезпечити конфіденційність пін-коду, навіть у випадках, коли можливе знімання даних з клавіш. Токен RSA SecurID SD520 зображений на рисунку 3.4.

Рисунок 3.4 – Токен RSA SecurID SD520.

Процедура налаштування RSA Authentication Manager та RSA Authentication Agent (рис. 3.5).

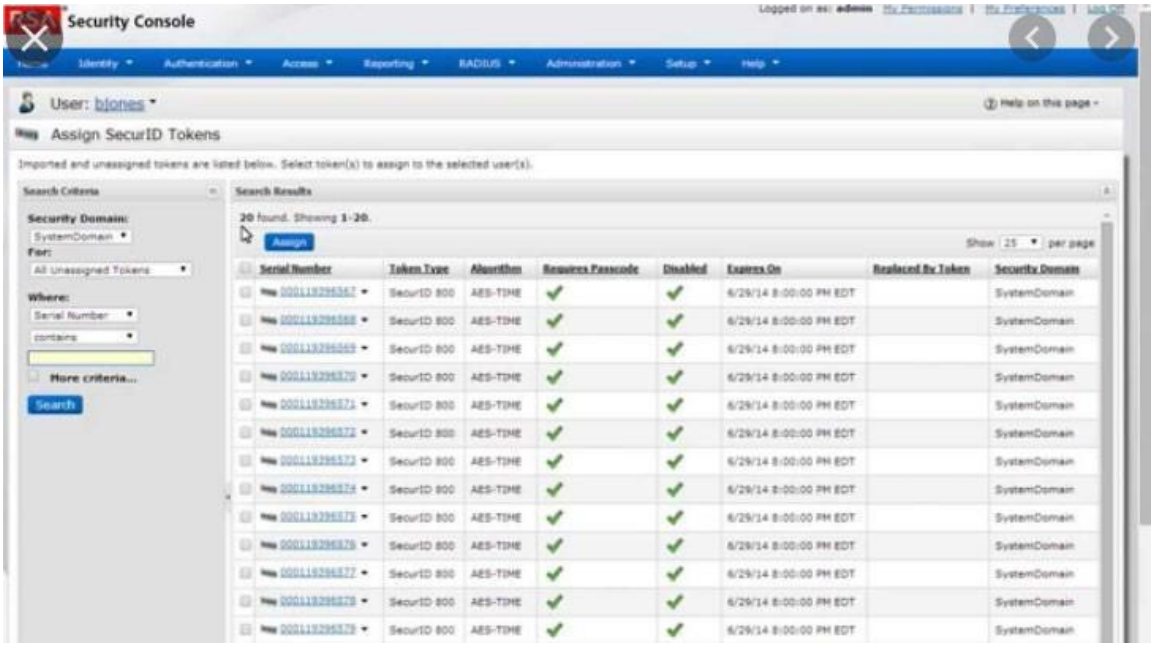

Рисунок 3.5 – Консоль управління RSA Authentication Manager.

У панелі безпеки потрібно вибрати "Доступ", далі "Агенти автентифікації" і натиснути "Створити нового".

В області "Домен безпеки" слід додати домен, до якого буде прив’язано нового агента.

У секції "Основні налаштування агента автентифікації" слід виконати наступне:

3.1. В поле "Ім'я хосту" ввести ім'я нового хосту для агента, потім клікнути на "Визначити IP". IP-адреса з'явиться автоматично. Нове ім'я має бути унікальним.

3.2. (Опціонально) У полі "IP-адреса" можна ввести IP-адресу агента. Якщо використовується вже існуюче ім'я сервера, дане поле автоматично заповнюється і доступне тільки для перегляду. Якщо адреса не вказана, агенти UDP будуть використовувати автоматичну реєстрацію для отримання адреси сервера.

3.3. (Опціонально) У полі "Альтернативні IP-адреси" вказати додаткові IP-адреси агента. Це потрібно, якщо у агента декілька мережевих карт або він знаходиться за мережевим брандмауером. У випадку використання вже існуючого імені сервера, дане поле також буде заповнене автоматично і доступне лише для перегляду.

(Опціонально) У секції "Атрибути агента автентифікації" можна встановити такі параметри:

• Вибрати тип агента. Якщо агент є веб-агентом, слід вибрати "Веб-агент", або залишити стандартне значення "Стандартний агент". Типи агентів слугують маркерами для RSA Authentication Manager, проте вибір між веб-агентом та стандартним агентом не вносить функціональних відмінностей. Для тимчасового призупинення доступу до ресурсу можна обрати "Агент вимкнено".

• Для додавання обмеженого агента, обрати "Дозволити доступ тільки користувачам певної групи", які мають право користуватися цим агентом.

• Щоб налаштувати новому агенту список контактів вручну або автоматично, можна використати "Кнопки списку контактів менеджера автентифікації".

(Опціонально) Для налаштування методу автентифікації користувачів з довіреної зони до цього агента, вибрати "Увімкнути надійну автентифікацію сфери" та визначити, чи дозволяти всім довіреним користувачам проходити автентифікацію через нового агента або тільки тим довіреним користувачам, які

належать до відповідної групи.

Настроювання компонентів захисту включає:

• Налаштування брандмауера через сторінку безпеки брандмауера.

• Вмикання та налаштування веб-проксі на сторінці захисту веб-проксі.

• Активація та налаштування поштового проксі через сторінку "Захист поштового проксі".

В якості міжмережевого екрану використовується Cisco ASA 5515-X для системи та Windows Firewall для комп’ютерів користувачів.

Процедура налаштування Cisco ASA 5515-X описана у командах на рисунку 3.6.

Останній крок — це збереження налаштувань шляхом вибору опції "Зберегти". Після цього користувач отримує фізичний токен для входу в систему.Для конфігурації інтерфейсу і IP-адреси необхідно в консолі Cisco ASA 5515-X використати команди з рисунку 3.6.

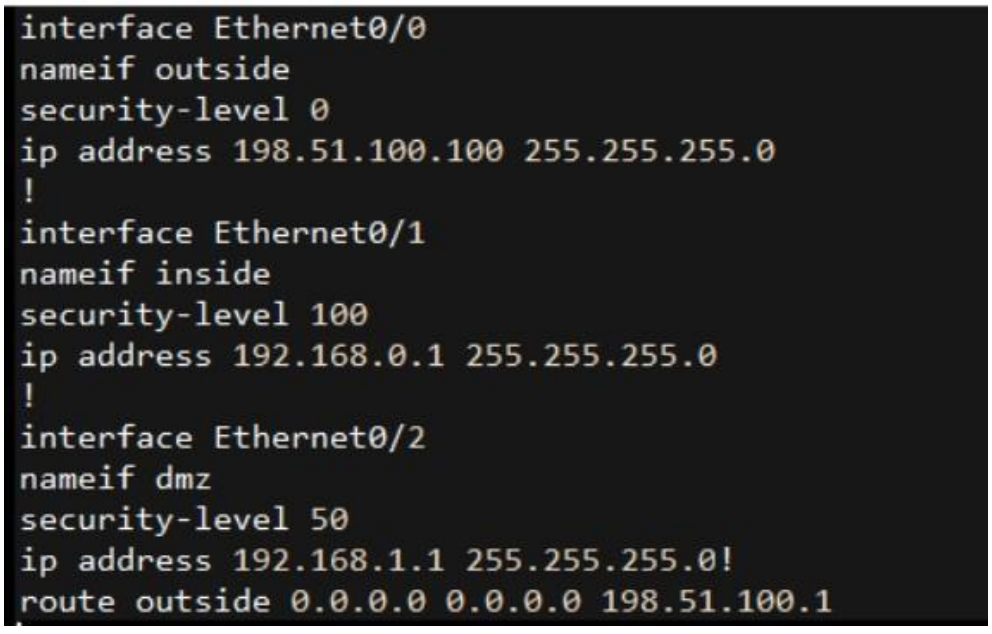

Рисунок 3.6 – Конфігурація та налаштування інтерфейсу і IP-адреси.

Також в налаштуваннях брандмауера необхідно виконати налаштування WEB- серверу за допомогою таких команд (рис. 3.7).

```
object network webserver-external-ip
host 198.51.100.101
!
object network webserver
host 192.168.1.100
nat (dmz,outside) static webserver-external-ip service tcp www www
```

Рисунок 3.7 – Налаштування WEB-серверу в консолі управління брандмауера

Процедура налаштування Windows Firewall

1) Необхідно клацнути на іконку пошуку поруч із пунктом «Пуск» і ввести фразу «Панель управління».

2) В наступному вікні, з вибором всіх налаштувань, які пропонує операційна система Windows 10, потрібно перейти до параметра, яким є «Брандмауер захисника Windows». Цей брандмауер оснащений вбудованим протоколом безпеки, який реєструє IP-адреси та іншу інформацію, пов’язану з підключеннями в домашніх та офісних мережах або Інтернеті. Він надає можливість фіксувати як успішні з’єднання, так і непередані пакети. Така функціональність дозволяє відслідковувати моменти підключення комп’ютерів у мережі до різноманітних веб-сайтів.

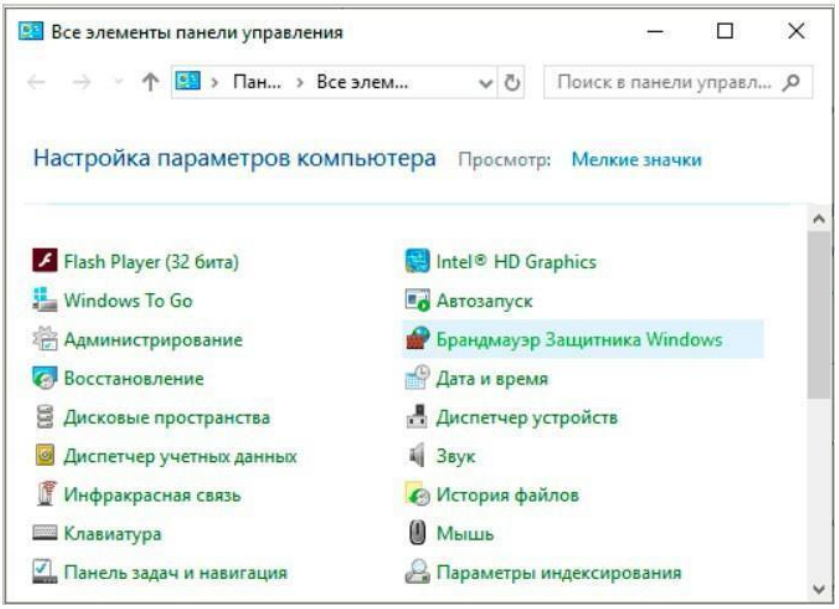

Рисунок 3.8 Вибір пункту «Брандмауер захисника Windows»

У наступному вікні виберіть опцію "Додаткові параметри" для доступу до розширених функцій налаштування брандмауера.

У розділі "Додаткові параметри" можна оглянути поточний статус захисника та його основні налаштування, що розміщені в першому пункті під назвою "Монітор брандмауера". Це включає правила для вхідних та вихідних з'єднань, а також правила безпеки та моніторингу.

Щоб налаштувати блокування певних програм, перейдіть до колонки "Правила для вихідних з'єднань" та виберіть опцію "Створити правило".

Вікно, що з'явиться, пропонує кілька варіантів для блокування мережі: блокування окремої програми, блокування визначеного порту, правило для управління підключеннями Windows, а також можливість налаштувати правило відповідно до індивідуальних потреб користувача. Зокрема, буде застосовано блокування обраної програми.

Для блокування конкретної програми необхідно вибрати опцію "Шлях програми" та вказати потрібну програму. Наприклад, блокування виконується для браузера Google Chrome, розташованого за шляхом "C: \ Program Files (x86) \ Google \ Chrome \ Application".

Після вибору програми, виберіть дію "Заблокувати з’єднання" та натисніть "Далі".

У наступному вікні виберіть профілі, для яких буде застосовано нове правило блокування, як показано на рис. 3.17. Профілі можуть бути доменними (для корпоративних мереж), приватними (для особистих мереж вдома чи на роботі) або публічними (для загальнодоступних мереж).

В останньому вікні вкажіть назву правила та використовуйте поле "Опис" для внесення додаткових нотаток, які можуть бути корисними користувачу. Для завершення налаштування використовуйте кнопку "Готово".

Так само можна блокувати обраний порт.

Засіб криптографічного захисту, який було обрано для проєкту, - це програма BestCrypt Volume Encryption. Цей інструмент здатний шифрувати не лише окремі секції жорстких дисків чи мобільні носії, такі як флеш-накопичувачі, а й різні

складні томи, включаючи звичайні, дзеркальні та RAID5 томи. Це робить його ідеальним для захисту комерційної інформації на серверах.

Основною особливістю BestCrypt Volume Encryption є використання різних криптографічних технологій, таких як AES (256-біт), Blowfish (448-біт), CAST (128-біт), RC6 (256-біт), Serpent (256-біт), Twofish (256-біт). Всі вони відомі своєю надійністю та глибоким дослідженням. Генерація ключа шифрування відбувається завдяки хаотичним натисканням клавіш і рухам миші, що вважається найкращим підходом для гарантування надійності шифрування, оскільки не залежить від якості генератора випадкових чисел. За замовчуванням, ключ шифрування зберігається на жорсткому диску і захищений паролем.

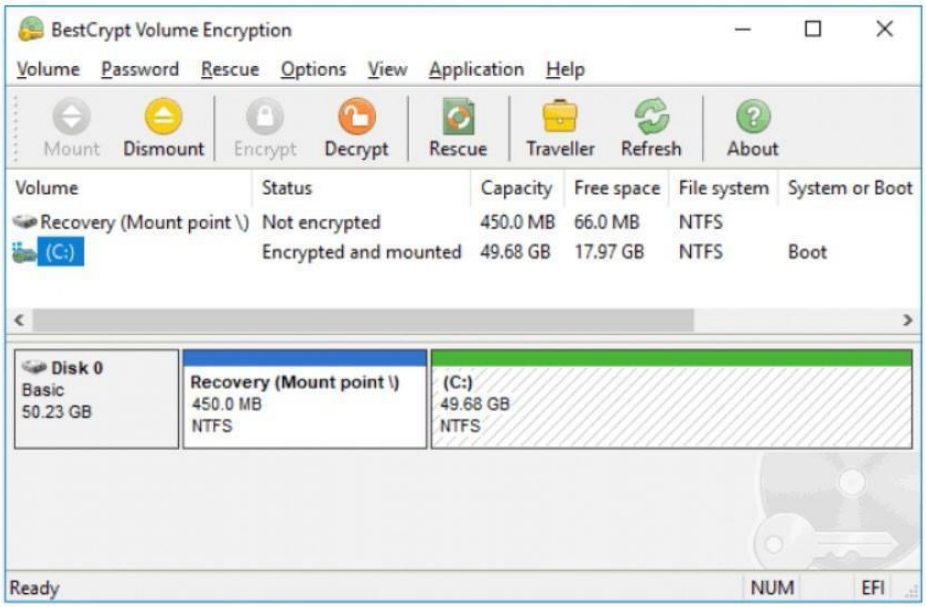

Рисунок 3.9 – Вікно програми BestCrypt Volume Encryption

Однією з ключових особливостей програми BestCrypt Volume Encryption є можливість шифрувати системний розділ жорсткого диска, що відкриває користувачам шлях до вирішення низки серйозних проблем. Перш за все, програма забезпечує запуск операційної системи тільки після введення правильного пароля до вже зашифрованого диску. Також користувач має змогу вибрати одну з тем для повідомлень, які з'являються при старті комп'ютера та при помилковому введенні пароля. З шести доступних тем, дві імітують типові помилки, що виникають під час

збоїв операційної системи, а третя – зупинений процес завантаження Windows. Це створює ілюзію поломки ПК для незнайомих з захистом осіб, що служить додатковим рівнем безпеки.

Ще однією корисною особливістю програми BestCrypt Volume Encryption, особливо важливою для корпоративних користувачів, є підтримка мережевої функціональності. Якщо на диску до шифрування існували загальнодоступні папки, то після розшифрування всі встановлені дозволи знову активуються, що дозволяє безпечно використовувати цей продукт для захисту будь-яких даних на сервері, включаючи документи та бази даних.

У контексті захисту WEB-серверу, в файлі налаштувань nginx.conf рекомендується збільшити обмеження кількості файлів та відкритих з'єднань. Для цього спершу потрібно налаштувати nginx для Web-серверу, вказавши у розділі http необхідні параметри для виконання скриптів на мові Lua:

```
lua_shared_dict whitelist 100m;
lua_shared_dict banlist 1000m;
lua_package_path '/home/ Vladyslav/antiddos/?.lua;;';
init_by_lua ‘
local whitelist = ngx.shared.whitelist
whitelist:add("4.1.2.3", true)
whitelist:add("7.5.8.6", true) ;
access_by_lua_file /home/Vladyslav/antiddos/main1.lua;
```

У параметрі lua_shared_dict встановлюється ключ для створення словника, що використовується для зберігання так званих «білих» та «чорних» списків. Цей словник може також включати параметр тривалості життя ключового значення, що є ідеальним для управління лічильниками шкідливого ПЗ, коли необхідно обмежувати кількість запитів протягом певного часу.

Параметр lua_package_path вказує шляхи до пошуку Lua модулів, інтеграції з каталогом скриптів. Використовуючи крапки з комою на кінці строки, можна додати заданий шлях до існуючого значення шляху без його заміни.

У директиві init_by_lua визначається код, який виконується одноразово при запуску сервера для створення білого списку IP-адрес. Також використовується

значення «true» для оператора умови if, оскільки третій параметр часу життя відсутній, застосовується необмежений час.

access_by_lua_file задає шлях до сценарію, який запускається при кожному запиті до сервера.

ZeroBrane Studio, відкрите середовище розробки для Lua, підтримує написання коду, виділення синтаксису, аналіз коду, кодування в режимі реального часу та налагодження для версій Lua 5.1, Lua 5.2, Lua 5.3, LuaJIT та інших реалізацій Lua. Воно базується на наборі інструментів wxWidgets і компоненті Scintilla для обробки файлів.

Сценарій захисту веб-сервера від атак типу «Denial of Service» (відмова в обслуговуванні) дозволяє ефективно забезпечити безпеку ресурсів.

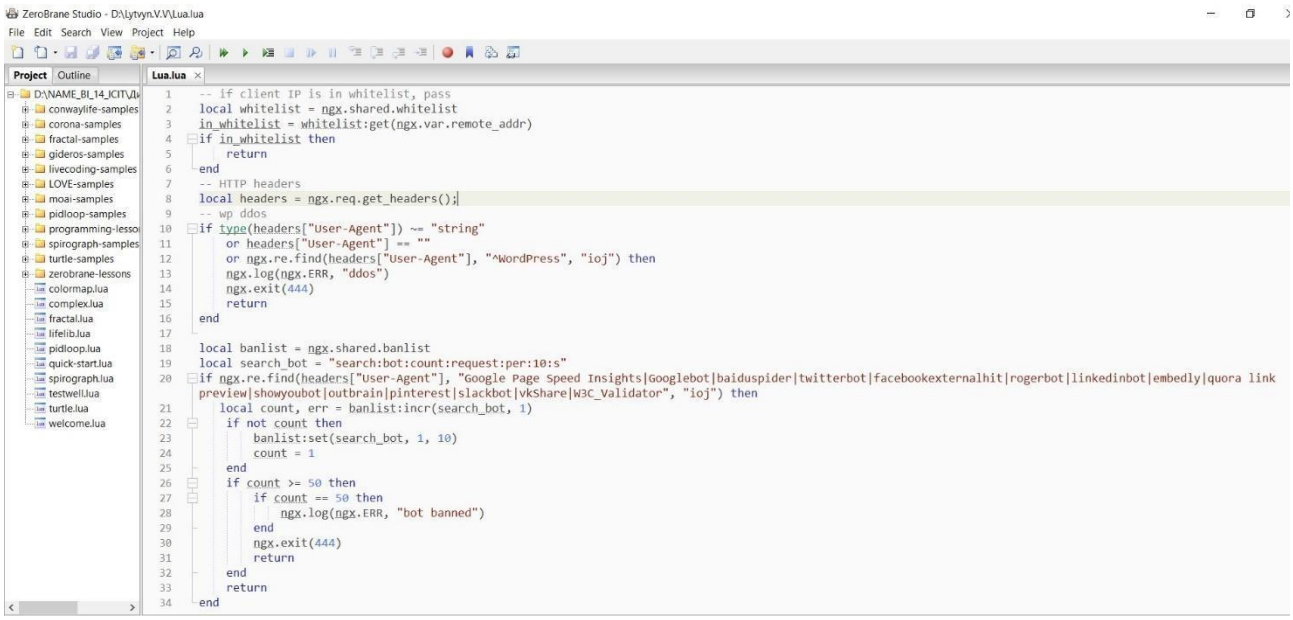

Рисунок – 3.10 Скрипт захисту web-ресурсу

Глобальна змінна «ngx» використовується для взаємодії з серверним контекстом nginx. Команда «return» в кінці функції дозволяє здійснювати повернення контролю від модуля. Це означає, що якщо IP-адреса знаходиться у списку дозволених, то скрипт зупиняється, і запит продовжує оброблятись. Далі процес передбачає ідентифікацію можливої атаки, заснованої на параметрах, що використовуються в CMS WordPress. У разі виявлення атаки, обробка завершується

з кодом помилки 444: ngx.exit (444).

Процес пошуку ботів вимагає введення лічильника, адже кіберзлочинці часто маскують свої дії під діяльність пошукових ботів. Команда «ban_list: set (search_bot, 1, 10)» запускає лічильник, який скидає своє значення до нуля через десять секунд після активації. Команда «ban_list: incr (search_bot, 1)» збільшує лічильник на одиницю, тим самим рахуючи кількість ботів.

Подальша ідентифікація ботів та зловмисників можлива за різними параметрами. Скрипт залежить від таких чинників, як підтримка клієнтом перенаправлень, налаштування cookies, та виконання коду. Також можливо використати налаштований Web-сервер як проксі, який захистить основний сервер, розміщений під іншою IP-адресою, фільтруючи і блокуючи небажані IP-запити.

94.242.55.0	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH...	1	[]
82.146.36.0	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gec...	1	[]
165.227.208.0			[]
46.173.218.0	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gec...	18	[]
46.173.219.0	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gec...	15	[]
37.9.113.0	Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	1	[]
87.236.16.0	WordPress/5.2.4; http://seliane.ru	131	[]
157.55.39.0	msnbot/2.0b (+http://search.msn.com/msnbot.htm)	1	[]
5.45.207.0	Mozilla/5.0 (compatible; YandexMetrika/2.0; +http://yandex.com/bot...	2	[]
95.108.181.0	Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	1	[]
95.173.146.0	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/2010010...	1	[]
95.169.184.0	Zend\\Http\\Client	1	[]
188.127.249.0	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH...	6	[]
74.125.76.0	FeedBurner/1.0 (http://www.FeedBurner.com)	1	[]
52.162.161.0	Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot...	1	[]
87.250.224.0	Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	1	[]
141.8.142.0	Mozilla/5.0 (compatible; YandexMetrika/2.0; +http://yandex.com/bot...	2	[]
95.163.105.0	Mozilla/5.0 (Windows; Linux i686; en-us) like Gecko Safari/563.9	240	[]
95.108.213.0	Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	1	[]
95.213.196.0	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, l...	2	[]
94.242.57.0	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH...	11	[]
89.151.179.0	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, l...	1	[]
2.135.67.0	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHT...	1	[]
207.46.13.0	msnbot/2.0b (+http://search.msn.com/msnbot.htm)	2	[]
77.111.247.0	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHT...	1	[]
193.124.181.0	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko...	2	[]
199.249.230.0	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko...	2	[]

Рисунок 3.11 – Результат роботи скрипта.

6) Засіб фізичного захисту

До засобів фізичного захисту можна віднести біометричний захист робочих станцій Hamster Pro від Securegen (рис 3.12).

Рисунок 3.12 – Біометричний зчитувач Hamster Pro

Hamster Pro від Secugen є одним із лідерів серед біометричних зчитувачів, завдяки своїй високій ефективності, компактності та доступній ціні. Цей USB-сканер використовується для покращення захисту доступу до комп'ютерних робочих станцій, мережевих ресурсів та веб-серверів. Він зазвичай використовується для захисту станцій, що мають доступ до критично важливої інформації, наприклад, до платіжних систем чи корпоративних даних. Оновлений зчитувач підтримує Windows Biometric Framework (WBF), що дозволяє використовувати Hamster Pro для біометричної аутентифікації через відбитки пальців при вході в операційну систему. Вбудований оптичний датчик має роздільну здатність 500 точок на дюйм, а також забезпечений автоматичним виявленням сканування та виявленням дефектів, посилюючи тим самим захист від фізичних пошкоджень.

Процедура налаштування:

Зчитувач приєднується до комп'ютера через порт USB-A без потреби встановлення додаткового програмного забезпечення.

Необхідні драйвери автоматично завантажуються і встановлюються.

Щодо програми Acronis True Image, вона є ідеальним рішенням для централізованого резервного копіювання даних на робочих станціях у корпоративній мережі. Програма дозволяє створювати повні резервні копії жорстких дисків та їх розділів, включаючи всі збережені дані, операційні системи та застосунки, а також важливі для користувача файли та папки. Сумісність з 64-

бітними та 32-бітними версіями Windows гарантує захист даних на станціях різних поколінь. У разі серйозних збоїв програмного чи апаратного характеру Acronis True Image дозволяє провести повне або часткове відновлення системи. Вбудована консоль управління Acronis дозволяє віддалено керувати всіма комп'ютерами в мережі, спрощуючи роботу системного адміністратора та знижуючи загальні витрати на підтримку мережі.

Також існує ефективна технологія Acronis Drive Snapshot, яка за допомогою робочої станції Acronis True Image робить резервну копію даних не вимикаючи або перезапускаючи саму робочу станції, що дозволить не припиняти роботу персоналу. Якщо Acronis True Image створював резервні копії файлів по одному, то відкритий файл, швидше за все, буде змінено з моменту початку резервного копіювання, а потім збережено в резервній копії в інший момент часу і дані в резервній копії будуть суперечливими. Для усунення цього Acronis True Image створює так званий знімок, який фіксує дані для резервного копіювання до певного моменту часу.

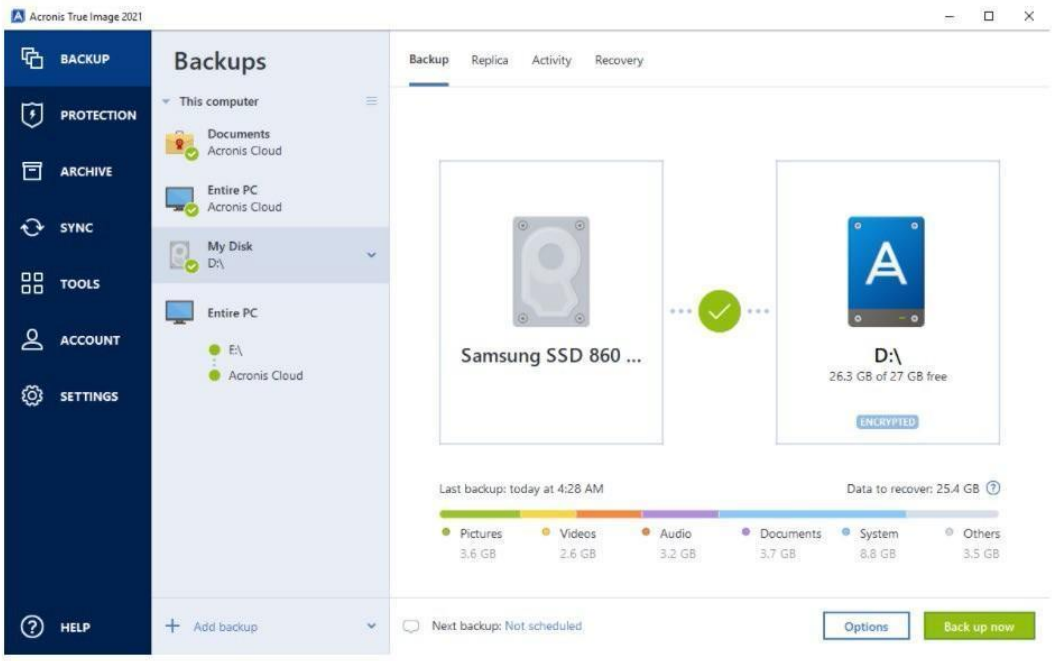

Рисунок 3.13 – Меню резервного копіювання в програмі Acronis True Image

Наступним кроком вибір параметри «New backup», тобто нового файлу

бекапу.

Щоб налаштувати програму Acronis True Image для створення резервної копії, слід виконати наступні кроки. У головному меню вибрати опцію "Резервне копіювання" та натиснути на "Змінити джерело". Далі потрібно вказати джерело для резервної копії, наприклад, "Диски та розділи", а потім обрати "Локальний диск (C/D/E:)", що є необхідним для створення копії. Крім того, можна вибрати опції "весь комп'ютер", "файли та папки", або "мобільний телефон/планшет". Додатково, є можливість обрати "весь комп'ютер", "файли та папки", "мобільний пристрій", і програма автоматично створить відповідні резервні копії.

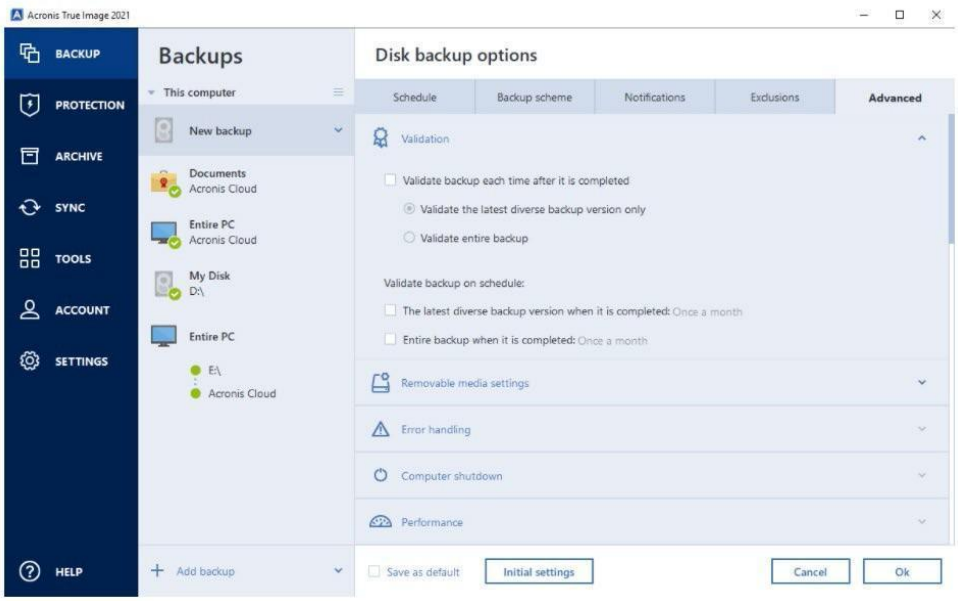

Рисунок 3.14 – Налаштування резервного копіювання Acronis True Image.

Далі треба вказати місце збереження резервної копії, натиснувши "Обрати місце збереження". Також є можливість використовувати хмарне сховище Acronis Cloud або зовнішній жорсткий диск. Під час вибору дисків для резервного копіювання слід увімкнути "Повний список розділів". Також треба відзначити зарезервований системою диск, такий як "Диск бекапу", щоб усі дані зберігалися саме на цьому диску. Після цього можна перейти до створення резервної копії, натиснувши "Створити копію".

Після виконання цих кроків створена резервна копія диску, і в будь-який момент можна повернутися до неї за необхідності.

ВИСНОВКИ

У ході дослідження було розглянуто теоретичні аспекти систем захисту інформаційних ресурсів, що включають основні поняття інформаційної безпеки та класифікацію загроз. Були детально проаналізовані архітектура систем захисту від шкідливого програмного забезпечення, а також принципи та методи захисту інформації.

Особлива увага була приділена технологіям захисту від шкідливого програмного забезпечення, включаючи сутність антивірусного захисту та його основні характеристики. Було розглянуто різні технології розпізнавання та блокування шкідливих програм, а також методи оновлення баз даних антивірусних програм, що є надзвичайно важливими для забезпечення актуальності та ефективності захисних систем.

Практична частина роботи присвячена системі захисту інформаційних ресурсів від шкідливого програмного забезпечення. Були описані фізичні, апаратні та програмні засоби, що використовуються для захисту інформаційних ресурсів. Проведено дослідження системи захисту, що дозволило виявити її сильні та слабкі сторони, а також розробити рекомендації щодо її вдосконалення.

Загалом, результати дослідження демонструють, що ефективна система захисту інформаційних ресурсів повинна включати комплексний підхід, що поєднує фізичні, апаратні та програмні засоби захисту. Постійне оновлення та вдосконалення антивірусних програм, а також використання сучасних технологій розпізнавання та блокування шкідливих програм є ключовими елементами забезпечення надійної інформаційної безпеки.

Важливим аспектом є також постійний моніторинг та аналіз нових загроз, що дозволяє своєчасно реагувати на них та вживати необхідних заходів для їх нейтралізації. Таким чином, системи захисту інформаційних ресурсів повинні бути динамічними та здатними адаптуватися до змін у середовищі загроз, забезпечуючи безперервність бізнес-процесів та захист конфіденційної інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Шемчук, В. В. Загрози інформаційній безпеці: проблеми визначення та подолання. *Експерт: парадигми юридичних наук і державного управління*, 2020. №(1(7), 285-296.
2. Шемчук В. В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктрини й законодавчої основи. *Теорія та історія держави і права; історія політичних і правових учень*, 2019.Том 30 (69) № 4. С. 31-37.
3. Харченко С. О. Наукові підходи до класифікації загроз інформаційній безпеці. *Державне управління*, 2019. № 2 (66). С. 191-197.
4. Методологічні аспекти забезпечення інформаційної безпеки підприємства / П. А. Фісуненко, О. І. Судакова, С. В. Деркач, Є. О. Притуляк // *Східна Європа: економіка, бізнес та управління*, 2019. № 23. С. 426-431.
5. Бараннік В. В. Архітектурні особливості систем захисту веб-ресурсів від несанкціонованого доступу / В.В. Бараннік, О.В. Слободянюк, Н.В. Бараннік // НІСТ'2019. Наукоємні технології в інфокомунікація : матеріали III Міжнар. наук.-практ. конф. Харьков. 2019. С.45-46.
6. Архітектура сфери захисту інформації та інформаційної безпеки. URL: https://salo.li/d587Cf7
7. Основні дії для захисту персональних комп’ютерів від шкідливого програмного забезпечення. URL: https://ua5.org/protect/2146-osnovni-diyi-dlya-zahystu-personalnyh-kompyuteriv-vid-shkidlyvogo-programnogo-zabezpechennya.html
8. Карпович І. М., Гладка О .М., Наконечна Ю. А. Аналіз ризиків безпеки інформаційної системи іт-підприємства. *Таврійський національний університет Імені в.І. Вернадського*. Технічні науки, 2020. Том 31 (70) № 5. С. 69-74.
9. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – Київ: Видавництво НА СБ України, 2020. 256 с.

10. Мельник І. Розробка макросу та дослідження шифру Віженера та його модифікації. Вінницький національний аграрний університет. *Журнал студентських наукових праць*, 2022. №5. С. 256-253.
11. Костюк К. О. Дослідження криптографічних протоколів захисту інформації в мережі Інтернет. Тернопіль: ТНТУ, 2023. 63 с.
12. Інформаційна безпека: види загроз і методи їх усунення. URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/
13. Моделі і методи захисту від загрозливих програм інформаційних систем / В. М. Джулій, В. О. Бойчук, В. Ю. Тітова, О. В. Сєлюков, О. В. Мірошніченко // Зб. наук. праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ : ВІКНУ, 2020. Вип. 67. С. 72–84.
14. Free and Open Source Software : матеріали XV Міжнар. наук.-практ. конф., м. Харків, 13-14 лютого 2024 р. Харків: Харківський національний економічний університет імені Семена Кузнеця, 2024. 148 с.
15. Балакін С. В. Застосування штучних імунних систем при виявленні шкідливих програм в комп'ютерній мережі. *Проблеми інформатизації та управління*, 2017. №1-2(57-58). С. 7-11.
16. Фільтри веб-сервера. URL: https://javarush.com/ua/quests/lectures/ua.questservlets.level12.lecture05
17. Гавриш Б. М., Тимченко О. В., Борзов Ю. О. Класифікація шкідливого програмного забезпечення та основні методи захисту. *Комп'ютерні технології друкарства*, 2022. №2 (48). С. 142-154.
18. Безверхня Ю. В. Хеджування як елемент управлінського обліку. *Сучасні проблеми обліку, аналізу, аудиту й оподаткування суб'єктів господарської діяльності: теоретичні, практичні та освітянські аспекти* : зб. наук. праць за матеріалами IV Всеукр. наук.-практ. конф. 30-31 березня 2020 р. С. 17-20.
19. Антоненко Н., Дігтяр Я., Крикун Н. Сучасні методи боротьби з комп'ютерними вірусами. *Економіка та суспільство*, 2022. №43. URL: https://www.economyandsociety.in.ua/index.php/journal/article/view/1739/1674

20. Історія антивірусного програмного забезпечення огляд ключових етапів. URL: http://surl.li/tucxk