Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“____” _____ 2025 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“Дослідження та програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси”

Виконав здобувач вищої освіти
ІІ курсу, групи КН-24М
ОПП «Комп’ютерні науки»
спеціальності 122 «Комп’ютерні науки»
_____ Кіріченко Т.М.
«____» _____ 2025 р.

Керівник проекту
доктор філософії (PhD)
_____ Дрєєва Г.М.
«____» _____ 2025 р.
Рецензент _____
_____

м. Кропивницький

АНОТАЦІЯ

Кіріченко Т.М. Дослідження та програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси. 122 Комп'ютерні науки. Центральноукраїнський національний технічний університет. Кропивницький. 2025.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи нейромережевих експертів безпечної маршрутизації у антивіруси.

Метою розробки є дослідження та програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси.

Об'єктом дослідження є процес нейромережевих експертів безпечної маршрутизації у антивіруси.

Предметом дослідження є методи нейромережевих експертів безпечної маршрутизації у антивіруси.

Методи дослідження базуються на методах штучного інтелекту, методах комп'ютерних мереж, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі Python.

Ключові слова: комп'ютерні науки, нейрона мережа, маршрутизація, антивірус

ABSTRACT

Kirichenko T.M. Research and software implementation of the system of neural network experts for secure routing in antiviruses. 122 Computer Science. Central Ukrainian National Technical University. Kropyvnytskyi. 2025.

In this final qualification work for the second (master's) level of higher education, software has been developed, which is intended for the system of neural network experts for secure routing in antiviruses.

The purpose of the development is the research and software implementation of the system of neural network experts for secure routing in antiviruses.

The object of the research is the process of neural network experts for secure routing in antiviruses.

The subject of the research is the methods of neural network experts for secure routing in antiviruses.

The research methods are based on artificial intelligence methods, computer network methods, information protection methods, mathematical statistics methods, software development methods.

The result of the work is a software implementation of a neural network expert system for secure routing in antiviruses.

In the process of working on the software model, an analysis of existing hardware and software was performed. All components of the developed software are fully described.

A convenient user interface has been developed. Instructions for working with the software are provided.

The program can be used on a PC with Windows 10/11 OS.

The program was developed in the Python environment.

Keywords: computer science, neural network, routing, antivirus

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ІБ	–	інформаційна безпека
ТКС	–	телекомунікаційна система
КМ	–	комп’ютерна мережа
КСАЗ	–	комплексна система антивірусного захисту
МЕ	–	міжмережний екран
ПЗ	–	програмне забезпечення
ПК	–	персональний комп’ютер
ACL	–	Access Control List
FTP	–	File Transfer Protocol
http	–	HyperText Transfer Protocol
POP3	–	Post Office Protocol Version 3
SMTP	–	Simple Mail Transfer Protocol
VLAN	–	Virtual Local Area Network

ВСТУП

Актуальність теми. Випереджати кіберзагрози з огляду на значне зростання кіберзлочинності – це постійний виклик. Зустрічайте хмарний антивірус, який змінює правила гри в кібербезпеці. Але що відрізняє його від традиційних антивірусних рішень і чому він стає вибором як для приватних осіб, так і для бізнесу?

Хмарний антивірус являє собою сучасний зсув у кібербезпеці, переносячи важку обробку даних з вашого пристрою на потужні віддалені сервери. На відміну від традиційного антивірусного програмного забезпечення, яке зберігає всі дані локально, хмарний антивірус працює переважно через сервери, підключені до Інтернету, що значно зменшує навантаження на вашу систему.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем нейромережевих експертів безпечної маршрутизації у антивіруси.

– Дослідження системи нейромережевих експертів безпечної маршрутизації у антивіруси.

– Програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси.

Об'єктом дослідження є процес нейромережевих експертів безпечної маршрутизації у антивіруси.

Предметом дослідження є методи нейромережевих експертів безпечної маршрутизації у антивіруси.

Методи дослідження базуються на методах штучного інтелекту, методах комп'ютерних мереж, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод нейромережевих експертів безпечної маршрутизації у антивіруси.

– Розроблено вітчизняний продукт нейромережевих експертів безпечної маршрутизації у антивіруси, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі нейромережевих експертів безпечної маршрутизації у антивіруси.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Робота апробована на LVII Науково-технічній конференції здобувачів вищої освіти LV науково-технічної конференції «Наука в ЦНТУ: основні досягнення та перспективи розвитку» (2025 р.), основні положення випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти надруковані у статті збірника праць молодих науковців ЦНТУ, випуск №15.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Штучний інтелект (ШІ) революціонізував роботу антивірусного програмного забезпечення. Традиційне антивірусне програмне забезпечення покладалося на виявлення шкідливих програм на основі сигнатур, але з розвитком шкідливих програм цей підхід став менш ефективним. Натомість антивірусне програмне забезпечення на базі ШІ використовує алгоритми машинного навчання для виявлення та блокування шкідливих програм у режимі реального часу.

1. Атаки нульового дня

Однією з ключових переваг антивірусного програмного забезпечення на базі штучного інтелекту є його здатність виявляти атаки нульового дня. Атаки нульового дня – це атаки, які використовують вразливості, що ще не були виявлені або виправлені постачальниками програмного забезпечення. Антивірусне програмне забезпечення на базі штучного інтелекту може ідентифікувати раніше невідоме шкідливе програмне забезпечення, аналізуючи його поведінку та виявляючи закономірності, що свідчать про зловмисні наміри.

2. Машинне навчання

Антивірусне програмне забезпечення на базі штучного інтелекту також може швидко адаптуватися до нових загроз. Алгоритми машинного навчання можуть аналізувати величезні обсяги даних та виявляти закономірності, що вказують на нові загрози, що дозволяє антивірусному програмному забезпеченню виявляти та блокувати нові загрози, щойно вони з'являються.

3. Автоматична реакція на загрози

Ще однією перевагою антивірусного програмного забезпечення на базі штучного інтелекту є його здатність автоматизувати процес реагування на

загрози. Коли загрозу виявляється, програмне забезпечення може вжити негайних заходів, таких як блокування файлу або програми, без необхідності втручання людини. Це може заощадити дорогоцінний час і ресурси, а також зменшити ризик пошкодження від атаки.

4. Продуктивність

Окрім своєї ролі у виявленні шкідливого програмного забезпечення, ШІ також може допомогти покращити продуктивність антивірусного програмного забезпечення. Алгоритми ШІ можуть аналізувати дані про продуктивність системи та виявляти можливості для оптимізації системних ресурсів, зменшуючи вплив антивірусного програмного забезпечення на продуктивність системи.

Роль штучного інтелекту в сучасному антивірусному програмному забезпеченні стає дедалі важливішою, оскільки середовище загроз продовжує розвиватися. Використовуючи алгоритми машинного навчання, антивірусне програмне забезпечення на базі штучного інтелекту може виявляти раніше невідоме шкідливе програмне забезпечення, зменшувати кількість хибнопозитивних результатів та автоматизувати процес реагування на загрози. Оскільки кібератак стає все більш витонченим, використання штучного інтелекту в антивірусному програмному забезпеченні буде важливим для забезпечення безпеки наших пристроїв і даних.

1.2 Область застосування

Областю застосування є хмарний антивірус. Він працює наступним чином. Процес елегантно простий, але водночас витончений:

1. Незначна місцева присутність:

– Невелика клієнтська програма встановлюється на ваш пристрій.

– Мінімальний вплив на системні ресурси.

– Безперервне підключення до хмарних серверів.

2. Процес інтелектуального виявлення:

– Файли миттєво порівнюються з гешами на наявність відомих загроз.

– Підозрілі файли аналізуються в безпечних хмарних середовищах.

– Розширений штучний інтелект та машинне навчання виявляють нові загрози.

3. Захист у режимі реального часу:

– Миттєві оновлення бази даних загроз.

– Поведінковий аналіз підозрілих файлів.

– Можливості виявлення загроз нульового дня.

Конфіденційність та безпека

Хоча хмарний антивірус надсилає дані на віддалені сервери, авторитетні постачальники впроваджують суворі заходи конфіденційності:

- Зашифрована передача даних.
- Аналіз анонімних файлів.
- Відсутність зберігання особистої інформації.
- Безпечна пісочниця для тестування підозрілих файлів.

Цей сучасний підхід забезпечує надійний захист без шкоди для продуктивності системи чи конфіденційності, що робить його дедалі популярнішим вибором як для особистого, так і для бізнес-користування.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти

У 2025 році ми ретельно протестували 39 антивірусних програм від 28 брендів. Щоб оцінити їхній захист, ми заразили нашу тестову систему 1200 зразками шкідливого програмного забезпечення, досліджуючи, наскільки добре кожне програмне забезпечення справляється з реальними загрозами.

Крім того, ми провели глибоке дослідження основних функцій безпеки, таких як брандмауери, менеджери паролів, інструменти захисту від фішингу, VPN тощо. На основі наших практичних тестів, ось найкращий антивірус на 2025 рік:

1. Антивірус Norton – №1 у 2025 році
2. Антивірус Avast
3. Антивірус TotalAV
4. Антивірус Bitdefender
5. Антивірус McAfee
6. Антивірус Panda
7. Антивірус Avira

Огляд Norton

1 місце з 28 антивірусів

Norton посідає перше місце серед 28 антивірусних брендів.

Norton – найкращий антивірус 2025 року. Він має ідеальний захист від шкідливих програм, не впливає на швидкість вашого ПК, має всі необхідні функції безпеки та чудову ціну.

Купуйте його, якщо хочете повного захисту. Ви отримаєте чудовий захист

від шкідливого програмного забезпечення, антифішингу, брандмауер, менеджер паролів та необмежений VPN, які захистять вашу конфіденційність в Інтернеті:

– Захист від шкідливого програмного забезпечення: 100%. Norton виявив та видалив кожен із 1200 зразків шкідливого програмного забезпечення в нашому тесті.

– Вплив на швидкість: 100%. Антивірусний механізм Norton є легким і не уповільнював наш тестовий ПК.

– Функції: 100% Norton включає захист від шкідливих програм, захист від фішингу, брандмауер, VPN, менеджер паролів та багато іншого .

– Ціна: 100%. Порівняно з аналогічними продуктами Bitdefender та McAfee, Norton пропонує краще співвідношення ціни та якості.

Спробуйте без ризику завдяки політиці повернення протягом 60 днів.

Огляд Avast

2 місце з 28 антивірусів

Avast посідає 2 місце серед 28 антивірусних брендів.

Avast – один із найкращих антивірусів 2025 року. Він має ідеальний захист від шкідливого програмного забезпечення, не впливає на швидкість вашого ПК, має багато функцій безпеки та один із найкращих дизайнів, які ми бачили.

Купуйте його, якщо вам потрібен відмінний захист і чудовий дизайн. Ви отримаєте захист від шкідливого програмного забезпечення, захист від фішингу, брандмауер і VPN. Однак Avast не включає менеджер паролів:

– Захист від шкідливого програмного забезпечення: 100%. Avast виявив та видалив усі 1200 зразків шкідливого програмного забезпечення в нашому тесті.

– Вплив на швидкість: 100%. Антивірусний рушій Avast легкий і не уповільнював наш тестовий ПК.

– Функції: 80%. Avast one включає захист від шкідливих програм, фішинг, брандмауер, VPN та багато іншого . Але немає менеджера паролів.

– Ціна: 100%. Враховуючи чудові функції безпеки та дизайн Avast, його ціна більш ніж справедлива.

Спробуйте без ризику завдяки 30-денній політиці повернення.

Огляд TotalAV

3 місце з 28 антивірусів

TotalAV посідає 3 місце серед 28 антивірусних брендів.

TotalAV – один із найкращих антивірусів 2025 року. Він має майже ідеальні результати тестів на захист від шкідливого програмного забезпечення, інтуїтивно зрозумілий дизайн, не впливає на швидкість вашого ПК та має безліч функцій безпеки.

Купуйте його, якщо вам потрібен простий у використанні антивірус за чудовою ціною. Ви отримаєте захист від шкідливих програм, антифішингу, менеджер паролів і VPN, які захистять вашу конфіденційність в Інтернеті. Але без брандмауера:

– Захист від шкідливого програмного забезпечення: 99,8%. TotalAV виявив та видалив майже всі з 1200 зразків шкідливого програмного забезпечення в нашому тесті.

– Вплив на швидкість: 100%. Антивірусний рушій TotalAV легкий і не уповільнював наш тестовий ПК.

– Функції: 90%. TotalAV включає захист від шкідливого програмного забезпечення, захист від фішингу, VPN та менеджер паролів. Але не має брандмауера.

– Ціна: 90%. TotalAV пропонує щедрі знижки протягом першого року, але високі ціни на поновлення протягом другого року.

Спробуйте без ризику завдяки 30-денній політиці повернення.

Огляд Bitdefender

4 місце з 28 антивірусів

Bitdefender посідає 4 місце серед 28 антивірусних брендів.

Bitdefender – чудова антивірусна програма . Вона має ідеальний захист від шкідливих програм, не впливає на швидкість вашого ПК, має багато функцій безпеки та чудову ціну.

Купуйте його, якщо хочете отримати винятковий захист. Але пам’ятайте, що ви отримаєте захист від шкідливих програм, фішинг, брандмауер і кілька додаткових функцій. Не менеджер паролів чи безлімітний VPN:

– Захист від шкідливого програмного забезпечення: 100%. Bitdefender виявив та видалив кожен із 1200 зразків шкідливого програмного забезпечення в нашому тесті.

– Вплив на швидкість: 100%. Антивірусний рушій Bitdefender легкий і не уповільнював наш тестовий ПК.

– Функції: 80%. Bitdefender має захист від шкідливого програмного забезпечення, фішинг та брандмауер, але йому бракує менеджера паролів та VPN.

– Ціна: 100%. Хоча Bitdefender позбавлений кількох функцій, він має чудову ціну, що забезпечує йому гарне співвідношення ціни та якості.

Спробуйте без ризику завдяки 30-денній політиці повернення.

Огляд McAfee

5 місце з 28 антивірусів

McAfee посідає 5-те місце серед 28 антивірусних брендів.

McAfee – чудова антивірусна програма. Він має ідеальний захист від шкідливих програм, не впливає на швидкість вашого ПК, має інтуїтивно зрозумілий дизайн та всі необхідні функції безпеки.

Купуйте його, якщо хочете повного захисту. Ви отримаєте захист від шкідливого програмного забезпечення, фішинг, брандмауер, менеджер паролів, VPN та, залежно від місця вашого проживання, захист від крадіжки особистих даних:

– Захист від шкідливого програмного забезпечення: 100%. McAfee виявив та видалив кожен із 1200 зразків шкідливого програмного забезпечення в нашому тесті.

– Вплив на швидкість: 100%. Антивірусний механізм McAfee є легким і не уповільнював наш тестовий ПК.

– Функції: 100%. McAfee включає захист від шкідливих програм, захист від фішингу, брандмауер, VPN, менеджер паролів та багато іншого .

– Ціна: 90%. McAfee трохи дорожчий за Norton, але дозволяє захистити необмежену кількість пристроїв.

Спробуйте без ризику завдяки 30-денній політиці повернення.

Огляд Panda

6 місце з 28 антивірусів

Panda посідає 6-те місце серед 28 антивірусних брендів.

Panda – чудова антивірусна програма. Вона має майже ідеальний захист від шкідливих програм, не впливає на швидкість вашого ПК, має всі необхідні функції безпеки та гнучке ціноутворення.

Купуйте його, якщо вам потрібен чудовий захист та можливості налаштування. Ви отримаєте захист від шкідливого програмного забезпечення, захист від фішингу, брандмауер, менеджер паролів та необмежений VPN, які захистять вашу конфіденційність в Інтернеті:

– Захист від шкідливого програмного забезпечення: 99%. Panda виявила та видалила майже всі з 1200 зразків шкідливого програмного забезпечення в нашому тесті.

– Вплив на швидкість: 100%. Антивірусний механізм Panda є легким і не уповільнював наш тестовий ПК.

– Функції: 100% Panda Dome включає захист від шкідливого програмного забезпечення, захист від фішингу, брандмауер, VPN, менеджер паролів та багато іншого .

– Ціна: 80%. Порівняно з аналогічними продуктами Norton, Panda Dome дорогий. Однак його гнучке ціноутворення чудове.

Спробуйте без ризику завдяки 30-денній політиці повернення.

Огляд Avira

7 місце з 28 антивірусів

Avira посідає 7 місце серед 28 антивірусних брендів.

Avira – чудова антивірусна програма. Вона має ідеальний захист від шкідливих програм, не впливає на швидкість вашого ПК, має всі необхідні функції безпеки та чудовий дизайн.

Купуйте його, якщо вам потрібен чудовий захист та інтуїтивно зрозумілий дизайн. Ви отримаєте захист від шкідливих програм, антифішинг, менеджер паролів та VPN. Крім того, Avira нарешті включає чудовий брандмауер:

– Захист від шкідливого програмного забезпечення: 100%. Avira виявила

та видалила всі 1200 зразків шкідливого програмного забезпечення в нашому тесті.

– Вплив на швидкість: 100%. Антивірусний механізм Avira легкий і не уповільнював наш тестовий ПК.

– Функції: 100%. Avira включає захист від шкідливих програм, захист від фішингу, брандмауер, VPN, менеджер паролів та багато іншого .

– Ціна: 90%. Avira має чудову ціну. Але з Norton ви отримаєте кілька додаткових функцій за ті ж гроші.

Спробуйте без ризику завдяки політиці повернення протягом 60 днів.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python – це потужна мова програмування, яка проста у вивченні. Він має ефективні структури даних високого рівня та простий, але ефективний підхід до об'єктно-орієнтованого програмування. Елегантний синтаксис і динамічна типізація Python разом з його інтерпретованим характером роблять його ідеальною мовою для створення сценаріїв і швидкої розробки додатків у багатьох сферах на більшості платформ.

Інтерпретатор Python і обширна стандартна бібліотека доступні у вихідному або двійковому вигляді для всіх основних платформ на веб-сайті Python https://www.python.org/ і можуть вільно поширюватися. Цей же сайт також містить дистрибутиви та вказівники на багато безкоштовних сторонніх модулів Python, програм і інструментів, а також додаткову документацію.

Інтерпретатор Python легко розширюється за допомогою нових функцій і типів даних, реалізованих у C або C++ (або інших мовах, які можна викликати з C). Python також підходить як мова розширення для налаштовуваних програм.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за другим (магістерським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи нейромережевих експертів безпечної маршрутизації у антивіруси.

В процесі розробки випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти необхідно виконати наступний обсяг роботи:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформувати висновки про виконаний обсяг робіт та одержані результати.

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Алгоритми формування множини маршрутів передачі геш-файлу метаданих у хмарні антивірусні системи

Аналіз процесу функціонування телекомунікаційної системи, а також дослідження процесів формування, передачі й обробки метаданих у хмарних антивірусних системах [7, 9], дозволили визначити щільність розподілу ймовірностей часу передачі геш-файлу метаданих у хмарні антивірусні системи, а також обробки й доставки команд передачі керування, сформувати й математично формалізувати знання про зміни й характер поводження основних ймовірносно-часових показників якості обслуговування в телекомунікаційній системі.

Обмін метаданими між програмним клієнтом і сервером, у загальному випадку, здійснюється через транзитні маршрутизатори, послідовність яких на шляху від відправника до одержувача в рамках дипломної роботи визначимо як маршрут [13].

Нехай $\Re = \{V_n \mid n \in 1, N\}$ – безліч маршрутизаторів у ТКС, V_n – n-й маршрутизатор, $N = |\Re|$ – число маршрутизаторів, $\Im = \{\theta_\xi \mid \xi \in 1, \Theta\}$ – безліч каналів зв'язку в ТКС, де θ_ξ – ξ-й канал зв'язку, Θ – кількість каналів зв'язку в ТКС, $|Z|$ – потужність множини *Z*.

Інформаційні пакети метаданих для аналізу програмному серверу можуть бути передані по одному з маршрутів, що становлять безліч $\aleph = \{\eta_s \mid s \in 1, M\}$, де $\eta_s = \{\theta_{s,c} \mid \theta_{s,c} \in \Im; \quad c \in 1, \Theta\}$ – s-*й* маршрут, $s \in 1, M$, $|\eta_s| = \Psi_s$, M – кількість

маршрутів, $\theta_{s,c}$ – канал зв'язку з номером *з*, що належить s-*му* маршруту, Ψ_s – кількість каналів зв'язку на s-*м* маршруті.

Формування множини $\aleph$ маршрутів являє собою складний ітераційний процес, що складається у виконанні декількох алгоритмів:

– алгоритм пошуку найкоротших шляхів між вузлами в ТКС;

– алгоритм формування базової множини маршрутів передачі метаданих;

– алгоритм безпечної маршрутизації на базовій множини шляхів передачі метаданих у програмний сервер.

Початок роботи з хмарним антивірусом зазвичай простий. Ось загальний огляд кроків налаштування. Пам’ятайте, що точні кроки та інтерфейс можуть дещо відрізнятися залежно від обраного вами постачальника.

1. Встановлення:

– Завантаження: Відвідайте веб-сайт та завантажте інсталяційний файл. *Ніколи не завантажуйте програмне забезпечення з неофіційних джерел.*

– Запустіть інсталятор: знайдіть завантажений файл (зазвичай це.exe або.dmg) і двічі клацніть його, щоб розпочати інсталяцію.

– Налаштування облікового запису: Вам, ймовірно, буде запропоновано створити обліковий запис або увійти, якщо він у вас вже є. Це часто необхідно для керування підпискою та доступу до функцій.

2. Початкова конфігурація (зазвичай автоматична):

Більшість хмарних антивірусних рішень розроблені для ефективної роботи з налаштуваннями за замовчуванням. Зазвичай автоматично вмикаються такі параметри:

– Захист у режимі реального часу : цей захист постійно контролює вашу систему на наявність загроз.

– Хмарне сканування : це дозволяє програмному забезпеченню надсилати файли до хмари для аналізу.

– Автоматичні оновлення : це гарантує, що ваш антивірус завжди оновлений найновішими визначеннями загроз.

3. Додаткове налаштування (за потреби):

Після початкового налаштування ви можете ознайомитися з деякими додатковими параметрами:

– Планування сканування: налаштуйте регулярне сканування, щоб автоматично перевіряти систему на наявність загроз у певний час.

– Інтенсивність сканування: Деякі програми пропонують різні рівні сканування (наприклад, швидке сканування, повне сканування). Повне сканування перевіряє всі файли, але займає більше часу.

– Захист веб-сайту: налаштуйте параметри, пов’язані з блокуванням шкідливих веб-сайтів та спроб фішингу.

– Виключення файлів: Якщо у вас є певні файли або папки, яким ви довіряєте та не хочете, щоб їх сканували (наприклад, файли розробки), ви можете додати їх до списку виключень. *Використовуйте цю функцію обережно.*

4. Перевірка та тестування:

– Запустіть ручне сканування: виконайте повне сканування системи, щоб переконатися, що все працює правильно.

– Перевірте стан захисту: знайдіть видимий значок у системному треї або області сповіщень, який вказує на активність захисту в режимі реального часу.

– Тестування оновлень: Перевірте наявність оновлень вручну, щоб підтвердити, що функція оновлення працює.

Поради професіоналів для оптимальної продуктивності:

– Стабільне інтернет-з’єднання: Хмарний антивірус потребує інтернет-з’єднання для сканування. Переконайтеся, що у вас стабільне з’єднання для найкращої продуктивності.

– Час початкового сканування: Запуск повного сканування системи може зайняти деякий час, якщо ви активно не використовуєте комп’ютер.

Більшість хмарних антивірусних програм розроблені з урахуванням зручності використання та вимагають мінімального налаштування. Налаштування за замовчуванням часто забезпечують достатній захист для більшості

користувачів. Якщо ви не впевнені щодо будь-яких налаштувань, зазвичай краще залишити їх як є. Зверніться до документації або ресурсів підтримки вашого постачальника антивірусної програми, якщо у вас є особливі потреби або виникли проблеми.

3.2 Розробка структурної схеми

Хмарні антивірусні рішення – це ті, що зберігають інформацію про варіанти шкідливого програмного забезпечення в хмарі, а не на пристрої користувача. Традиційні, так звані «спискові» антивірусні рішення зберігають списки відомих шкідливих фрагментів коду на самому пристрої, що може негативно вплинути на продуктивність машини.

Щоб краще зрозуміти хмарне антивірусне програмне забезпечення, вам допоможе розуміння терміну «хмара». Хмара – це просто децентралізований простір для зберігання даних, до яких ваш комп'ютер має доступ через Інтернет.

Наше хмарне антивірусне програмне забезпечення захищає вас або ваш бізнес, взаємодіючи з базою даних загроз, яка зберігається не на вашому комп'ютері, а в хмарі.

Як працює хмарний антивірус

Зберігаючи визначення загроз (файли, класифіковані як шкідливі програми або небезпечні IP-адреси та URL-адреси) у хмарі, а не на самому пристрої, хмарне антивірусне програмне забезпечення не потребує зберігання всіх цих мільйонів визначень на власному жорсткому диску, звільняючи місце.

А оскільки оновлення можна надсилати до вашого антивірусного програмного забезпечення віддалено через хмару, ви не будете змушені мати статичний список загроз, від яких програмне забезпечення знає, що його потрібно захищати. Щойно нові загрози виявляються, наприклад, командою дослідників загроз, які підтримують ваше антивірусне програмне забезпечення, оновлення може бути розповсюджено на всі пристрої, які його використовують. Це

забезпечує захист майже в режимі реального часу від постійно мінливого ландшафту загроз, що існує в Інтернеті.

Переваги хмарних антивірусних рішень:

– Доступ до більшої бази даних загроз без необхідності зберігати її на жорсткому диску

– Менший інсталяційний агент для вашого антивірусного програмного забезпечення, тому він займає менше місця

– Оновлення визначень майже в режимі реального часу на основі даних, зібраних з усієї мережі користувачів

Існуючий каталог поліморфного шкідливого програмного забезпечення, фішингу нульового дня та аналогічних загроз, що розвиваються, є величезним. Розміщення такої величезної кількості даних на одному комп'ютері знизить продуктивність до такої міри, що комп'ютер стане практично непрацездатним під час сканування.

На щастя, значні досягнення у хмарних обчисленнях відбулися на початку нового тисячоліття. Ті компанії, які змогли використати можливості хмари для антивірусного програмного забезпечення, чекали суттєвих покращень швидкості та продуктивності. Менші агенти встановлення означали менше часу та місця, що використовуються під час встановлення. Менша кількість визначень, що зберігаються на пристрої, почала означати менше або взагалі відсутність перерв для планового сканування.

Окрім зменшення навантаження на сховище окремих пристроїв, оновлення визначень – ці виправлення курсу, додані до програмного забезпечення для захисту від нещодавно виявлених загроз – займають лічені хвилини, а не дні чи тижні, які можуть знадобитися для створення тих самих оновлень без допомоги хмари. Якщо вам коли-небудь доводилося чекати, поки ваш комп'ютер оновиться, ви знаєте, як це розчаровує. Не кажучи вже про загрози, з якими ви могли зіткнутися в проміжку між оновленнями версій.

Хмарний антивірус для бізнесу

Хмарні антивірусні рішення не менш важливі для бізнесу, ніж для домашніх користувачів. Навпаки, під час встановлення засобів захисту кінцевих точок на велику кількість пристроїв, повільна інсталяція, спричинена великими агентами, характерними для традиційних антивірусних рішень, може значно збільшитися.

Крім того, хмарний антивірус для бізнесу гарантує, що кожен пристрій буде захищено від нових загроз лише за кілька хвилин після їх виявлення будь-якою захищеною кінцевою точкою, у всьому світі, без ручних оновлень чи інших перерв у роботі.

Структурна схема системи представлена на рис. 3.1.

Для нормального функціонування системи нейромережевих експертів безпечної маршрутизації необхідно підготувати й систематизувати дані, на основі яких виробляється навчання його окремих нейромережевих компонентів. Для рішення цього завдання блок формування навчальної й тестової вибірки формує дані для навчання нейронної мережі, упорядковує й організує з метою забезпечення можливості їхньої подальшої обробки за допомогою нейромережевих технологій.

Цей етап роботи алгоритму є одним з найбільш важливих, тому що дозволяє реалізувати в сукупності нейронних мереж здатність до узагальнення. Вхідні дані, необхідні для виконання своїх функцій даним блоком, і спосіб їхнього одержання для формування навчальної й тестової множини асоціативної машини формуються відповідно до принципів, наведених вище.

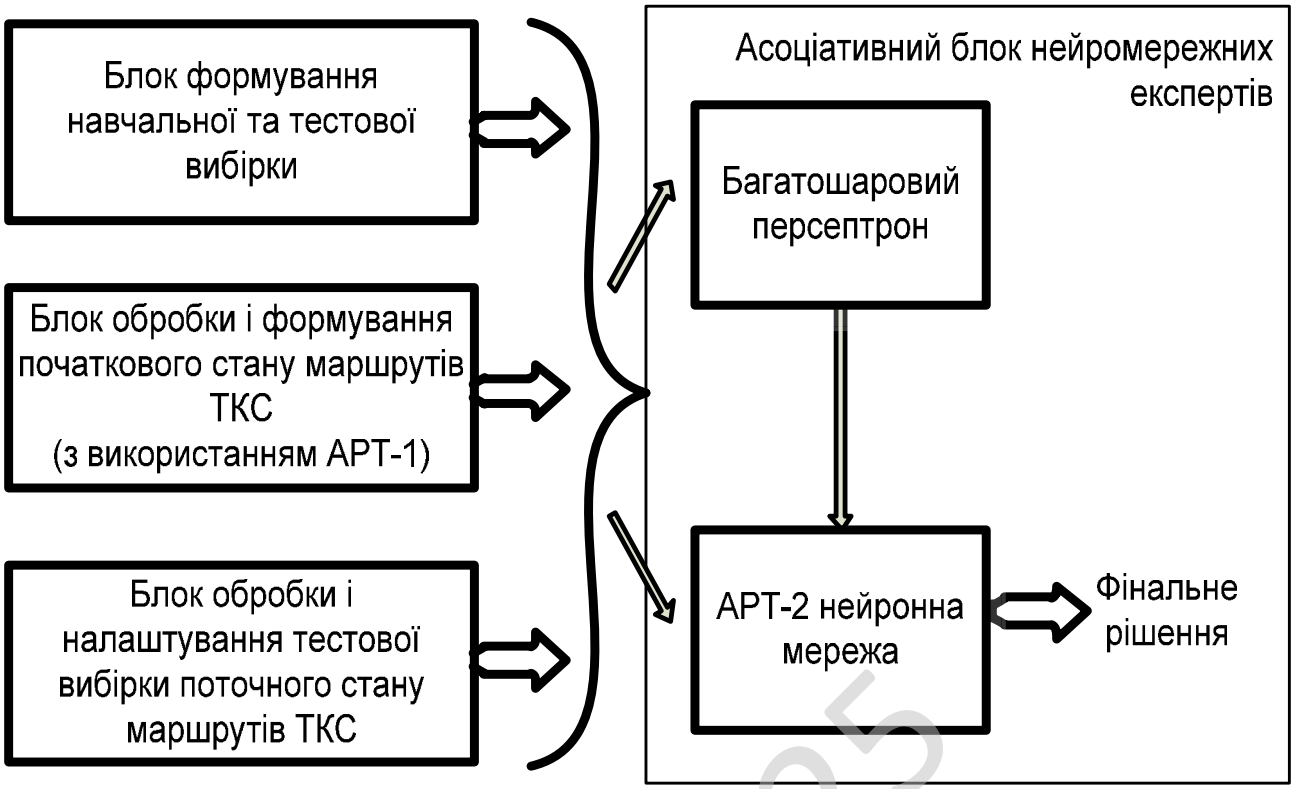

Рисунок 3.1 – Структурна схема системи

Блок обробки й формування початкового стану маршрутів ТКС формує значення параметрів всієї системи перед початком її навчання. Якщо змінні навчальної системи, що налаштовується, ініціалізувати таким чином, щоб вони були наближені до оптимальних значень, то процедура навчання буде зведена до «підстроювання» моделі. Синтез оптимального алгоритму ініціалізації значно скоротить час навчання нейромережевих експертів.

У якості алгоритму початкової установки параметрів запропонований кооперативний імунний алгоритм із генерацією рішень на основі процедури генетичного пошуку з використанням нейронної мережі АРТ-1.

У загальну структуру блоку нейромережевих експертів доцільно включити блок обробки й налаштування тестової вибірки поточного стану маршрутів ТКС, що виконує адаптацію компонентів нейронної мережі для рішення поставленого завдання. У дипломній роботі процедура навчання здійснювалася для всіх нейронних мереж по алгоритмах, адаптованим до їх архітектурам.

Антивірус на основі агента

Антивірусний агент розгортається на кожній віртуальній машині в рамках проекту та взаємодіє з модулем на гіпервізорі. Це створює споживання обчислювальних ресурсів, що робить цей підхід неефективним у великих масштабах.

Безагентний антивірус

Безагентний підхід базується на використанні Virtual Security Appliance (VSA) для сканування файлів, до яких мають доступ віртуальні машини, та Network Security Appliance (NSA) для сканування мережевого трафіку між віртуальними машинами, розташованими на хості. На жаль, лише VMware, Citrix та Microsoft підтримують VSA та NSA.

Ці рішення використовують потужність гіпервізора для зменшення навантаження на віртуальні машини, спричиненого звичайними антивірусними програмами. Однак вони мають кілька обмежень, пов'язаних із виявленням атак нульового дня:

– Антивірус, навіть оснащений евристичним механізмом, у більшості випадків не виявляє невідоме шкідливе програмне забезпечення нульового дня. Щоб уникнути виявлення, сучасні платформи кібершпигунства, такі як EquationDrug, що використовуються Regin та Epic Turla APT, використовують драйвер руткіту в режимі ядра, щоб приховати свої файли, ключі реєстру та процеси, перехоплюючи деякі функції Native API.

– Розширене шкідливе програмне забезпечення може знешкодити антивірус після виявлення на цільовій машині.

– Хмара в багатьох випадках є гетерогенним (гібридним) середовищем, побудованим на різних операційних системах та гіпервізорах, що збільшує витрати на розгортання та експлуатацію, а також робить ваш захист негнучким та залежним від постачальника.

Не рекомендуємо значних інвестицій у захист від шкідливого програмного забезпечення на вузлах. Достатньо правильно налаштувати вбудований

брандмауер Linux, використовувати розумну політику контролю доступу (логіни/паролі, ключі SSH тощо) та розгорнути NGFW або IDPS для моніторингу мережевого трафіку. Для розширеного захисту від атак нульового дня та цілеспрямованих атак використовуйте рішення на основі «пісочниці», куди можна завантажувати підозрілі файли та URL-адреси для аналізу.

Переваги хмарного антивіруса:

1. Мінімальний вплив на продуктивність пристрою: Хмарний антивірус використовує мінімальну кількість ресурсів пристрою, що забезпечує плавнішу роботу з комп'ютером без зниження продуктивності, спричиненого традиційним антивірусним програмним забезпеченням.

2. Оновлення в режимі реального часу та виявлення загроз: База даних виявлення загроз знаходиться в хмарі, що дозволяє їй отримувати миттєві оновлення для боротьби з новими загрозами в міру їх появи. Це гарантує захист вашої системи від найновіших вірусів та шкідливих програм без необхідності ваших дій.

3. Швидше сканування: Сканування хмари на наявність загроз дозволяє швидше проводити аналіз, скорочуючи час взаємодії з системою. Це дозволяє швидше проводити перевірки з використанням найсучасніших заходів безпеки.

4. Використовує колективний інтелект: Хмарний антивірус використовує комплексну мережу інформації про загрози, навчаючись на основі даних, зібраних від усіх користувачів. Це колективне розуміння робить антивірус розумнішим та ефективнішим у виявленні та нейтралізації нових загроз.

Хоча хмарний антивірус пропонує чудовий захист, пам'ятайте про такі фактори:

1. Залежність від Інтернету:

– Для оптимальної роботи потрібне стабільне з'єднання

– Розгляньте можливості захисту в автономному режимі

2. Вплив на продуктивність:

– Можливі незначні затримки сканування.

– Мінімальне використання локальних ресурсів порівняно з традиційним антивірусом.

З появою генеративного штучного інтелекту та його впливом на автоматизацію безпеки, хмарні загрози розвиваються. Поява Інтернету речей (IoT) принесла підприємствам численні інноваційні можливості, але також принесла безпрецедентні ризики. Ми також повинні враховувати геополітичні зрушення, зміну динаміки ринку та економічного ландшафту. Усі ці сфери впливають на кібербезпеку та її зростання.

Кіберстійкість більше не є необов'язковою; вона стає обов'язковою, оскільки організаціям потрібно йти в ногу зі зміною темпів загроз. Зловмисники стають креативними у способах здійснення атак і можуть саботувати бізнес-операції, руйнуючи ланцюжки створення вартості за лічені секунди.

Генеративний штучний інтелект може створювати дипфейки, маніпулювати даними та розробляти спеціалізовані схеми соціальної інженерії. Підприємства не можуть уникнути цих загроз або впоратися з ними, використовуючи звичайні заходи безпеки. Для ефективної боротьби з ними їм потрібні складні засоби захисту, включаючи прогнозну розвідку загроз. Кібербезпека та хмарна безпека – це два різні типи цифрової безпеки. Обидва є критично важливими. У цьому блозі ми обговоримо відмінності між хмарною безпекою та кібербезпекою, щоб ви могли вирішити, як ефективно поєднати обидва.

Що таке хмарна безпека?

Хмарна безпека – це розділ кібербезпеки, який захищає клієнтів, постачальників хмарних послуг та організації. Вона забезпечує конфіденційність та безпеку даних клієнтів. Хмарна безпека ідеально підходить для організацій, які розміщують конфіденційні цифрові активи в хмарі. З початку пандемії COVID-19 більшість організацій перейшли на моделі віддаленої роботи.

Хмарна безпека захищає користувачів хмари, їхні облікові записи, взаємодію та програми. Це модель спільної відповідальності, в якій клієнти

несуть відповідальність за завантаження та обмін своїми даними. Постачальник послуг зв'язку (CSP) відповідає за захист інфраструктури та встановлення виправлень, керування конфігурацією, фізичні хости та хмарні мережі.

Основні компоненти хмарної безпеки

Основні компоненти хмарної безпеки включають керування ідентифікацією та доступом (IAM), мережеву безпеку, безпеку даних, безпеку кінцевих точок та безпеку програм. Їх можна описати наступним чином:

– Безпека IAM: Компонент IAM безпеки хмари включає керування тим, хто має доступ до хмарних ресурсів, та діями, які вони можуть виконувати. Системи IAM керують ідентифікаторами користувачів, ведуть журнали аудиту та застосовують політики безпеки. Вони реалізують найменш привілейований доступ, розділяють обов'язки користувачів, виявляють незвичайну поведінку користувачів та виявляють ранні ознаки потенційних порушень безпеки.

– Мережева безпека: Мережева безпека поєднує системи виявлення вторгнень, системи запобігання вторгненням, віртуальні приватні мережі та брандмауери. Вона є критично важливою в хмарі, оскільки дані передаються від пристроїв до Інтернету.

– Безпека даних: Безпека даних – це компонент хмарних обчислень, який захищає дані під час передачі та в стані спокою. Він використовує різні заходи, такі як токенізація, шифрування, технології запобігання втраті даних та безпечне керування ключами. Контроль доступу та безпечні конфігурації також повинні застосовуватися до хмарних сховищ та баз даних.

– Безпека кінцевих точок : Багато організацій перейшли на моделі віддаленої роботи та запровадили політики «принеси свій власний пристрій» (BYOD) . Безпека кінцевих точок зосереджена на захисті пристроїв користувачів та кінцевих точок, які мають доступ до хмари або підключаються до неї. До них належать смартфони, планшети, ноутбуки, пристрої Інтернету речей, флеш-накопичувачі та інші портативні пристрої зберігання даних.

– Безпека додатків: Безпека додатків передбачає оптимізацію безпеки хмарних додатків. Вона захищає додатки від міжсайтового скриптингу, атак ін'єкцій та міжсайтових підробок. Вона включає сканування на вразливості, тести на проникнення, сканування інфраструктури як коду, сканування образів контейнерів та інші практики. Для додавання додаткових рівнів захисту вона також включає самозахист додатків під час виконання та брандмауери веб-додатків.

Кібербезпека – це акт і мистецтво захисту мереж, даних і пристроїв від несанкціонованого доступу та злочинного використання. Вона забезпечує дотримання практик, що забезпечують цілісність, конфіденційність та доступність інформації.

Кібербезпека захищає будь-які активи, підключені до Інтернету. Вона виходить за межі критичної інфраструктури, такої як електромережі, системи водопостачання чи будь-які апаратні рішення, що підключаються до Всесвітньої мережі. Кібербезпека гарантує безпеку ваших мереж від зовнішніх вторгнень.

Кожен бізнес повинен захищати свої дані. Цей захист не обмежується онлайн-системами; він може включати офлайн-системи та цифрові системи. Кібербезпека виходить за рамки традиційного розуміння, зосереджуючись на безпеці локальної інфраструктури та даних. Вона має спеціальні ресурси для розміщення ваших активів, мереж, пристроїв та систем.

Ключовим моментом є те, що кібербезпека може бути передбачуваною. Ви знаєте масштаб вашої інфраструктури, і зазвичай вона фіксована. Ви не можете раптово масштабувати своє підприємство, а мобільність обмежена, оскільки дані обмежені фізичними межами організації.

Основні компоненти кібербезпеки

Ось огляд основних компонентів кібербезпеки:

– Критична інфраструктура: вона слугує основою бізнес-операцій компанії. Ваша критична інфраструктура міститиме фізичні та мережеві

компоненти, такі як електричні мережі, телекомунікаційне обладнання, апаратне забезпечення тощо.

– Інтернет речей (IoT) : IoT – це мережа підключених пристроїв, що з'єднуються з хмарними екосистемами. Він є частиною кібербезпеки та включає принтери, сканери, датчики, камери та інше обладнання.

– Мережева безпека : Мережева безпека в контексті кібербезпеки включає брандмауери , поведінкову аналітику, засоби контролю доступу, антивірусне програмне забезпечення та засоби захисту від шкідливих програм.

– Навчання та обізнаність співробітників – це незначний, але водночас важливий компонент. Постійне навчання співробітників може допомогти вашим працівникам впроваджувати найкращі практики кібергігієни та знати, що робити, коли вони стикаються з онлайн-загрозами. Працівники повинні регулярно проходити навчання з розуміння тактик соціальної інженерії, створення надійних паролів та ознайомлення з політиками використання особистих пристроїв. Вони також повинні пам'ятати про політику «Принеси свій пристрій із собою» (BYOD) та боротися з тіньовими IT- загрозами.

Ось три критичні відмінності між хмарною безпекою та кібербезпекою.

1. Обсяг захисту

Кібербезпека захищає ваші мережі, обладнання, кінцеві точки та інші елементи вашої локальної інфраструктури. Хмарна безпека більше зосереджена на безпеці моделей хмарних сервісів, таких як IaaS, SaaS та PaaS. Вона використовує шифрування, керування ідентифікацією та доступом, а також безпечно налаштовує ваші хмарні ресурси.

2. Управління та розгортання

Рішення з кібербезпеки передбачають розгортання локально, що вимагає значних інвестицій у фізичну IT-інфраструктуру, апаратне забезпечення, пристрої та інші компоненти. Хмарні рішення безпеки більше базуються на програмному забезпеченні. Хмарні центри обробки даних поширені по всьому світу, і

постачальник відповідає за розміщення інфраструктури для надання хмарних послуг.

Підприємства повинні оформити підписку, щоб використовувати або орендувати ці інфраструктурні ресурси. Хмарне сховище та продуктивність чудові, і вони можуть знизити витрати на обладнання. Хмарна безпека пропонує максимальну гнучкість та масштабованість для підприємств, які бажають мобільного підходу до безпеки.

3. Типи атак

Традиційні загрози кібербезпеці включають програми-вимагачі, шкідливе програмне забезпечення, інсайдерські атаки, соціальну інженерію та фішинг. Загрози безпеці хмарних сервісів класифікуються як атаки SaaS-додатків, неправильні конфігурації робочого навантаження, незахищені API та витоки даних.

Організаціям доводиться вибирати між хмарною безпекою та кібербезпекою, залежно від налаштування своїх операцій, інфраструктури даних та пріоритетів безпеки. Хмарна безпека є критично важливою, якщо ваша організація значною мірою залежить від хмарних програм або послуг.

З іншого боку, кібербезпека є важливою для захисту локальних систем та активів, таких як локальні сервери, кінцеві точки та критична інфраструктура. Існує велика різниця між підходами до хмарної безпеки та кібербезпеки.

Галузі зі статичними середовищами даних або ті, що досі керують застарілими системами, такі як виробництво чи урядові організації, отримують велику користь від заходів кібербезпеки, які спрямовані на вирішення традиційних загроз, таких як шкідливе програмне забезпечення, програми-вимагачі та фішингові атаки.

Гібридні налаштування можуть вимагати балансу між обома, особливо зі зростанням впровадження хмарних технологій, але локальні системи залишаються невід'ємною частиною. Бізнеси, які переходять у хмару, повинні

забезпечити поступове зміщення акценту на безпеку для захисту як застарілих систем, так і нових хмарних платформ.

Зрештою, все зводиться до оцінки вразливостей та інвестування в безпеку. Незалежно від того, чи йдеться про захист динамічного середовища в хмарі, чи про фіксовану інфраструктуру локальних систем, зосередження на правильній області гарантує повний захист від загроз, що постійно змінюються.

Ось деякі варіанти використання хмарної безпеки та кібербезпеки . Давайте розглянемо, в яких галузях використовуються ці технології та якими способами:

– Індустрія фінансових послуг найбільше потребує найкращих рішень у сфері кібербезпеки. Фірми повинні шифрувати транзакції, захищати автентифікацію та захищати себе від шкідливого програмного забезпечення та фішингових інцидентів.

– Галузь охорони здоров'я може бути використана для крадіжки особистих даних, вимагання або шантажу. Зловмисники можуть погрожувати лікарням та захоплювати бази даних. Цей сегмент потребує кібербезпеки для швидкого реагування на загрози. Він підтримує всі системи в актуальному стані з використанням найновіших протоколів, механізмів передачі даних, алгоритмів шифрування тощо. Хмарні рішення безпеки оптимізують процес реєстрації пацієнтів та спрощують процес. Вони також можуть зберігати медичні записи та обмінюватися ними з лікарями, а також записуватися на прийом.

– Роздрібна торгівля та електронна комерція є популярним випадком використання кібербезпеки. Бренди повинні захищати номери кредитних карток клієнтів, паролі, облікові дані для входу та іншу конфіденційну інформацію. Компанії використовують рішення з кібербезпеки для запобігання несанкціонованому доступу та впроваджують надійну багаторівневу автентифікацію та шифрування.

– Хмарні рішення безпеки використовуються компаніями, що активно працюють на платформах соціальних мереж, для аналізу настроїв та запобігання

зловмисній поведінці. Це може допомогти виявити потенційних зловмисників та запобігти внутрішнім загрозам.

Вибір рішень для хмарної безпеки та кібербезпеки вимагає ретельного врахування потреб, бюджетів та ресурсів організації. По-перше, проаналізуйте свої бюджетні обмеження. Хмарні рішення для безпеки, часто на основі підписки, усувають необхідність інвестицій в обладнання та загалом знижують початкові витрати, пов'язані з такими покупками. З іншого боку, рішення для кібербезпеки можуть вимагати значних капітальних витрат на їх розгортання та подальше обслуговування, тому вони краще підходять для організацій з уже великим IT-бюджетом.

Географічне розташування також є фактором. Через масштабованість та мобільність глобальні організації з розподіленими командами частіше зосереджуються на хмарній безпеці. Водночас місцеві компанії зі стаціонарними операціями можуть більше використовувати традиційні заходи кібербезпеки для захисту локальних активів.

Інші вирішальні фактори включають розмір вашої команди та рівень досвіду. Невеликі або погано оснащені команди можуть побачити переваги хмарної безпеки, такі як керовані сервіси та просте налаштування. Однак більші компанії з великими IT-відділами можуть захотіти зберегти повний контроль над налаштуваннями та налаштуваннями, доступними за допомогою локальних рішень кібербезпеки.

Врахуйте свою поточну інфраструктуру та потреби щодо майбутньої масштабованості. Якщо ваша організація планує розширюватися, хмарні рішення є більш масштабованими та легшими для інтеграції з новими технологіями. З іншого боку, якщо ваша інфраструктура статична, а траєкторія зростання стабільна, традиційних інвестицій у кібербезпеку може бути достатньо.

Якщо раніше ви не могли вирішити між кібербезпекою та хмарною безпекою, тепер у вас є відповідь: вам потрібні обидві.

Хмарна безпека та кібербезпека стали важливими для захисту сучасних цифрових екосистем. У той час як хмарна безпека зосереджена на захисті хмарних середовищ та збереженні конфіденційності даних, кібербезпека захищає локальні системи та мережі. Будь-який з варіантів залежить від інфраструктури вашої організації, операційних потреб та траєкторії зростання. Зі зростанням кіберзагроз стає важливим знайти баланс, впроваджуючи хмарні та традиційні заходи безпеки.

Оцініть свої вразливості та співпрацюйте з перевіреними постачальниками, щоб розробити індивідуальну та стійку систему безпеки. Ви можете захистити свої активи та досягти довгострокового успіху за допомогою правильних інструментів.

3.3 Розробка функціональної схеми

Хмарний антивірус, що розроблений у результаті виконання дипломного проектування – захист вашого комп'ютера від шкідливих програм, що включає базові функції забезпечення безпеки вашого ПК. Хмарний антивірус використовує новітні технології захисту, завдяки якому забезпечується безпека й стабільна роботу комп'ютера.

Основні функції хмарного антивірусу, що розроблений:

– Захист у режимі реального часу.

– Базовий захист при роботі в мережі Інтернет і з електронною поштою.

– Мінімальне завантаження комп'ютера.

– Інтуїтивно зрозумілий інтерфейс.

– Для повноцінного захисту комп'ютера крім хмарного антивірусу рекомендується використовувати міжмережний екран.

– Перевірка файлів, веб-сторінок, поштових і ICQ-повідомлень.

– Блокування посилань на заражені веб-сайти й сайти, що перехоплюють інформацію.

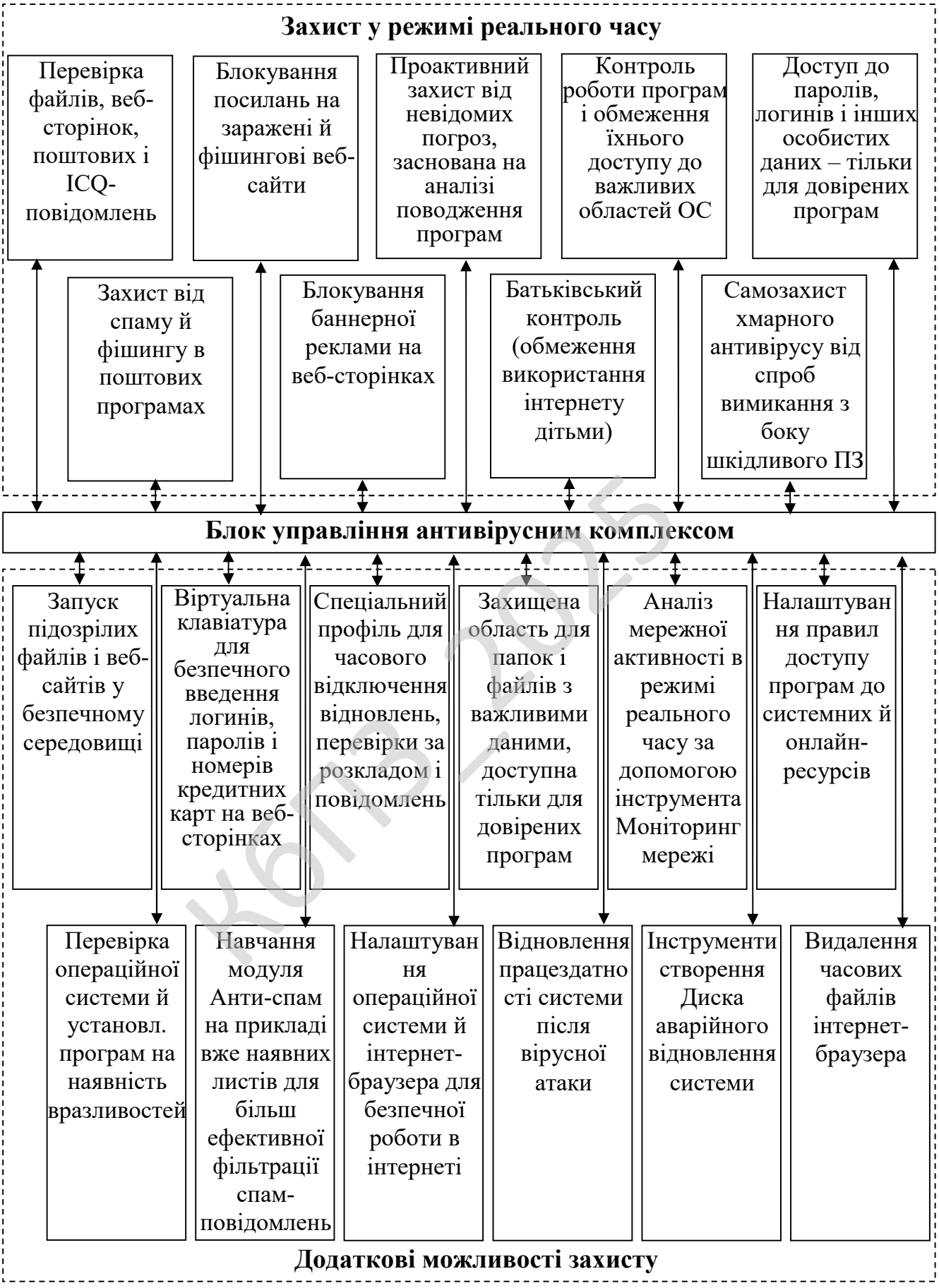

Рисунок 3.2 – Функціональна схема системи

– Проактивний захист від невідомих погроз, заснована на аналізі поводження програм.

– Самозахист хмарного антивірусу, що розроблений попереджає погрозу вимикання з боку шкідливого ПЗ.

– Система миттєвого виявлення погроз, що моментально блокує нові шкідливі коди.

– Реалізовано модуль «Перевірка посилань», що попереджає про заражені або небезпечні веб-сайти.

– Проактивний захист нового покоління від невідомих погроз.

– Віртуальна клавіатура для безпечного введення логінів, паролів і номерів кредитних карт на веб-сторінках.

– Перевірка операційної системи й установлених програм на наявність уразливостей.

– Налаштування операційної системи й інтернет-браузера для безпечної роботи в мережі Інтернет.

– Відновлення працездатності системи після вірусної атаки.

– Видалення часових файлів інтернет-браузера.

На рисунку 3.2 зображена функціональна схема системи. Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

Діаграма взаємодії процесів системи, розробленої у результаті виконання дипломного проектування, наведена на рисунку 3.3.

Першим процесом у розробленій системі являється процес виведення системних ресурсів.

Після нього користувач може перейти до наступних процесів:

– встановлення параметрів хмарного антивірусу;

– контроль процесів;

– вибір ресурсів для сканування.

Контроль процесів пов’язаний з наступними процесами:

– виведення статистики;

– зупинки/запуску контролю процесів.

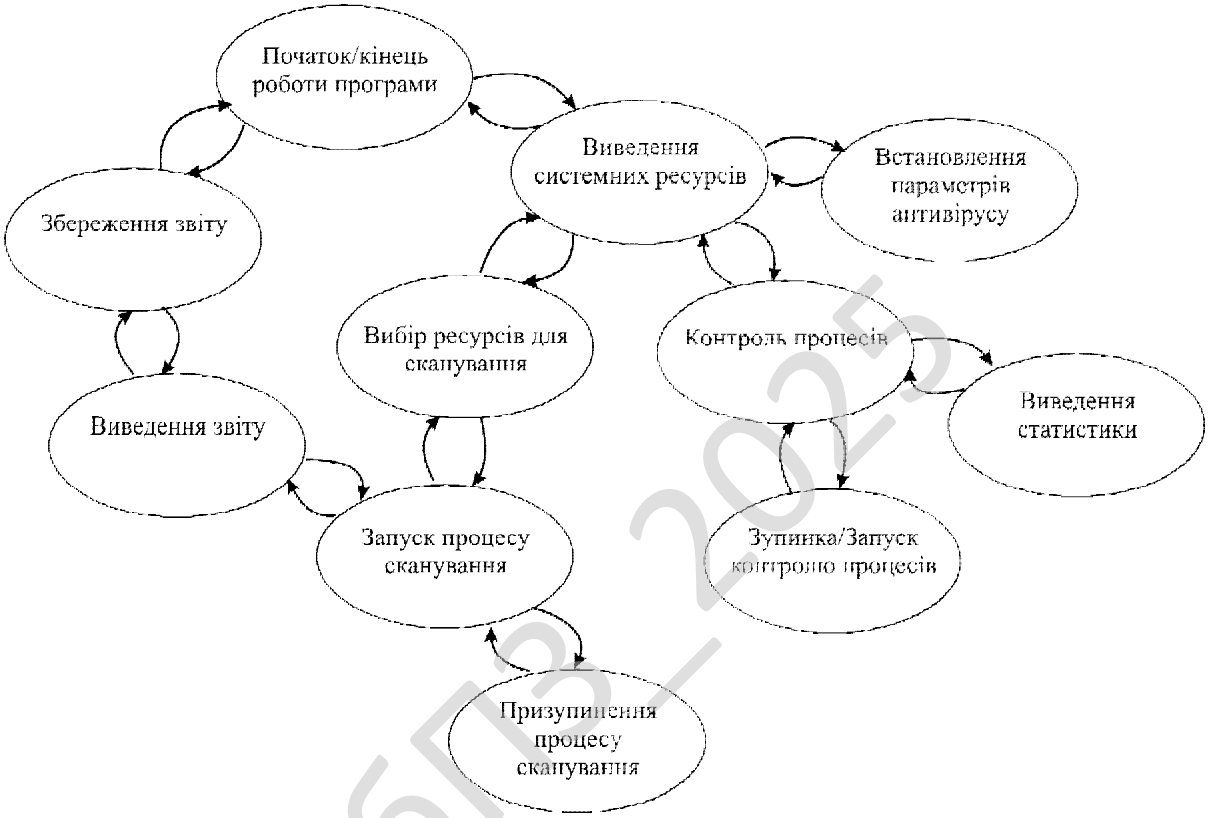

Рисунок 3.3 – Діаграма взаємодії процесів

Після вибору ресурсів для сканування слідує процес запуску сканування, що в свою чергу пов’язаний з процесами:

– призупинення сканування;

– виведення звіту;

– збереження звіту.

Таким чином розглянувши структурну схему, функціональну схему та діаграму взаємодії процесів перейдемо до опису блок-схем програмного забезпечення та алгоритмів їх функціонування.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Система обробки й формування початкового стану маршрутів ТКС

Для нормального функціонування блоку нейромережевих експертів необхідно сформувати їхні початкові стани, виражені попередньою установкою вагових коефіцієнтів нейронних мереж. У зв'язку із цим необхідно використовувати принципи оптимізації на основі кооперативної коеволюції з декількома популяціями [2], що враховують спільне функціонування нейронних мереж. Як було зазначено раніше для рішення поставленого завдання доцільно використовувати імунний алгоритм оптимізації, побудований на основі принципів імунітету живих організмів, запропонований у роботі [4].

Передбачувані ваги нейронних мереж кодуються в антитілах, що утворять популяцію. Як антиген розглядається завдання ініціалізації початкового стану експертів.

Як популяція антигенів виступає область всіх можливих значень векторів ваг і порогів нейронів. Кожне антитіло кодує вектори вагових коефіцієнтів і пороги нейронів.

Під кодування кожного параметра вагового коефіцієнта приділяється 20 біт даних. Антитіло має розрядність кратну 20 биткам і в ньому закодовані всі вагові коефіцієнти нейромережевого експерта. У нейронну мережу послідовно підставляються параметри, закодовані в кожному з антитіл популяції. Обчислюється помилка навчання для кожного антитіла.

При обміні антитілами з популяцій віддаляється частина антитіл, також це відбувається й після застосування оператора мутації, тому що для одержання

правильного куба з антитіл необхідно виконувати їхнє клонування для одержання потрібної кількості. Просте видалення гірших антитіл може привести до видалення певної частини даних, що приводить до неефективного функціонування алгоритму навчання й збільшенню часу на пошук оптимального рішення. Для того щоб зберегти інформацію, накопичену в антитілах, був використаний адаптивний метод кластеризації за структурою заснований на застосуванні нейронної мережі АРТ-1 [2, 8].

Мережа навчається без учителя й реалізує простий алгоритм кластеризації. Відповідно до цього алгоритму перше антитіло вважається зразком першого кластера. Наступне антитіло рівняється зі зразком першого кластера. Антитіло належить першому кластеру, якщо відстань до зразка першого кластера менше порога. У противному випадку, друге антитіло – зразок другого кластера. Цей процес повторюється для всіх наступних антитіл. Після того, як вся популяція антитіл буде розбита на кластери, обчислюється середня аффінність кожного кластера. Антитіла спочатку віддаляються їхнього гіршого кластера й далі із всіх кластерів один по одному в порядку аффінності. Це дозволяє зберегти різноманітну структуру антитіл [4].

Блок-схема основної програми представлена на рисунку 4.1.

У результаті, для кожного нейромережевого експерта створюється окремий комплекс популяцій антитіл, усередині кожної популяції виробляється розвиток антитіл, мутація й видалення. Після зміни рішень імунними операторами виробляється запуск механізму міграцій. При перевірці експерта виробляється видалення тих антитіл з популяції, які не задовольняють критеріям функціонування нейромережевой асоціативної машини. Навіть якщо в антитілі закодоване краще рішення для конкретного експерта, а на рівні асоціативної машини воно показало незадовільний результат, то воно буде вилучене [14].

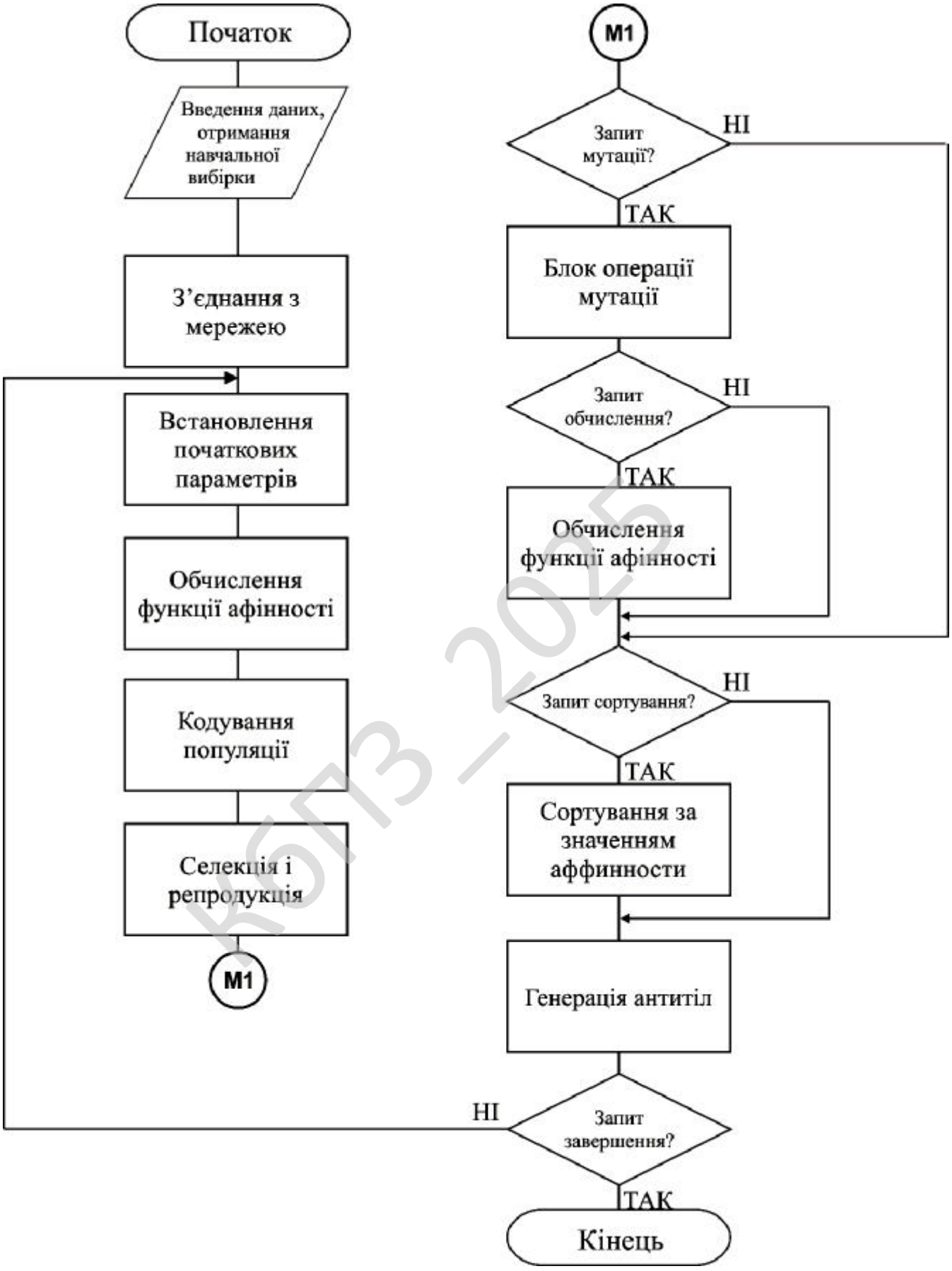

Рисунок 4.1 – Блок-схема основної програми

Розробка асоціативного блоку нейромережевих експертів

Аналіз літератури, а також проведені дослідження показали можливості використання моделі АР-2 Гроссберга-Карпентера [1] для рішення завдань класифікації, кластеризації й розпізнавання аномального стану ліній зв'язку ТКС, тому що ця модель сполучає в собі властивості пластичності й стабільності, а також не вимагає досить більших апріорних знань.

Однак, ця модель має й істотні недолік. Вона припускає використання всього одного шару нейронів (не вважаючи вхідного, асоційованого із сенсорами). Це приводить до того, що нейронна мережа працює тільки з метрикою первинних ознак і обчислює відстань між образами, використовуючи звичайно евклідову відстань.

Даний факт, в умовах наявних розходжень у поточних метриках характеристик ліній зв'язку ТКС, може привести до значного неточностям при визначенні аномалій на маршрутах передачі метаданих у хмарних антивірусних системах.

Тому в дипломній роботі для підвищення точності й забезпечення інваріантності визначення аномалій у лініях зв'язку пропонується використовувати багатошарові персептрони, що формують на проміжних шарах у процесі навчання побічні ознаки.

Можна відзначити, що в персептронах кожний шар забезпечує перетворення однієї метрики образів в іншу. У такій комбінованій моделі перші кілька шарів нейронів організовані як персептрон прямого поширення, виходи якого є входами моделі АР-2. Персептрон забезпечує перетворення метрики первинних ознак у метрику побічних ознак у просторі значно меншої розмірності. Нейронна мережа АР-2 розпізнає відхилення в характеристиках ліній зв'язку по побічних ознаках.

Блок-схема підпрограми, що реалізує функціонування пропонованої в дипломній роботі моделі представлена на рисунку 4.2.

Слід уточнити, що якщо відстань для нейрона-переможця менше *R*, те в моделі АР-2 для нейрона-переможця перераховуються ваги зв'язків, наближаючи центр кластера до вхідного розпізнаного вектора моделі АР-2 з урахуванням кількості розпізнаних раніше векторів цього кластера (чим їх було більше, тим менше зміна ваг нейрона-переможця).

Для персептрона виконується перерахування ваг по алгоритму зворотного поширення помилки [14]. При цьому вихідним еталонним вектором уважається новий вектор ваг вихідного нейрона переможця моделі АР-2, і кількість ітерацій може бути невеликим (зокрема, може бути всього одна ітерація).

Таким чином, розроблена модель системи нейромережевих експертів, що відрізняється від відомих комплексним використанням нейронних мереж різного типу й конфігурації.

Це дозволило синхронізувати роботу асоціативного блоку нейромережевих експертів і підвищити точність ухвалення рішення про аномальність характеристик оптоволоконних ліній зв'язку.

У розділі розроблений метод антивірусного захисту даних у ТКС за рахунок безпечної маршрутизації метаданих у хмарні антивірусні системи. Основними складовими методу є: алгоритми формування множини маршрутів передачі метаданих, метод контролю ліній зв'язку ТКС, моделі системи нейромережевих експертів безпечної маршрутизації.

Рішення оптимізаційного завдання вибору й формування базової множини шляхів передачі даних проведено за критерієм мінімуму часу передачі метаданих на вузол програмного сервера. У той же час рішення приватної оптимізаційного завдання формування множини обраних маршрутів здійснювалося за критерієм максимуму ймовірності безпечної передачі даних.

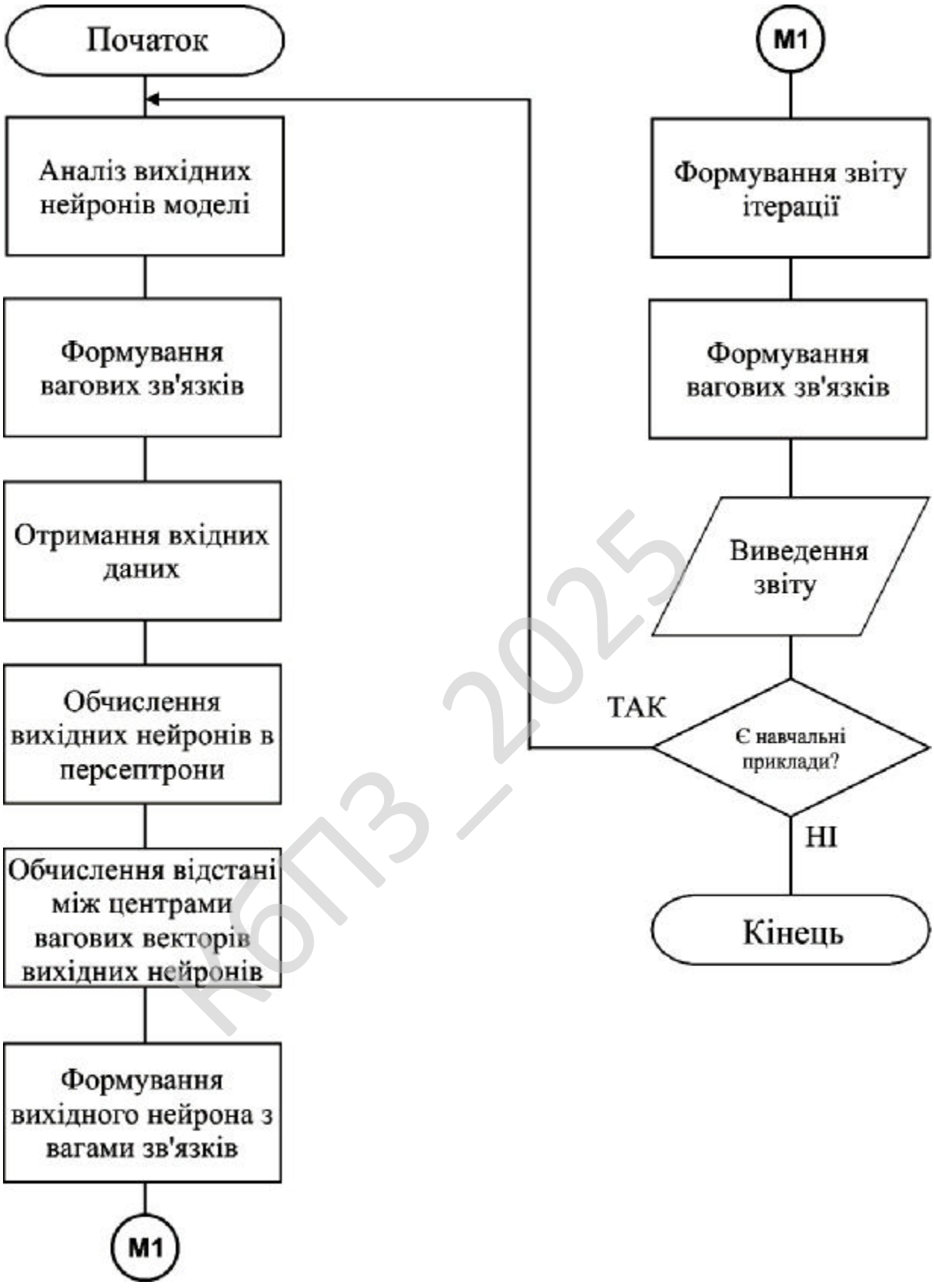

Рисунок 4.2 – Структурна схема підпрограми

Для постійного моніторингу й рішення завдання переформатування маршрутів зв'язку з вузлом програмного сервера розроблений метод контролю ліній зв'язку ТКС. Використання даного методу дозволить виявляти зміну характеристик ВОЛЗ у процесі функціонування ТКС, (одержати необхідні дані для початку процедури навчання нейронних експертів) і видавати необхідні сигнали аномалій (можливих кібератак) у лініях зв'язку в систему нейромережевих експертів безпечної маршрутизації. Відмінною рисою запропонованого методу є введення процедури обліку «скомпрометованих» біт даних спеціальних сигнатур, переданих у хмарні антивірусні системи. Це дозволить знизити ймовірність маніпуляцій метаданими, переданими у вузли програмного сервера.

Для підвищення точності прийняття рішень про можливі атаки несанкціонованого доступу до ВОЛЗ і рішення в цілому завдання безпечної маршрутизації розроблена модель системи нейромережевих експертів, що відрізняється від відомих комплексним використанням нейронних мереж різного типу й конфігурації. Даний механізм робить інтеграцію знань, накопичених експертами, у загальне рішення, що має пріоритет над кожним рішенням окремого експерта. При цьому рішення експертів, отримані на основі обробки даних, пов'язаних з безпечною маршрутизацією, дозволяють підвищити точність ухвалення правильного рішення про несанкціонований доступ на маршруті передачі метаданих.

4.2 Захист розробленого програмного забезпечення

Розроблене програмне забезпечення захистимо за допомогою алгоритму захисту інформації RSA. Спочатку необхідно обчислити пару ключів (секретний ключ і відкритий ключ). Для цього відправник електронних документів обчислює два більших простих числа P и Q, потім знаходить їхній добуток $N = P*Q$ і значення функції $\varphi(N) = (P-1)(Q-1)$. Далі відправник обчислює число E з умов E

< $\varphi(N)$, НЗД (E, $\varphi(N)$) = 1 і число D з умов $D < N$, $E*D \equiv 1(\text{mod } \varphi(N)$.

Пари чисел (E, N) є відкритим ключем. Цю пару чисел автор передає партнерам по переписці для перевірки його цифрових підписів. Число D зберігається автором як секретний ключ для підписування.

Допустимо, що відправник хоче підписати повідомлення M перед його відправленням. Спочатку повідомлення M (блок інформації, файл, таблиця) стискають за допомогою геш-функції h(-) у ціле число m: $m = h(M)$.

Потім обчислюють цифровий підпис S під електронним документом M, використовуючи геш-значення m і секретний ключ D: $S = m \pmod N$.

Пари (M, S) передається партнерові-одержувачеві як електронний документ M, підписаний цифровим підписом S, причому підпис S сформований власником секретного ключа D.

Після прийому пари (M, S) одержувач обчислює геш-значення повідомлення M двома різними способами. Насамперед, він відновлює геш-значення m', застосовуючи криптографічне перетворення підпису S з використанням відкритого ключа E: $m' = S^E \pmod N$.

Крім того, він знаходить результат гешування прийнятого повідомлення M с допомогою такої ж геш-функції h(-): $m = h(M)$.

Якщо дотримується рівність обчислених значень, тобто $S^E(\text{mod}) = h(M)$, то одержувач визнає пару (M, S) справжньою. Доведено, що тільки власник секретного ключа D може сформувати цифровий підпис S по документі M, а визначити секретне число D по відкритому числу E не легше, ніж розкласти модуль N на множники. Крім того, можна строго математично довести, що результат перевірки цифрового підпису S буде позитивним тільки в тому випадку, якщо при обчисленні S був використаний секретний ключ D, що відповідає відкритому ключу E. Тому відкритий ключ E іноді називають "ідентифікатором" того, хто підписав.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Розроблене програмне забезпечення реалізує систему нейромережевих експертів безпечної маршрутизації у антивіруси.

Програмно-апаратні вимоги:

- Загальний обсяг ОЗП: 512 Мбайт.
- Вільний простір на жорсткому диску: 27 Мбайт.
- Операційна система Microsoft Windows /11.

Дана програма – це простий у використанні і в той же час повноцінний профілактичний антивірусний сканер з високою швидкістю сканування. Сканер має гнучку систему налаштувань.

Даний хмарний антивірус забезпечує повноцінний захист комп'ютера від шкідливого ПЗ, а система Контроль процесів – постійно контролює всі процеси користувача, що дозволяє запобігти зараженню системи. Докладна система звітності, дозволяє перевірити всю інформацію про сканування, і зробити висновки про захищеність системи.

Дана програма виявляє віруси, троянські програми, руткіти та хробаків. Робить пошук і детектування наступних різновидів шкідливого ПЗ:

1. SpyWare, AdvWare програм.
2. Руткітів та інших шкідливих програм.
3. Мережних і поштових хробаків.
4. Троянських програм.

В програму вбудована потужна модульна система, що забезпечує додавання нових можливостей у сканер. Кожний користувач може створити свій унікальний модуль, що у свою чергу забезпечує максимальну гнучкість сканера.

Головне вікно програми зображене на рисунку 5.1.

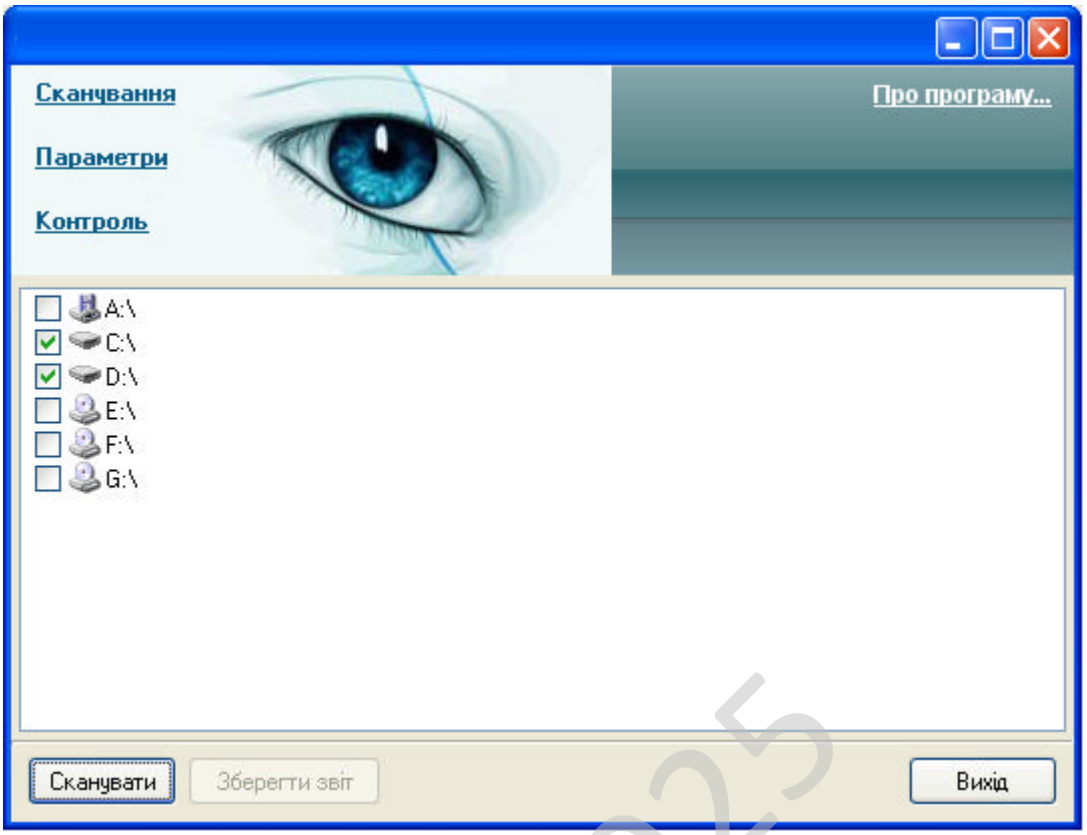

Рисунок 5.1 – Головне вікно програми

На ньому розташовані наступні посилання:

– Сканування.
– Параметри.
– Контроль.
– Про програму…

Та кнопки:

– Сканувати.
– Зберегти звіт.
– Вихід.

А також воно містить список дисків встановлених у системі, з якого користувач вибирає ті, які потрібно сканувати.

Для запуску процесу сканування слід вибрати диски, що необхідно перевірити та натиснути кнопку «Сканувати», процес сканування зображено на рисунку 5.2. На рисунку 5.3 зображено звіт, що виводиться в кінці сканування.

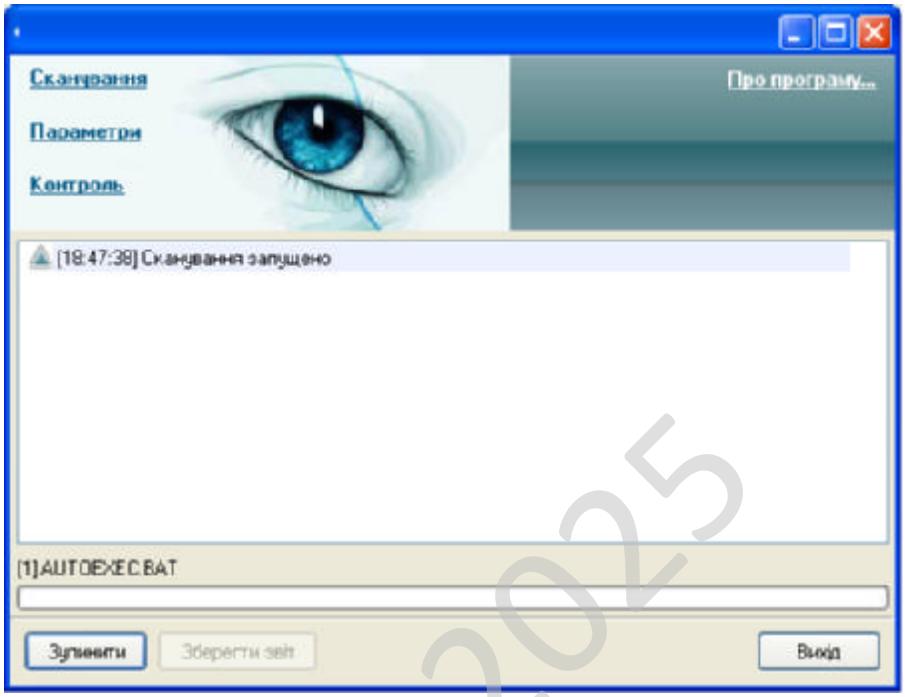

Рисунок 5.2 – Сканування

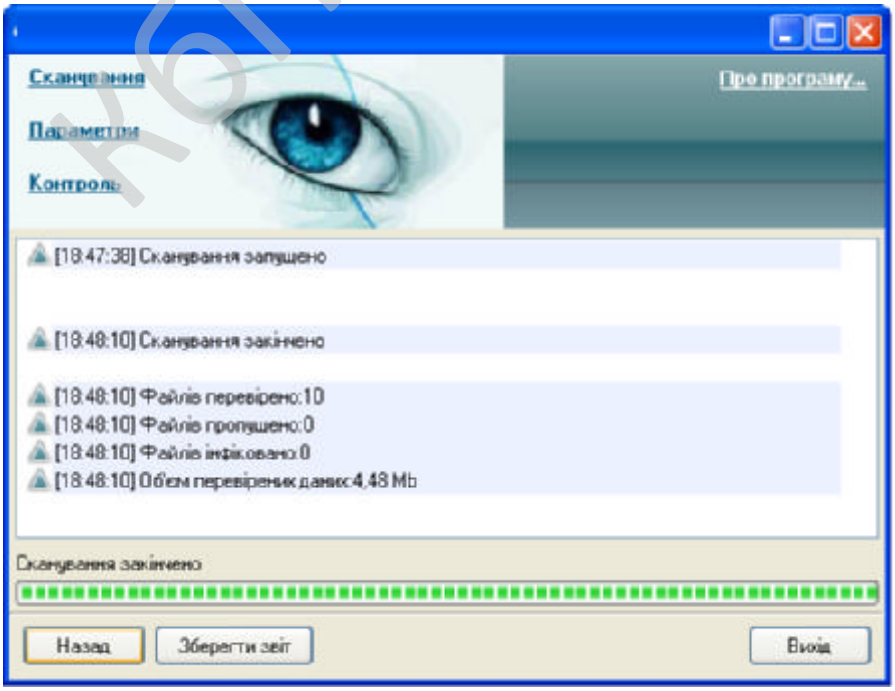

Рисунок 5.3 – Звіт

Для встановлення параметрів програми необхідно натиснути на посилання «Параметри» (рисунки 5.4 – 5.7).

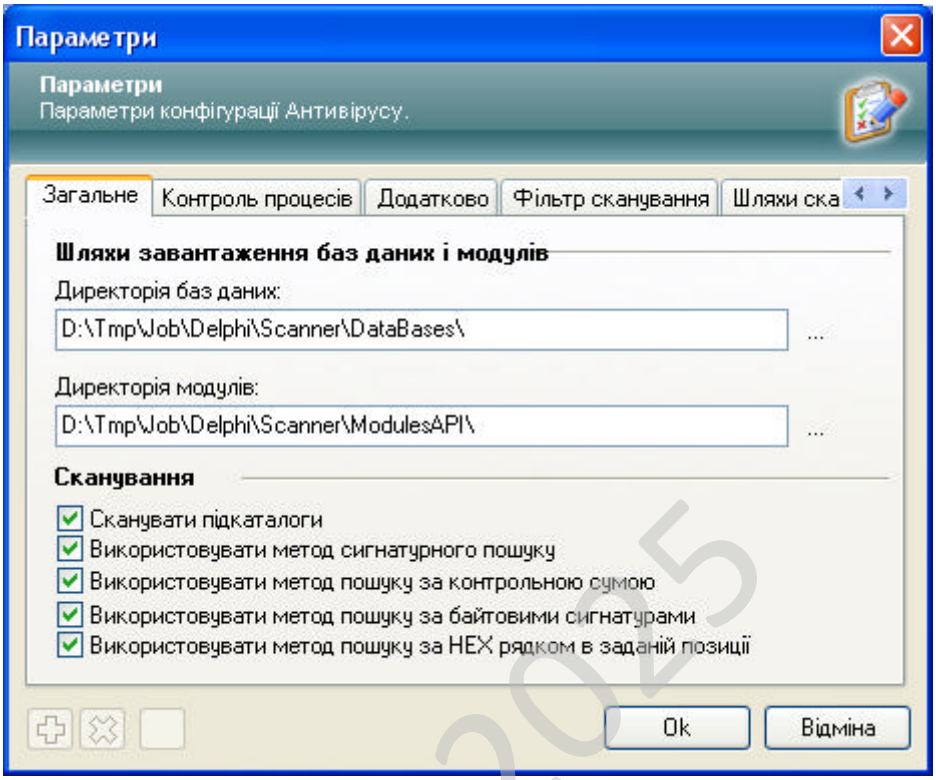

Рисунок 5.4 – Параметри (загальне)

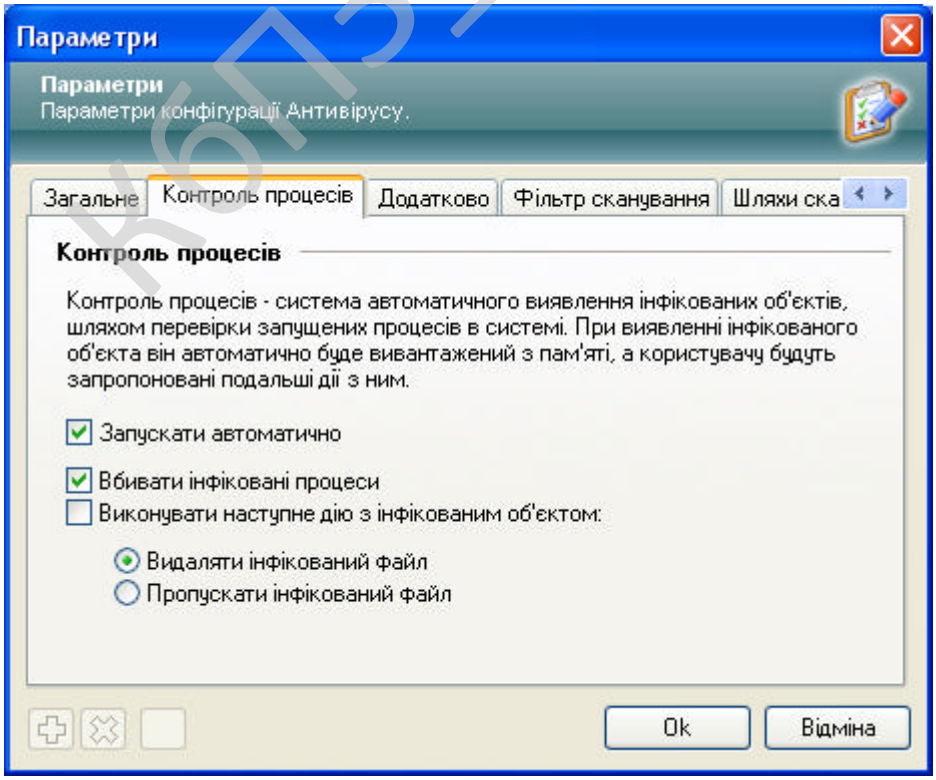

Рисунок 5.5 – Параметри (контроль процесів)

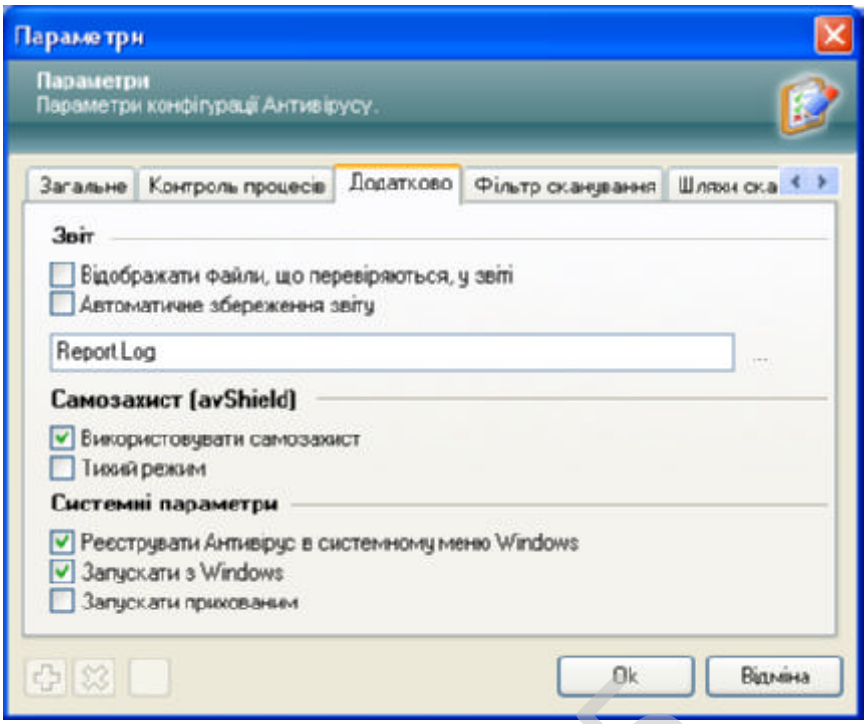

Рисунок 5.6 – Параметри (додатково)

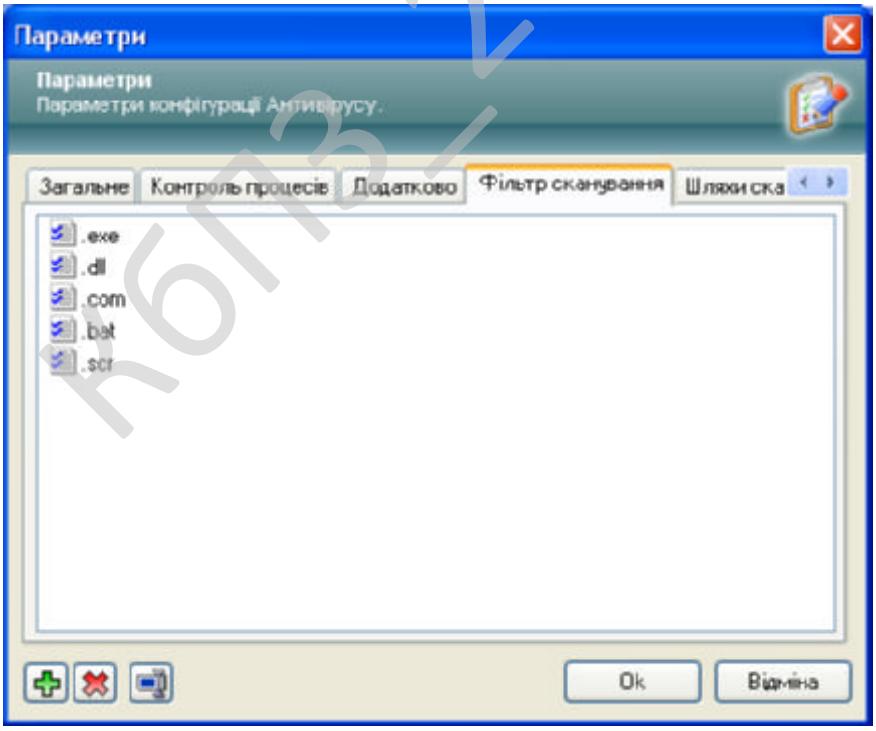

Рисунок 5.7 – Параметри (фільтр сканування)

В розробленій програмі є система Контроль процесів, призначена для автоматичного виявлення інфікованих об'єктів, шляхом перевірки запущених процесів в системі. При виявленні інфікованого об'єкта він автоматично буде вивантажений з пам'яті, а користувачу будуть запропоновані подальші дії з ним. Для перегляду роботи даної системи слід натиснути посилання «Контроль», після чого відкриється вікно, зображене на рисунку 5.8.

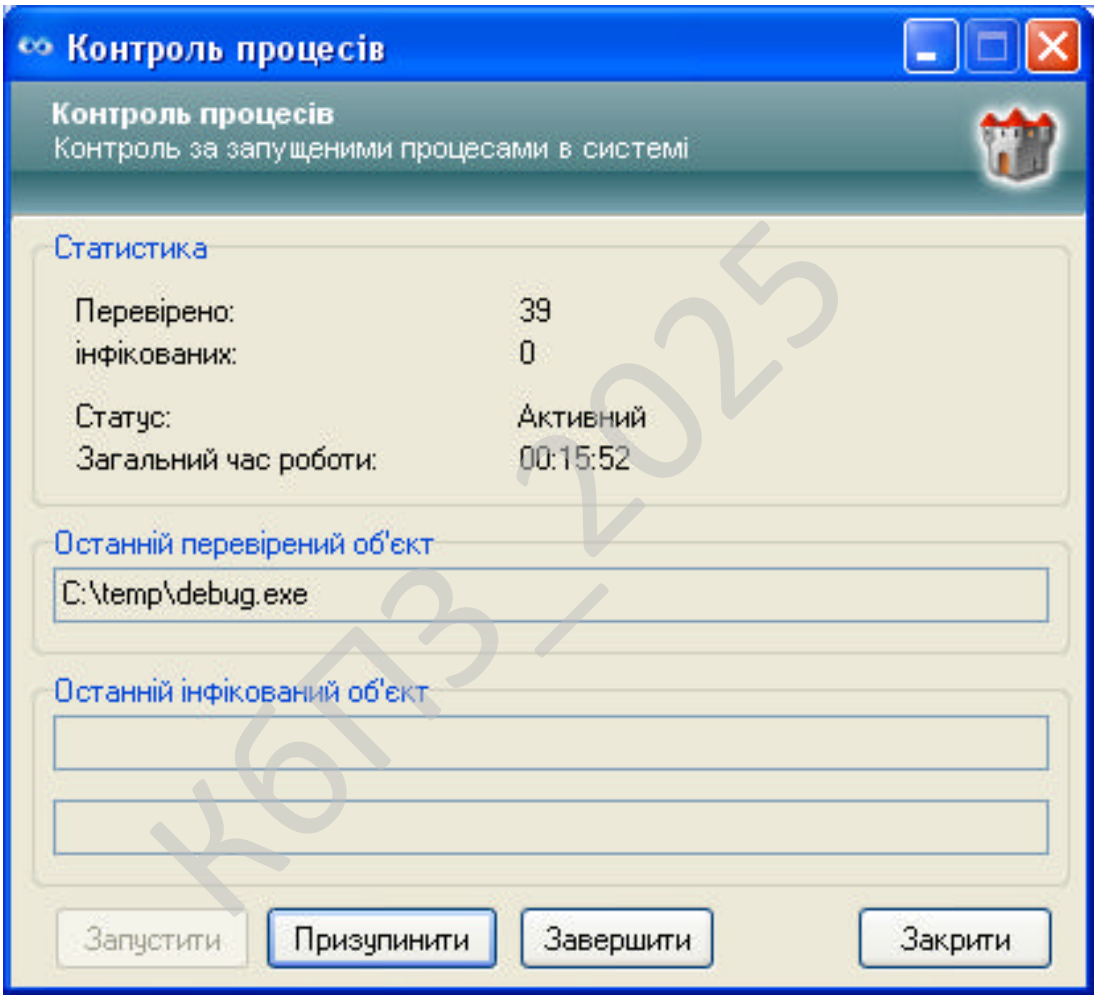

Рисунок 5.8 – Контроль процесів

Коротку довідку про розроблену програму можна переглянути натиснувши посилання "Про програму…", після чого з'явиться вікно зображене на рисунку 5.9.

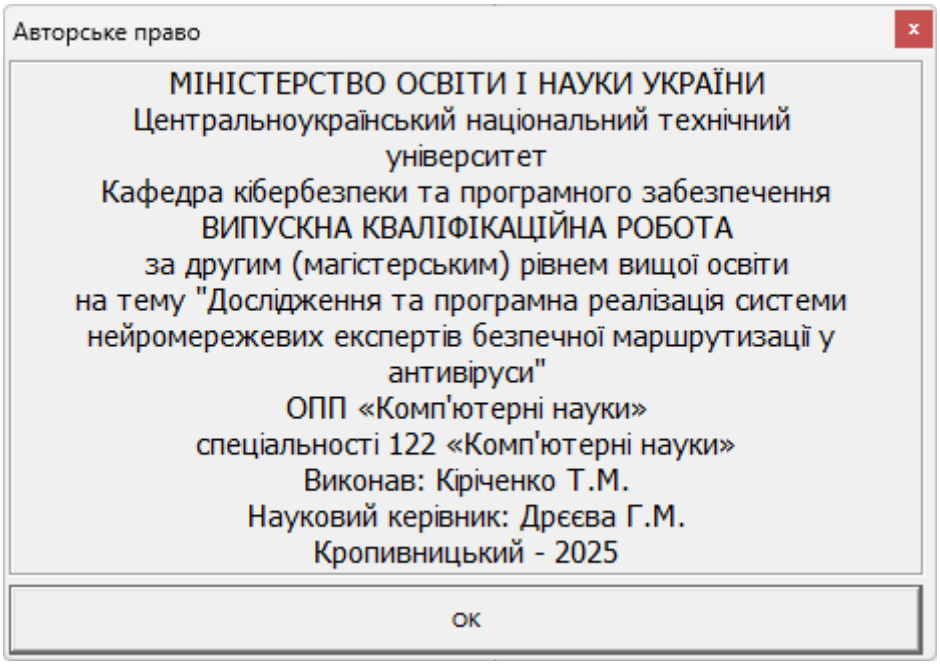

Рисунок 5.9 – Вікно «Про програму…»

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи нейромережевих експертів безпечної маршрутизації у антивіруси.

Метою розробки є дослідження та програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси.

Об'єктом дослідження є процес нейромережевих експертів безпечної маршрутизації у антивіруси.

Предметом дослідження є методи нейромережевих експертів безпечної маршрутизації у антивіруси.

Методи дослідження базуються на методах штучного інтелекту, методах комп'ютерних мереж, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод нейромережевих експертів безпечної маршрутизації у антивіруси.

– Розроблено вітчизняний продукт нейромережевих експертів безпечної маршрутизації у антивіруси, який має більш широкі можливості, на відміну від існуючих аналогів.

7 МАРКЕТИНГОВЕ ТА ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ІТ-ПРОЄКТУ

7.1 Визначення цільової аудиторії кінцевого готового продукту

Результати дослідження та розробки системи нейромережевих експертів безпечної маршрутизації можуть зацікавити передусім компанії, що працюють у сфері кібербезпеки та розробки антивірусного програмного забезпечення. Для таких організацій ця технологія є реальним способом підвищити ефективність виявлення загроз і зменшити кількість помилкових спрацьовувань системи. Оскільки традиційні антивірусні рішення часто відстають від динамічного розвитку шкідливих технологій, інтеграція нейромережевого модуля дає можливість забезпечити глибший і більш контекстний аналіз трафіку.

Також проєкт може бути цікавим для великих корпоративних клієнтів, які мають складну мережеву інфраструктуру, наприклад, банки, телекомунікаційні компанії чи промислові підприємства. Вони потребують автоматизованих рішень, здатних швидко реагувати на потенційні кібератаки та зменшувати ризики витоку конфіденційних даних. Такі компанії готові інвестувати в технології, що дозволяють не просто реагувати на інциденти, а передбачати їх.

Науково-дослідні установи також можуть зацікавитися цією розробкою, адже система відкриває нові можливості для вивчення застосування нейронних мереж у сфері безпечної маршрутизації. Для них важливим є аспект навчання алгоритмів на різних типах даних та оцінка їхньої адаптивності до нових умов. Крім того, результати дослідження можуть бути корисними для освітніх програм із кібербезпеки, штучного інтелекту та комп'ютерних мереж, де така розробка може слугувати прикладом практичної інтеграції інтелектуальних технологій у безпекові рішення.

7.2 Оцінка привабливості шляхом застосування методів експертних оцінок

Для оцінки привабливості системи можна залучити експертів із різних напрямів: спеціалістів із кібербезпеки, розробників антивірусного ПЗ, аналітиків з машинного навчання та ІТ-менеджерів. Вони можуть оцінити систему за кількома критеріями – технологічна новизна, ефективність виявлення загроз, інтеграційна сумісність, ринковий потенціал і економічна вигода від упровадження. Наприклад, за десятибальною шкалою середня оцінка інноваційності може становити 9 балів, а економічна доцільність – 8,5, що свідчить про високу перспективність системи.

На підставі зібраних оцінок можна побудувати зведену таблицю з ваговими коефіцієнтами, де кожен критерій має власну важливість. Наприклад, якщо технологічна ефективність оцінюється як найважливіша, то її коефіцієнт може становити 0,3, тоді як маркетингова привабливість – 0,2. Після підрахунку підсумкового інтегрального показника можна дійти висновку, що загальна привабливість системи перевищує 8 балів, що є високим показником для ІТ-проєктів із впровадженням нейромережевих технологій.

Такий підхід дозволяє не лише визначити перспективність розробки, а й виявити потенційні зони вдосконалення. Наприклад, якщо експерти звертають увагу на складність впровадження або потребу у великих обчислювальних потужностях, це може бути сигналом для оптимізації архітектури системи. У результаті метод експертних оцінок допомагає сформувати комплексне уявлення про ринкову цінність та технологічну готовність продукту.

7.3 Вибір методу оцінки вартості ПЗ

Для такої системи найдоцільніше застосувати метод оцінки вартості на основі витрат (Cost-Based Method) у поєднанні з аналізом майбутніх вигод

(Benefit-Cost Analysis). Це пояснюється тим, що проєкт передбачає значні початкові інвестиції у розробку, навчання моделі, тестування та інтеграцію з існуючими антивірусними системами. Метод дозволяє врахувати всі етапи життєвого циклу розробки – від створення прототипу до технічної підтримки після впровадження.

Водночас, для оцінки прибутковості інвестицій варто застосувати метод дисконтованих грошових потоків (DCF), який дозволяє оцінити реальну вартість майбутніх вигод від системи з урахуванням фактору часу. Наприклад, економія на зменшенні інцидентів безпеки або зниження навантаження на IT-підтримку може бути оцінена в грошовому еквіваленті на кілька років уперед.

Завдяки поєднанню цих підходів можна отримати реалістичну оцінку рентабельності проєкту. Це особливо важливо, адже нейромережеві рішення потребують періодичного донавчання моделей і постійної підтримки. Таким чином, метод оцінки вартості має враховувати не лише технічні витрати, а й довгострокові фінансові переваги, пов'язані з підвищенням ефективності антивірусного захисту.

7.4 Розрахунок економічної ефективності від впровадження реалізованого ПЗ як фактору його привабливості

Компанія-розробник антивірусного програмного забезпечення стикається з викликами збільшення обсягів шкідливого трафіку та появою складних атак типу zero-day, які вимагають динамічного аналізу поведінки. Традиційні антивірусні системи, що базуються на сигнатурному пошуку, мають обмеження в оперативності реагування та не завжди встигають ідентифікувати загрози в реальному часі.

Для вирішення цієї проблеми пропонується впровадження системи нейромережевих експертів безпечної маршрутизації, що забезпечує розумний аналіз мережевих потоків, автоматичне виявлення потенційно шкідливих

маршрутів і перенаправлення підозрілого трафіку до ізольованого середовища. Система базується на нейромережевій моделі, навченої на реальних даних, здатній адаптуватися до нових типів атак.

Головна мета впровадження – підвищення ефективності захисту мережі, зменшення часу виявлення загроз і скорочення фінансових збитків від інцидентів безпеки. Вхідні дані зафіксовано в таблиці 7.1.

Таблиця 7.1 – Вихідні дані для розрахунку

Показник	**До впровадження**	**Після впровадження**	**Економічний ефект**
Кількість кібератак на рік	120	120	—
Середня кількість успішних інцидентів	12	2	–10
Середній збиток від одного інциденту (грн)	300 000	50 000	–250 000
Річний обсяг збитків (грн)	3 600 000	100 000	–3 500 000
Витрати на адміністрування та реагування (грн/рік)	800 000	400 000	–400 000
Початкові інвестиції у систему (розробка, інтеграція, тестування)	—	1 500 000	—
Щорічні витрати на підтримку та навчання нейромережі	—	150 000	—

Розрахунок економічного ефекту демонструє наступне: зниження збитків від кіберінцидентів – 3 500 000 грн/рік, економія на витратах з реагування – 400 000 грн/рік, додатковий ефект від підвищення продуктивності ІТ-відділу (скорочення часу ручного аналізу загроз на 30% – еквівалентно ≈ 250 000

грн/рік), сукупний річний економічний ефект – 4 150 000 грн/рік, чистий економічний ефект – 4 000 000 грн/рік, термін окупності (Payback Period) ≈ 0,38 року (4,5 місяці), рентабельність інвестицій ≈ 266 %.

Додаткові нефінансові переваги: зменшення часу виявлення загроз – із годин до хвилин завдяки адаптивним моделям нейронних мереж, підвищення точності класифікації трафіку – менше хибнопозитивних спрацьовувань, що зменшує навантаження на ІТ-відділ, автоматизація процесу реагування – система може самостійно перенаправляти підозрілий трафік або блокувати підключення, безперервне навчання – чим більше даних система аналізує, тим точніше прогнозує загрози, покращення репутації компанії – демонстрація високого рівня кіберзахисту сприяє довірі клієнтів.

Отже, система нейромережевих експертів є ключовим інструментом у сучасній архітектурі безпеки, який не тільки захищає мережу від загроз, а й створює фінансовий фундамент для стабільного розвитку компанії.

7.5 Пропозиція алгоритму просування проєкту розробки ПЗ

Першим кроком просування має стати створення демонстраційної версії системи, яку можна протестувати на обмеженій кількості користувачів або підприємств. Це дозволить продемонструвати практичну користь нейромережевої маршрутизації на прикладі реальних мережевих загроз. Далі важливо опублікувати результати тестів і кейси успішного впровадження у фахових ІТ-журналах та на конференціях з кібербезпеки, щоб підкреслити інноваційність підходу.

Паралельно потрібно працювати з потенційними партнерами – компаніями, що розробляють антивірусні платформи. Їм можна запропонувати інтеграційні модулі або API, які легко вбудовуються в їхні продукти. Такий підхід дає можливість швидко масштабувати розробку через уже існуючі ринки.

Варто також створити програму пілотного тестування для корпоративних клієнтів, надаючи безкоштовний доступ на обмежений час. Якщо клієнти побачать зменшення кількості інцидентів безпеки, вони будуть готові перейти на комерційну версію. На заключному етапі можна запустити маркетингову кампанію, орієнтовану на IT-директорів та керівників служб безпеки, з акцентом на фінансову вигоду та ефективність рішень.

7.6 Оптимізація каналів збуту та шляхів реалізації ПЗ

Для ефективної реалізації проєкту можна поєднати прямі продажі корпоративним клієнтам із дистрибуцією через партнерські IT-компанії. Великі інтегратори можуть виступати як офіційні партнери, пропонуючи систему в складі своїх комплексних рішень з інформаційної безпеки. Це дозволить охопити ширшу аудиторію без значного збільшення власних ресурсів на маркетинг і підтримку.

Крім того, доцільно розробити хмарну версію продукту за моделлю Software as a Service (SaaS). Це зробить систему доступнішою для малих і середніх компаній, які не мають потужної технічної інфраструктури. Такий формат також спростить оновлення, моніторинг і ліцензування.

Ще один напрям – участь у державних і корпоративних програмах цифрової трансформації, де потрібні рішення для захисту інформаційних систем. Це не лише покращить впізнаваність бренду, а й відкриє можливості для співпраці з урядовими структурами та великими корпораціями.

7.7 Визначення ключових факторів успіху конкретного проєкту

Ключовими факторами успіху проєкту є висока точність роботи нейромережевої моделі, стабільність алгоритмів і можливість масштабування системи. Якщо система здатна ефективно аналізувати трафік у режимі реального

часу, мінімізуючи хибні спрацьовування, це створює довіру з боку користувачів і партнерів.

Не менш важливим чинником є швидкість адаптації до нових типів загроз. У сучасному цифровому світі кіберзлочинці постійно вдосконалюють методи атак, тому система має здатність до самонавчання, що забезпечується використанням нейромережевих підходів.

Успіх також залежить від доступності технічної підтримки та регулярного оновлення алгоритмів. Компанії, які впроваджують такі рішення, очікують, що продукт буде не лише ефективним, а й зручним у використанні. Нарешті, важливу роль відіграє рентабельність: якщо система доведе свою здатність скорочувати витрати на реагування на інциденти, вона матиме стабільний попит і перспективи для подальшого розвитку.

8 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

8.1 Вступ

Охорона праці – система збереження життя і здоров'я працівників у процесі трудової діяльності, що включає правові, соціально-економічні, організаційні, технічні, санітарно-гігієнічні, лікувально-профілактичні, реабілітаційні та інші заходи.

Згідно закону України “Про охорону праці” [3] кожна компанія впроваджує заходи з охорони праці. Реалізується трудові відносини з вживанням необхідних засобів з охорони праці та розробки відповідних документів:

– Інструкцій з охорони праці по кожній професії і загальні.

– Положення про охорону праці.

– Накази з охорони праці.

– Журнали реєстрації та інструктажу.

Роботодавець створює відділ який працює відповідно до типового положення, яку затверджується центральним органом виконавчої влади і забезпечує виконання вимог державної політики у сфері охорони праці.

За недотриманням вимог, керівники ІТ-компаній можуть бути притягнуті до відповідальності, яка виглядає у виді накладання штрафу. Якщо в результаті порушення умов охорони праці є постраждалі працівники то керівні особи ІТ-компаній притягуються до кримінальної відповідальності.

Законом України “Про охорону праці” [3] регламентуються загальні положення державної політики в галузі охорони праці, а конкретизуються ці положення нормативно-правовими актами про охорону праці, зокрема Наказом Міністерства соціальної політики України 14.02.2018 № 207, який зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за №508/31960 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи

з екранними пристроями» [5], яким затверджено нормативно-правовий акт з охорони праці НПАОП 0.00-7.15-18, «Правила охорони праці під час експлуатації електронно-обчислювальних машин», та «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-98 [2].

Науково-технічний прогрес вніс серйозні зміни в умови виробничої діяльності робітників розумової діяльності. Їх праця стала більш інтенсивною, напруженою і вимагає значних витрат розумової, емоційної і фізичної енергії. Це призвело до необхідності у знаходженні комплексного рішення проблем ергономіки, гігієни і організації праці, регламентації режимів праці та відпочинку.

Охорона здоров'я робітників, забезпечення безпеки умов праці, ліквідація та профілактика професійних захворювань і виробничого травматизму складає одну з головних турбот людського суспільства.

8.2 Пожежна безпека

Вимоги до пожежної безпеки на підприємстві неухильно повинен дотримуватися кожен співробітник, а організаційна складова при цьому покладається на посадових осіб за відповідним рішенням керівництва і прописується в посадових інструкціях і положеннях по структурним підрозділам.

Зокрема, вказуються конкретні території, ділянки, зони, об’єкти, цілі будівлі і їх частини, поверхи, на яких відповідального співробітника повинне проводити такі організаційні роботи.

Відповідальні особи зобов’язуються розробити, впровадити та підтримувати в певному інструкцією і положенням на ввірених їм об’єктах протипожежний режим і інструкції відповідно до вимог, викладених в нормативних актах. Передбачено також створення підрозділу добровільної пожежної охорони та пожежно-рятувальної команди в його складі.

Встановлений режим включає порядки з описом місць спеціального призначення та правила їх користування та утримання, наприклад:

– евакуаційних шляхів;

– так званих «курилок»;

– місць складування продукції та сировини;

– стоянки транспорту.

Також встановлюється порядок роботи та технічного обслуговування:

– вентиляційного устаткування;

– засобів пожежогасіння і захисту від загорянь;

– нагрівальних приладів;

– електрообладнання.

Розробляються і впроваджуються правила роботи з відкритим вогнем і горючими матеріалами. Створюються графіки проходження інструктажів з пожежної безпеки співробітників, а також порядок і терміни перевірок знань пожежно-технічного мінімуму, в тому числі, тих працівників, які відповідальні за цю ділянку роботи на підприємстві. При цьому можуть передбачатися внутрішні лекції, семінари, тренінги та практичні заняття на підприємстві, а також зовнішні – на базі спеціалізованих навчальних центрів з професійними викладачами. Важливою складовою протипожежного режиму на будь-якому об’єкті є розробка і впровадження порядку дій при виникненні пожежі. Неодмінно має бути план евакуації, описано, як повинні відключатися електроустановки, що і в якій послідовності необхідно робити співробітникам. Відповідно, для кожного об’єкта, кожного приміщення (крім коридорів, санвузлів, басейнів і подібних приміщень), окремих видів робіт складаються інструкції, за якими повинен працювати персонал, залучений на певних ділянках і в виконанні окремих видів робіт. За інструкціями проводиться навчання (інструктаж) персоналу з подальшим контролем знань. Детально про те, як розробити протипожежний режим, прописати порядки та інструкції, пояснюють на тематичних курсах і семінарах. [4]

8.3 Пропозиції щодо підвищення працездатності ІТ-фахівців

Поява та впровадження нових інформаційно-комунікаційних технологій зумовлює необхідність подальшого вдосконалення охорони праці фахівців ІТ-індустрії. Все це потребує розробки нових нормативно-правових актів з регламентації праці та відпочинку фахівців ІТ-індустрії і стандартів підприємств, центрів комп'ютерної техніки, центрів інформаційних технологій, сучасних комп'ютерних класів. Для підвищення розумової працездатності то зорової роботи повинна здійснюватися ергономічна оптимізація в рамках системи «оператор-термінал», яка сприятиме результативній фізичній та інтелектуальний працездатності і відновленню психосоматичного здоров'я фахівців ІТ-індустрії.

Особливе значення у соціальному захисті цієї категорії працівників належить прийняття комплексного договору, який може забезпечити фахівців додатковими пільгами та компенсаціями.

Пропозиції щодо підвищення працездатності ІТ-фахівців, розіб'ємо на декілька категорій:

Середовище і розпорядок праці. Для мінімізації негативних ефектів, що пов'язані з перевтомленням ІТ-фахівців, потрібно чітко прописати і реалізувати графік періодів праці-відпочинку, щоб фахівець міг можливість переключити увагу, дати можливість відпочити очам, мозку, елементарно, встати розім'яти ноги. Також потрібно зробити максимально комфортними умови мікроклімату у офісному приміщенні, де працюють ІТ-фахівці. Мається на увазі встановлення і експлуатація, коли виникає необхідність, кондиціонерів, опалення, та системи вентиляції, задля попередження перегрівання, переохолодження ІТ-фахівців, і подальшої неможливості ними виконувати свої функції. Також, за можливості, нами пропонується введення практики віддаленої праці ІТ-фахівцями, якщо роботодавець не може забезпечити оптимальні і безпечні умови в офісному приміщенні, або якщо фахівця вони не влаштовують із певних причин.

Фізичні і психоемоційні чинники. Першим і найважливішим чинником, що впливає на працездатність ІТ-фахівців є робоче місце, і саме тому, роботодавець має забезпечити максимальний його комфорт і безпеку. Гарантією цих факторів може слугувати сертифікація меблів, що використовуються на підприємстві ІТ-галузі. Тому нами пропонується закупівля тільки меблів, які пройшли сертифікацію на відповідність. Під психоемоційними чинниками ми розуміємо гарне самопочуття фахівців, позитивний настій, гарний психологічний клімат у колективі, тощо. Задля того, щоб психоемоційні чинники мали максимально позитивний ефект, керівництву слід поводити заходи, які сприятимуть укріпленню і покращенню міжособистісних стосунків у колективі, таких як психологічні тренінги, таймбілдінг, спортивні змагання і естафети. Також, сюди можна віднести розробку і впровадження системи мотивації працівників, як фінансової, так моральної і адміністративної.

8.4 Розробка заходів з умов поліпшення охорони праці

Згідно аналізу умов праці в розглянутому приміщенні, ми одержали наступні результати:

– розмірі приміщення, у розрахунку на одному працюючого, відповідають нормативам;

– мікроклімат відповідає нормативному значенню;

– акустичні умови роботи не перевищують нормативних значень;

Таким чином можна припустити, що основною причиною можливого зниження працездатності програміста є психофізіологічний фактор, тому основна пропозиція буде така: дотримання позитивної психологічної атмосфери в колективі та регламентованого режиму праці та відпочинку, організація робочого місця з урахуванням ергономічних вимог.

Рекомендовані заходи: регулярні періодичні наочні огляди персоналом шляхів для евакуації людей із приміщення, відповідно до плану евакуації (який

повинен розташовуватись на видному місці у приміщенні), включення до колективного договору мінімально можливого вмісту аптечок з обов'язковою наявністю масок-клапанів, або іншого спорядження для штучного дихання. Регулярна періодична перевірка параметрів заземлення та занулення (вимірювання опору ланцюга) [9].

Регулярна наочне знайомство персоналу із шляхами для евакуації людей із приміщення відповідно до плану евакуації, забезпечення розподільних щитів спеціальними розетками з заземлюючими контактами; організація заземлення всіх приладів і пристроїв, які працюють при напрузі вище 36 В.

Так як при ураженні електричним струмом у людини може статися фібриляція шлуночків серця, в організації бажано мати дефібрилятор і підготовлений персонал для роботи з ним.

8.5 Розрахункова частина

Для захисного штучного заземлення будемо застосовувати вертикальні електроди з сталевого прокату круглого перерізу діаметром 35 мм, довжиною L=2 м, та горизонтальний електрод – металева полоса з перетином 35·4 мм. Напруга – 220/380 В. Розрахункова схема розташування заземлюючих електродів – по контуру (прямокутником) (рис. 8.1).

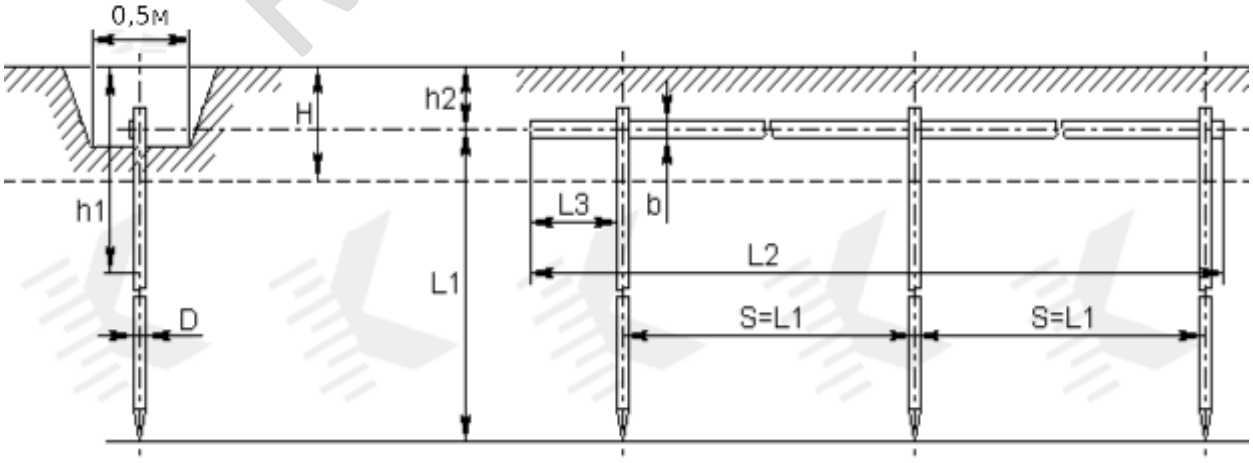

Рисунок 8.1 – Схема штучного заземлення

Розрахунок проводиться за допустимим опором розтіканню струму заземлювача.

Початкові дані для розрахунку захисного заземлення:

– тип верхнього шару ґрунту – чорнозем, нижнього шару ґрунту – глина (питомий опір ρ_2 = 40 Ом·м);

– умовна товщина верхнього шару ґрунту: H=0,6 м;

– відстань між вертикальними заземлювачами (електродами) A=3 м;

– глибина закладення горизонтального контура заземлення t=0,75 м;

– опір заземлювача, який нормується: $R_{ЗН}$ = 4 Ом.

Необхідно визначити необхідну кількість вертикальних заземлювачів та довжину полоси (горизонтального заземлювача).

Виконаємо розрахунок.

Відстань від центра вертикального заземлювача до поверхні землі:

$$T= t + L/2 = 0,75 +2/2 =1,75 \text{ м.}$$

Розрахунковий питомий опір ґрунту (з врахуванням того, що фактично вся конструкція заземлювача розташовується у нижньому шарі ґрунту):

$$\rho = \psi \rho =1,36 \cdot 40=54,5 \text{ Ом·м.}$$

де

ψ = 1,36 – табличне значення коефіцієнта сезонності для відповідної кліматичної зони у багатошаровому ґрунті [10];

ρ_2= 40 Ом·м – табличне значення питомого опору нижнього шару ґрунту (глина) [10].

Діаметр вертикального електрода (заданий) Dв= 35 мм = 0,035 м.

Відношення A/L=3/2=1,5.

Опір розтіканню електричного струму одного електрода вертикального заземлювача з урахуванням заглиблення заземлювача [10]:

$$R_O=0,366 \cdot (\rho/L) \cdot [\lg(2L/Dв)+(1/2) \cdot \lg((4T+L)/(4T-L))]=$$

$$=0,366 \cdot (54,5/2) \cdot [(\lg(2 \cdot 2/0,035)+(1/2) \cdot \lg((4 \cdot 1,75+2)/(4 \cdot 1,75-2))]=21,7 \text{ Ом.}$$

Визначаємо коефіцієнт екранування вертикальних електродів Кев=0,53 при орієнтовній кількості вертикальних електродів, яке дорівнює 5 [10].

Визначаємо необхідну кількість вертикальних електродів заземлювача (без врахування горизонтального заземлювача), при $R_{ЗН}$ = 4 Ом:

$$N=R_О /(Кев\ R_{ЗН})= 21,7 / (0,53\cdot4)= 10,2 \approx 10 \text{ шт.}$$

Визначаємо довжину з'єднуючої полоси:

$$L_П =1,05\cdot A\cdot N= 1,05\cdot3\cdot10=32,3\approx 32 \text{ м.}$$

Опір розтіканню електричного струму з'єднуючої полоси з урахуванням кліматичного коефіцієнта питомого опору ґрунту $K_П$ [10]:

$$R_П =0,366\cdot(\rho\cdot K_П/L_П)\cdot\lg(2(L_П \cdot L_П)/(B\cdot t))=$$

$$=0,366\cdot(40\cdot5/40)\cdot\lg((2\cdot40^2)/(0,035\cdot0,75))=11,14 \text{ Ом.}$$

де $K_П$=5 – табличне значення кліматичного коефіцієнта питомого опору ґрунту для відповідної кліматичної зони для з'єднуючої полоси [10]:

B = 35 мм. = 0,035 м.- ширина з'єднуючої полоси (задана).

Загальний опір розтіканню електричного струму заземлювача [10]:

$$R =(R_О\cdot R_П)/(R_О\cdot\eta_П+ N\cdot R_П\cdot Кев)=$$

$$=(21,7\cdot 11,14)/(21,7\cdot 0,55+ 10\cdot 11,14\cdot 0,53)=3,4 \text{ Ом.}$$

де $\eta_П$ = 0,55 – табличне значення коефіцієнта екранування з'єднуючої полоси [10].

Умова $R \le R_{ЗН}$ виконується ($3,4 \le 4$).

Оскільки при 10 вертикальних електродах R суттєво більше $R_{ЗН}$, зменшимо кількість вертикальних електродів N до 9 і виконаємо перерахунок. У результаті остаточно отримали: R = 3,9 Ом. при кількості вертикальних електродів N = 9.

Висновки до розділу

Дотримання всіх необхідних умов праці не лише сприяє збереженню здоров'я працівників, а також підвищує ефективність виробництва в цілому.

З цих міркувань було здійснено аналіз приміщення, призначеного для праці програмістів, проведено розгляд питань пожежної безпеки, небезпечних та шкідливих факторів, що негативно впливають на програмістів під час роботи.

Тільки повна усвідомленість працівника про можливі небезпеки, що можуть підстерігати його на робочому місці та дотримання вимог нормативних актів о питань охорони праці та відповідних рекомендацій фахівців, дозволять значною мірою знизити негативний вплив шкідливих та небезпечних факторів при роботі з комп’ютером на організм людини.

Виконано розрахунок захисного штучного заземлення, як одного з ключових факторів безпеки програміста.

9 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи нейромережевих експертів безпечної маршрутизації у антивіруси.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти наведені теоретичне узагальнення й рішення наукового завдання дослідження методів нейромережевих експертів безпечної маршрутизації у антивіруси.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем нейромережевих експертів безпечної маршрутизації у антивіруси.

– Досліджена система нейромережевих експертів безпечної маршрутизації у антивіруси.

– На основі отриманих результатів досліджень створена програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання нейромережевих експертів безпечної маршрутизації у антивіруси.

Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня Python. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10/11.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм RSA.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Проведено маркетингове та економічне обґрунтування ІТ-проєкту, що дозволило визначити ключові фактори успіху даного проекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кіріченко Т.М. Дослідження та програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси // Збірник праць молодих науковців ЦНТУ. – Вип. 15. – Кропивницький: ЦНТУ, 2025.

2. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». *VII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення,* м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.

3. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 2(72), С. 170-178.

4. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings,* Volume 3187, 2022,

5. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». *Journal of Ambient Intelligence and Humanized Computing* Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.

6. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління,* № 2(70). 2022. С. 28-37.

7. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в

інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку,* 2022, № 3(69). С. 93-98.

8. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»,* № 2 (307). С. 46-52. 2022.

9. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.

10. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». *11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021,* Cracow, Poland, 22-25 September 2021. P. 414-418

11. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». *4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) – 2021*, Lviv, Ukraine, September 21-25, 2021. P. 255-260.

12. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». *2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020,* Kharkiv, 6 October 2020-9 October 2020, P. 358-362.

13. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». *CEUR Workshop Proceedings* Volume 2805, 2020, Pages *44-58.*

14. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.

15. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.

16. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.

17. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 122-131.

18. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 1-14.

19. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». *Lecture Notes in Networks and Systems*, vol 152. Springer, Cham. 2021, pp 66-84.

20. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 161-165.

21. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I.,Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT),* Ukraine, Kyiv, May 14-18. 2020. P. 166-171.

22. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT),* Ukraine, Kyiv, May 14-18. 2020. P. 172-177.

23. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.

24. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 125-136.

25. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». *International Journal of Computer Network and Information Security (IJCNIS)*. Vol. 12, No. 3, 2020. PP.33-43.

26. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», *CEUR Workshop Proceedings* Volume 2608, 2020, Pages 646-660.

27. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.

28. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T),* Kyiv, Ukraine, 8 – 11 October 2019. P.517-522.

29. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, Vol 2588, P. 215-227, 2019.

30. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». *CEUR Workshop Proceedings*, Vol 2588, P. 90-106, 2019.

31. Smirnov, O., Kuznetsov, A., Kiian, A., Gorbenko, Y., Cherep, O., Bexhter L. «Code-based Pseudorandom Generator for the Post-Quantum Period», *2019 IEEE International Conference on Advanced Trends in Information Theory (IEEE ATIT 2019).* 18.12.19-20.12.19 Kyiv Ukraine. P. 204 – 209.

32. Smirnov, O., Kuznetsov, A., Nariezhnii, O., Stelnyk, S., Kokhanovska, T., Kuznetsova T., «Side Channel Attack on a Quantum Random Number Generator», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*; Metz; France; 18 - 21 September 2019. P.713-718.

33. Kuznetsova, T., «Code-Based Schemes for Post-Quantum Digital Signatures», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019;* Metz; France; 18-21 September 2019. P. 707-712.

34. Smirnov, O., Kuznetsov, A., Stefanovych, O., Gorbenko, Y., Krasnobaev, V., Kuznetsova K. «Information Hiding Using 3D-Printing Technology», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*; Metz; France; 18-21 September 2019. P.701-706.

35. Smirnov, O., Hu, Z., Vasiliu, Y., Sydorenko, V., Polishchuk, Y., «Abstract Model of Eavesdropper and Overview on Attacks in Quantum Cryptography Systems», *10th IEEE International Conference on Intelligent Data Acquisition and*

Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P.399-405.

36. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019*/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.

37. Smirnov, O., Kuznetsov, A., Kiian, A., Babenko, B., Zhosan, H., Prokopovych-Tkachenko, D., «Soft Decoding Method for Turbo-Productive Codes», *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019*, Lviv, Ukraine, 2-6 July, 2019, P. 129-134.

38. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 353-358.

39. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 347-352.

40. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», *CEUR Workshop Proceedings* Volume 2353, *CEUR Workshop Proceedings* 2019, Pages 618-629.

41. Smirnov, O., Kuznetsov, A., Kiian, A., Kuznetsova, K., Ivko, T., Prokopovych-Tkachenko, D., «Soft Decoding Based on Ordered Subsets of Verification Equations of Turbo-Productive Codes», *CEUR Workshop Proceedings* Volume 2353, *CEUR Workshop Proceedings* 2019, Pages 873-884.

42. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention

systems», *Telecommunications and Radio Engineering*. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.

43. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New Technique for Hiding Data in Cover Images Using Adaptively Generated Pseudorandom Sequences». *CEUR Workshop Proceedings* Volume 2732, 2020, Pages 214-227.

44. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. «Вступ до кібербезпеки»: навчальний посібник – Кропивницький: ЦНТУ – 2022. – 968 с.

45. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник / [В.М. Петрик, С.О. Гнатюк, М.М. Присяжнюк та ін.]; за заг. ред. С.О. Гнатюка, В.М. Петрика та О.А Смірнова. – Полтава, 2022. – 334 с.

46. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019*; Odessa; Ukraine; 9-13 September 2019. P.22-28.

47. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.

48. О.А. Смірнов, П.С. Усік, «Дослідження перспектив використання технологічних рішень в мережах 5G» у *Кібербезпека та інформаційні технології: монографія.* – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.

49. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.

50. Smirnov, O., Kuznetsov, A., Shekhanin, K., Chepurko, I. Detecting Hidden Information in FAT. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 412-429. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook)

51. Smirnov, O., Kuznetsov, A., Kuznetsova., K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).

52. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.

53. Смірнов О.А., Стасєв Ю.В., Бараннік В.В. Коваленко О.В., Доренський О.П., Дрєєв О.М., Вялкова В.І. Інформаційна безпека держави. Підручник – Кіровоград: РВЛ КНТУ, 2016. – 263 с

54. Смірнов О.А., Кавун С.В., Коваленко О.В., Дрєєв О.М. Мережні інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.

55. Смірнов О.А., Кавун С.В., Коваленко О.В., Доренський О.П., Дрєєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.