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
“____” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“Дослідження та програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів”

Виконав здобувач вищої освіти
ІІ курсу, групи КН-25М
ОПП «Комп’ютерні науки»
спеціальності F3 «Комп’ютерні науки»
_____ Мельник І.В.
«____» _____ 2026 р.

Керівник проекту
доктор технічних наук, професор
_____ Смірнов О.А.
«____» _____ 2026 р.

Нормоконтроль проекту
_____ Коваленко А.С.
«____» _____ 2026 р.

Рецензент _____
_____

Підписано КЕП
Центральноукраїнський національний технічний університет
Мельник Ілля Вадимович
Сертифікат: 514B5C86A1E5DA11040000007A800800492DF705
Дійсний з 21.07.2026 23:51:29 по 21.07.2027 23:51:28

Центральноукраїнський національний технічний університет
Факультет *Механіко-технологічний*
Кафедра *Кібербезпеки та програмного забезпечення*
Рівень вищої освіти *магістр*
Галузь знань _F_____*"*Інформаційні технології*"*_____
Спеціальність F3 *"*Комп'ютерні науки*"*
Освітньо-професійна (освітньо-наукова) програма _*"*Комп'ютерні науки*"*_

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.т.н., проф.
_____ Олексій СМІРНОВ
« 1 » вересня 2026 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ДРУГИМ (МАГІСТЕРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Мельнику Іллі Вадимовичу
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження та програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів*

2. Керівник роботи *Смірнов Олексій Анатолійович, доктор технічних наук, професор*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 42-13 від 17.08.2026 року

3. Строк подання студентом роботи до захисту *2.12.2026 р.*

4. Мета та завдання випускної кваліфікаційної роботи*: Метою розробки є дослідження та програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів*

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Призначення та область використання.	*5. Впровадження системи в промислову експлуатацію*
2. Перегляд аналогічних існуючих систем.	*6. Наукова новизна.*
3. Опис і обґрунтування проектних рішень.	*7. Заходи з охорони праці та техніки безпеки.*
4. Етапи програмування системи.	*8. Висновки.*

6. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Наукова новизна	*1 аркуш*
Структурна схема системи	*1 аркуш*
Функціональна схема системи	*1 аркуш*
Діаграма процесів	*1 аркуш*
Блок-схема алгоритму роботи додатку	*2 аркуша*

7. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Марченко К.М., к.т.н., доцент	06.10.2026	16.11.2026

8. Дата видачі завдання « 1 » вересня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.10.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.10.2026 р.	
3.	Розробка моделі компонента	20.10.2026 р.	
4.	Розробка структур даних	25.10.2026 р.	
5.	Розробка алгоритмів системи	30.10.2026 р.	
6.	Програмування алгоритмів	10.11.2026 р.	
7.	Розрахунки з охорони праці та техніки безпеки	15.11.2026 р.	
8.	Оформлення ПЗ	17.11.2026 р.	
9.	Попередній захист роботи	2.12.2026 р.	

Дата видачі завдання
« 1 » вересня 2026 р.

Підпис керівника

_____ _____
(прізвище та ініціали)

Завдання прийнято до виконання
« 1 » вересня 2026 р.

Підпис здобувача

_____ _____
(прізвище та ініціали)

АНОТАЦІЯ

Мельник І.В. Дослідження та програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів. ФЗ Комп'ютерні науки. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Метою розробки є дослідження та програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Об'єктом дослідження є процес інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Предметом дослідження є методи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Методи дослідження базуються на методах побудови нейронних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

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, нейромережеві експерти, антивірусний комплекс

ABSTRACT

Melnyk I.V. Research and Software Implementation of an Intelligent Threat Analysis System Based on an Ensemble of Neural Network Experts for Antivirus Complexes. F3 Computer Science. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

This master's-level final qualification thesis presents the development of software designed for an intelligent threat analysis system based on an ensemble of neural network experts for antivirus complexes.

The objective of this development is the research and software implementation of an intelligent threat analysis system based on an ensemble of neural network experts for antivirus complexes.

The object of the research is the process of intelligent threat analysis based on an ensemble of neural network experts for antivirus complexes.

The subject of the research consists of methods for intelligent threat analysis based on an ensemble of neural network experts for antivirus complexes.

The research methodology draws upon techniques for constructing neural networks, mathematical statistics, and software development.

The outcome of the work is a software implementation of an intelligent threat analysis system based on an ensemble of neural network experts for antivirus complexes.

During the development of the software model, an analysis of existing hardware and software tools was conducted. All components of the developed software are described in detail.

A user-friendly interface has been developed. Instructions for operating the software are provided. The program can be used on PCs running Windows 10/11.

The program was developed in a Python environment.

Keywords: computer science, neural network-based expert systems, antivirus complex

ВІДОМІСТЬ ПРОЕКТУ

		Текстові документи			
1	А4	Пояснювальна записка	80	–	
2	А4	Робоча програма	45	–	Додаток А
		Графічні документи			
3	А4	Наукова новизна	1	–	
4	А4	Структурна схема	1	–	
5	А4	Функціональна схема роботи системи	1	–	
6	А4	Діаграма взаємодії процесів	1	–	
7	А4	Блок-схема основної програми	1	–	
8	А4	Блок-схема роботи підпрограми	1	–	

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ 9
ВСТУП..... 10
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ 12
1.1 Призначення системи..... 12
1.2 Область застосування 12
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ 14
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти..... 14
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування 19
2.3 Розгорнута постановка завдання 20
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ 22
3.1 Опис функціонування системи 22
3.2 Розробка структурної схеми..... 29
3.3 Розробка функціональної схеми 37
3.4 Розробка діаграми процесів 40
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ 42
4.1 Розробка блок-схем та опис алгоритмів функціонування системи 42
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ..... 56
6 НАУКОВА НОВИЗНА 61

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ 62
7.1 Вступ 62
7.2 Шкідливі і небезпечні фактори при роботі з комп’ютером 63
7.3 Аналіз санітарно-гігієнічних умов праці
на робочому місці користувача ПК 64
7.4 Розробка заходів з умов поліпшення охорони праці 66
7.5 Протипожежний захист 68
7.6 Розрахункова частина 69
8 ОСНОВНІ ВИСНОВКИ 71
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 73

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. Загрози шкідливого програмного забезпечення стають дедалі динамічнішими та складнішими, і, відповідно, методи штучного інтелекту стали центральним елементом захисту інформації, оскільки вони вважаються більш придатними для боротьби з сучасними інцидентами, пов'язаними зі шкідливим програмним забезпеченням. Зокрема, нейронні мережі, завдяки своїй високій здатності до узагальнення, здатні вирішувати широкий спектр кіберзагроз. У даній роботі описується розробка та тестування підходу до виявлення шкідливого програмного забезпечення на основі ансамблю нейронних мереж, заснованого на гібридному механізмі пошуку. У цьому механізмі оптимізація окремих мереж здійснюється за допомогою адаптивного меметичного алгоритму з забороненим пошуком, який також використовується для покращення прихованих нейронів та ваг нейронних мереж. Адаптивний меметичний алгоритм поєднує методи глобальної та локальної оптимізації пошуку, щоб подолати передчасну конвергенцію та отримати оптимальний результат пошуку. Результати тестування доводять, що запропонований метод є сильно адаптивним та ефективним у виявленні низки загроз шкідливого програмного забезпечення, і що він генерує кращі результати, ніж інші існуючі методи.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

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

– Огляд існуючих систем інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

– Дослідження системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

– Програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Об'єктом дослідження є процес інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Предметом дослідження є методи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Методи дослідження базуються на методах побудови нейронних мереж, методах математичної статистики, методах розробки програмного забезпечення.

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

– Удосконалено метод інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

– Розроблено вітчизняний продукт інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

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 LVIII науково-технічній конференції здобувачів вищої освіти «Наука-виробництву», основні положення випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти надруковані у статті збірника праць молодих науковців ЦНТУ, випуск №17.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів, 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

У сучасному світі цифрових технологій кібербезпека стала важливішою, ніж будь-коли. Оскільки мережі стають більшими та складнішими, вони також стають більш вразливими до дедалі витонченіших кібератак. Традиційні системи, такі як засоби виявлення вторгнень на основі правил, часто намагаються встигати за зміною загроз. Машинне навчання (ML) стало перспективним рішенням, пропонуючи можливість навчатися на минулих моделях та інтелектуально виявляти підозрілу активність у режимі реального часу [1, 2]. Однак, покладаючись на один алгоритм, часто відбувається обмежена продуктивність, оскільки кожна модель має свої сильні та слабкі сторони. Наприклад, методи опорних векторів (SVM) ефективні для структурованих даних, але можуть пропускати нелінійні зв'язки [3, 4]. Глибокі нейронні мережі (DNN) є потужними, але вимагають великого обсягу даних та часу на навчання [5, 6]. Випадкові ліси стійкі до шуму, але можуть вносити упередженість, якщо їх неправильно налаштувати [7]. Завдання полягає в розробці систем, які збалансують ці відмінності, щоб приймати розумніші та надійніші рішення, особливо в середовищах з високими ставками, таких як інформаційна безпека.

1.2 Область застосування

Хоча ансамблеве навчання вивчалося в кібербезпеці, більшість існуючих досліджень застосовують або однорідні ансамблі (наприклад, кілька дерев рішень), або зосереджуються на гібридних моделях з двох моделей. Наш підхід базується на цій основі, але розвиває її у трьох важливих напрямках:

По-перше, ми використовуємо гетерогенний ансамбль із трьох різноманітних класифікаторів: Random Forest, SVM та DNN, призначених для фіксації як лінійних зв'язків, так і складної нелінійної поведінки атак.

По-друге, ми оцінюємо модель на кількох наборах даних для оцінки стійкості та надійності в різних середовищах, тоді як багато попередніх робіт обмежуються валідацією на одному наборі даних.

По-третє, наші порівняльні результати показують, що хоча окремі моделі, такі як логістична регресія, досягають дещо вищої точності, запропонований ансамбль пропонує найкращий показник AUC (за шкалою AUC), демонструючи сильнішу здатність балансувати точність і повноту, а також зменшувати кількість хибних тривог.

Ці досягнення підкреслюють внесок цього дослідження у вихід за межі існуючих ансамблевих конструкцій у напрямку більш узагальненої та практично корисної системи виявлення вторгнень.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів, 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 той час як традиційне антивірусне програмне забезпечення довгий час спиралося на бази даних сигнатур та евристичний аналіз, нові рішення на основі штучного інтелекту, такі як Aegis AI, переосмислюють методи виявлення та нейтралізації загроз. Дебати щодо Aegis AI та традиційного антивірусного програмного забезпечення у 2026 році стосуються не лише технологій, а й адаптивності, ефективності та майбутнього цифрової безпеки. Оскільки кіберзагрози стають дедалі складнішими, обмеження застарілих систем стають очевидними, змушуючи підприємства та споживачів переглянути свій захист.

Перехід не є плавним. Традиційні постачальники антивірусів десятиліттями вдосконалювали свої продукти, створюючи екосистеми перевірених брендів, які домінують на ринку. Однак зростання популярності інструментів безпеки на базі штучного інтелекту сигналізує про сейсмічний зсув. Наприклад, Aegis AI використовує машинне навчання для прогнозування та перехоплення загроз у режимі реального часу, що є можливістю, з якою традиційне антивірусне програмне забезпечення ледве справляється. Питання не в тому, чи замінить штучний інтелект застарілі системи, а в тому, як швидко організації впровадять ці рішення наступного покоління, і що це означає для кібербезпеки в цілому.

До 2026 року розрив між штучним інтелектом Aegis та традиційним антивірусним програмним забезпеченням буде більшим, ніж будь-коли. У той час як традиційні рішення продовжують спиратися на статичні визначення та реактивні заходи, платформи на базі штучного інтелекту вбудовують контекстуальну обізнаність у свою основну архітектуру. Це не просто

оновлення; це фундаментальне переосмислення того, як працює безпека. Ставки високі, і вибір, який організації роблять сьогодні, визначатиме їхню стійкість завтра.

Повний огляд Aegis AI у порівнянні з традиційним антивірусним програмним забезпеченням 2026 року

Ландшафт кібербезпеки у 2026 році визначається двома домінуючими силами: усталеним домінуванням традиційного антивірусного програмного забезпечення та революційним потенціалом альтернатив на базі штучного інтелекту, таких як Aegis AI. Традиційні антивірусні рішення, засновані на виявленні на основі сигнатур та поведінковому аналізі, були основою кібербезпеки протягом десятиліть. Вони чудово виявляють відомі варіанти шкідливого програмного забезпечення, але не справляються з експлойтами нульового дня та поліморфними загрозами. На противагу цьому, Aegis AI являє собою зміну парадигми, де безпека є не просто реактивною, а прогнозною, адаптивною та глибоко інтегрованою в цифрову екосистему.

Основна суперечність між Aegis AI та традиційним антивірусним програмним забезпеченням 2026 року полягає в їхніх фундаментальних підходах. Традиційний антивірус спирається на базу даних сигнатур загроз, яка періодично оновлюється для відповідності новим штамам шкідливого програмного забезпечення. Цей метод ефективний для відомих загроз, але залишає вразливості для нових ризиків. Однак Aegis AI використовує моделі машинного навчання в реальному часі, навчені на величезних наборах даних про кіберзагрози, що дозволяє йому виявляти аномалії та закономірності, які традиційні системи пропускають. Результат? Позиція безпеки, яка розвивається разом із ландшафтом загроз, а не відстає від нього.

Історична довідка та еволюція

Витоки традиційного антивірусного програмного забезпечення сягають 1980-х років, коли перші спалахи шкідливих програм змусили розробників створювати інструменти, здатні сканувати файли на наявність шкідливого коду. Ранні антивірусні програми були рудиментарними, спираючись на просте

зіставлення зі шаблонами для ідентифікації вірусів. З часом вони еволюціонували, включивши евристичний аналіз, пісочницю та хмарну аналітику загроз, але їхній основний механізм залишився незмінним: виявлення відомих загроз на основі заздалегідь визначених правил.

На противагу цьому, рішення безпеки на основі штучного інтелекту, такі як Aegis AI, виникли завдяки досягненням у машинному навчанні та аналітиці великих даних. Ці системи були розроблені для динамічного навчання на кіберзагрозах, зменшуючи залежність від статичних сигнатур. Перехід до штучного інтелекту в кібербезпеці набрав обертів у 2010-х роках, коли організації зіткнулися з експоненціальним зростанням складних атак, включаючи програми-вимагачі, передові постійні загрози (APT) та безфайлове шкідливе програмне забезпечення. Традиційне антивірусне програмне забезпечення, хоча й залишається актуальним, почало демонструвати свої обмеження в епоху, коли загрози мутують з безпрецедентною швидкістю.

Основні механізми: як це працює

Традиційне антивірусне програмне забезпечення працює за простим принципом: воно порівнює файли та поведінку системи з базою даних відомих сигнатур шкідливих програм. Коли знайдено збіг, програма або поміщає загрозу в карантин, або видаляє її. Цей метод дуже ефективний для добре задокументованого шкідливого програмного забезпечення, але неефективний проти невідомих або загроз, що розвиваються. Крім того, традиційні антивіруси часто покладаються на ресурсомістке сканування, що може погіршити продуктивність системи, особливо на старому обладнанні.

З іншого боку, Aegis AI використовує глибоке навчання та нейронні мережі для аналізу поведінки, контексту та закономірностей у режимі реального часу. Замість того, щоб чекати на виявлення та каталогізацію загрози, Aegis AI постійно відстежує активність системи, позначаючи аномалії, що відхиляються від нормальної поведінки. Такий проактивний підхід дозволяє виявляти експлойти нульового дня, внутрішні загрози та навіть складні атаки соціальної інженерії, перш ніж вони завдадуть шкоди. Система також адаптується з часом,

покращуючи свою точність, коли стикається з новими загрозами, роблячи її набагато стійкішою до порівнянь Aegis AI та традиційного антивірусного програмного забезпечення 2026 року.

Ключові переваги та вирішальний вплив

Дебати щодо Aegis AI проти традиційного антивірусного програмного забезпечення 2026 року стосуються не лише технічної переваги, а й реального впливу на безпеку, продуктивність та взаємодію з користувачем. Традиційні антивірусні рішення вже давно критикують за високий рівень хибнопозитивних результатів, що може призвести до непотрібних збоїв та розчарування користувачів. Aegis AI пом'якшує цю проблему, зменшуючи залежність від жорстких правил та натомість зосереджуючись на контекстному розумінні, що призводить до меншої кількості хибних тривог та більш плавного взаємодії з користувачем.

Більше того, масштабованість безпеки на основі штучного інтелекту не має собі рівних. Традиційні антивірусні системи ледве справляються з обсягом та складністю сучасних загроз, часто вимагаючи ручних оновлень та виправлень. Однак Aegis AI масштабується без зусиль, обробляючи мільйони точок даних у режимі реального часу без погіршення продуктивності. Ця можливість особливо важлива для підприємств з величезними розподіленими мережами, де традиційні антивіруси можуть не забезпечити повного покриття.

Основні переваги:

– Проактивне виявлення загроз: Aegis AI виявляє загрози до їх виконання, тоді як традиційний антивірус реагує на відомі сигнатури.

– Адаптивне навчання: моделі штучного інтелекту з часом удосконалюються, зменшуючи кількість хибнопозитивних результатів та підвищуючи точність у порівняннях Aegis AI та традиційного антивірусного програмного забезпечення у 2026 році.

– Зменшення системних накладних витрат: Традиційний антивірус часто уповільнює роботу систем через часте сканування; Aegis AI ефективно працює у фоновому режимі.

– Захист від загроз нульового дня: Традиційний антивірус безпорадний проти невідомих загроз; Aegis AI виявляє аномалії, які вказують на експлойти нульового дня.

– Розгортання корпоративного масштабу: Безпека на основі штучного інтелекту легко масштабується в глобальних мережах, на відміну від традиційних антивірусів, які можуть мати проблеми із затримкою та покриттям.

Майбутні тенденції та інновації

До 2026 року дебати щодо Aegis AI та традиційного антивірусного програмного забезпечення перестануть бути двостороннім вибором, а радше питанням інтеграції. Платформи безпеки на базі штучного інтелекту, такі як Aegis AI, будуть дедалі частіше розгортатися разом із традиційними антивірусами для створення гібридних систем захисту. Такий підхід використовує сильні сторони обох – прогностичних можливостей штучного інтелекту та перевіреного досвіду традиційного антивіруса у виявленні відомих загроз.

Нові тенденції свідчать про те, що ШІ також відіграватиме більшу роль в обміні інформацією про загрози, де організації співпрацюють для внесення колективних даних про загрози до централізованих моделей ШІ. Такий спільний підхід може ще більше знизити ефективність традиційних антивірусів, зробивши захист на основі ШІ більш надійним. Крім того, досягнення в квантових обчисленнях можуть вимагати переоцінки стандартів шифрування, висуваючи безпеку на основі ШІ на перший план як єдине життєздатне рішення для постквантових загроз.

Висновок

Ландшафт антивірусного програмного забезпечення Aegis зі штучним інтелектом та традиційним програмним забезпеченням у 2026 році швидко змінюється, і рішення на основі штучного інтелекту готові домінувати в епоху дедалі складніших кіберзагроз. Традиційний антивірус не зникне за одну ніч, але його роль переміститься з основного захисту на додатковий рівень у багатогранній стратегії безпеки. Організації, які не адаптуються, ризикують

стати жертвами атак, яким традиційний антивірус сам по собі не може запобігти.

Ключовий висновок очевидний: майбутнє належить адаптивній безпеці на базі штучного інтелекту. Aegis AI та подібні платформи представляють собою наступне покоління кібербезпеки, пропонуючи неперевершений захист як від відомих, так і від невідомих загроз. З наближенням 2026 року вибір між штучним інтелектом та традиційним антивірусом стосується не лише технологій, а й виживання у дедалі ворожішому цифровому світі.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Для розробки програмних модулів інтелектуального виявлення кіберзагроз, побудови ансамблів нейромережевих експертів та інтеграції в сучасні антивірусні комплекси обрано мову програмування Python. Це високорівнева мультиплатформна мова загального призначення, яка посідає провідні позиції у сфері розробки програмного забезпечення, штучного інтелекту та машинного навчання (Machine Learning).

Python є інтерпретованою об'єктно-орієнтованою мовою з динамічною типізацією, що забезпечує гнучкість передачі даних, високу швидкість прототипування та зручність інтеграції різнорідних алгоритмів. До ключових переваг мови належать:

– Простий і логічний синтаксис: забезпечує легкість читання коду та мінімізує ймовірність помилок під час реалізації складних нейромережевих архітектур.

– Об'єктна модель: код організовується у вигляді модулів і пакетів із підтримкою повної інтроспекції та аналізу структури об'єктів під час виконання.

– Масштабованість і розширюваність: можливість швидкого адаптування високорівневої логіки та оптимізації ресурсомістких обчислень за рахунок підключення низькорівневих бібліотек (C/C++).

– Розвинена екосистема: наявність потужних спільнот і спеціалізованих

інструментів для обробки великих масивів даних.

До умовних недоліків мови зазвичай відносять вищі вимоги до обчислювальних ресурсів та меншу швидкість виконання порівняно з компільованими мовами (наприклад, C++). Проте в задачах побудови інтелектуальних систем аналізу загроз швидкість розробки, гнучкість налаштування та можливість швидкого перенавчання моделей мають критично важливіший пріоритет.

Для реалізації алгоритмів інтелектуального аналізу поведінки шкідливого ПЗ та класифікації векторів атак використовується низка профільних бібліотек Python:

– NumPy та Pandas: забезпечують ефективне створення багатовимірних масивів, керування пам'яттю та зручну обробку структурованих наборів даних (датасетів телеметрії безпеки).

– Scikit-learn, PyTorch / TensorFlow: базові фреймворки для розробки, навчання та оптимізації ансамблів нейромережевих експертів, класифікаторів і рекурентних мереж виявлення аномалій.

– Requests та Matplotlib: застосовуються для взаємодії із зовнішніми API аналізу загроз (Threat Intelligence) та візуалізації метрик ефективності антивірусного комплексу (ROC-криві, матриці помилок).

Для організації середовища розробки та супроводу програмного забезпечення застосовуються професійні середовища інтегрованого типу, зокрема PyCharm, а також універсальні редактори коду (Visual Studio Code, Spyder), які забезпечують зручне відлагодження, тестування та управління проєктами кіберзахисту.

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 інтелектуального аналізу загроз на

основі ансамблю нейромережевих експертів для антивірусних комплексів.

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

Розуміння ансамблевих моделей у сфері безпеки ШІ: комплексне визначення

Ансамблеві моделі в системі штучного інтелекту безпеки представляють собою складний підхід до виявлення та реагування на загрози, який поєднує кілька методів штучного інтелекту для створення більш надійних, точних та надійних результатів безпеки. Замість того, щоб покладатися на одну методологію ШІ, ансамблеві моделі використовують сильні сторони різних технологій, включаючи моделі великих мов програмування (LLM), статистичний аналіз та системи на основі правил, для подолання індивідуальних обмежень та забезпечення передових можливостей виявлення для сучасних центрів операцій безпеки (SOC). Для керівників сфери безпеки та осіб, які приймають рішення у сфері безпеки, які керують корпоративними середовищами, розуміння ансамблевих моделей стало критично важливим, оскільки ландшафти загроз стають дедалі складнішими, а традиційні однометодні підходи виявляються недостатніми проти передових стійких загроз.

Що таке ансамблева модель у безпеці ШІ?

Ансамблева модель у контексті штучного інтелекту безпеки визначається як метод машинного навчання, який поєднує прогнози з кількох різних моделей ШІ для створення єдиного, точнішого результату. Уявіть собі це як консультацію з кількома експертами з безпеки перед прийняттям остаточного рішення щодо потенційної загрози, кожен експерт має різний досвід і перспективу, і разом вони доходять до кращих висновків, ніж будь-який окремий експерт міг би зробити самостійно.

Фундаментальний принцип, що лежить в основі ансамблевих моделей, полягає в тому, що різноманітні підходи компенсують слабкі сторони один

одного. Статистична модель може досягати успіху у виявленні аномалій у моделях мережевого трафіку, але мати труднощі з контекстним розумінням. Тим часом LLM може розуміти складні взаємозв'язки та природну мову, але може не мати точності систем, заснованих на правилах. Поєднуючи ці підходи, ансамблеві моделі досягають можливостей виявлення, які перевищують те, що може забезпечити будь-який окремий компонент.

Для операцій безпеки це означає меншу кількість хибнопозитивних результатів, краще виявлення нових моделей атак і більше дієвих сповіщень, на які аналітики безпеки можуть діяти з упевненістю. Ансамбльний підхід вирішує одну з найпостійніших проблем у сфері штучного інтелекту безпеки: балансування чутливості (виявлення реальних загроз) зі специфічністю (уникнення хибних тривог).

Основні компоненти ансамблевих моделей штучного інтелекту безпеки

Моделі ансамблю штучного інтелекту в галузі безпеки зазвичай інтегрують три основні типи інтелектуальних систем, кожна з яких має унікальні можливості:

– Моделі великих мов (LLM): ці нейронні мережі обробляють і розуміють природну мову, що дозволяє їм аналізувати журнали безпеки, звіти про загрози та документацію з розумінням, подібним до людського. LLM чудово виявляють зв'язки між, здавалося б, не пов'язаними подіями та розуміють контекстуальні нюанси в даних безпеки.

– Статистичні моделі та моделі машинного навчання: ці системи виявляють закономірності, аномалії та кореляції в числових даних. Вони особливо ефективні для встановлення базових ліній, виявлення відхилень та кількісної оцінки ризиків на основі історичних закономірностей та розподілів ймовірностей.

– Системи на основі правил: ці детерміновані механізми застосовують визначену експертами логіку та відомі сигнатури атак для класифікації загроз. Вони надають зрозумілі, узгоджені рішення на основі встановлених принципів

безпеки та вимог до відповідності.

Оркестрація цих компонентів створює систему виявлення, яка є одночасно інтелектуальною та надійною, поєднуючи адаптивність систем навчання з узгодженістю логіки на основі правил.

Пояснення того, як ансамблеві моделі працюють в операціях безпеки

Ансамблеві моделі в ШІ безпеки працюють за допомогою кількох різних методологічних підходів, кожен з яких пропонує різні переваги для робочих процесів виявлення та реагування на загрози.

Ансамблеві методи на основі голосування

Найпростіша форма ансамбльового моделювання використовує механізми голосування, де кілька моделей аналізують одну й ту саму подію безпеки та голосують за її класифікацію. Сповіщення безпеки може бути оцінене за допомогою LLM, що аналізує описи журналів, статистичної моделі, що оцінює моделі поведінки, та системи на основі правил, яка перевіряє відомі сигнатури атак.

При голосуванні більшістю обирається класифікація, яка отримує найбільше голосів, тоді як при зваженому голосуванні кожній моделі присвоюється різна важливість на основі її історичної точності для конкретних типів загроз. Цей підхід особливо добре працює, коли моделі мають взаємодоповнюючі сильні сторони, наприклад, системи на основі правил можуть мати більшу вагу для відомих шаблонів атак, тоді як моделі виявлення аномалій отримують вищу вагу для загроз нульового дня.

Підходи до стекування та мета-навчання

Більш складні ансамблеві архітектури використовують стекування, де метамодель навчається оптимально комбінувати результати базових моделей. Базові моделі (LLM, статистична та заснована на правилах) роблять свої індивідуальні прогнози, і ці прогнози стають вхідними даними для моделі вищого рівня, яка навчається найкращому способу їх комбінування для остаточної класифікації. Цей підхід метанавчання є особливо потужним, оскільки він може вивчати контекстно-залежні стратегії комбінування.

Ансамбль може дізнатися, що для певних типів сповіщень, таких як потенційне витікання даних, оцінка статистичної моделі повинна мати більшу вагу, тоді як для спроб соціальної інженерії розуміння природної мови LLM стає більш критичним.

Підвищення та послідовне навчання

Методи підвищення кваліфікації навчають моделі послідовно, причому кожна наступна модель зосереджується на випадках, коли попередні моделі працювали погано. Для операцій безпеки це означає, що ансамбль постійно покращує свою здатність виявляти найскладніші сценарії загроз, ті малопомітні атаки, які окремі моделі можуть пропустити.

Ансамбль підсилення може починатися з виявлення на основі правил, потім застосовувати статистичний аналіз до випадків, які не відповідають відомим шаблонам, і, нарешті, використовувати можливості LLM для найбільш неоднозначних ситуацій, що потребують контекстного мислення. Таке послідовне уточнення створює глибину виявлення, яка значно зменшує кількість хибнонегативних результатів.

Чому ансамблеві моделі важливі для сучасних операцій безпеки

Перехід до ансамблевих моделей у сфері штучного інтелекту безпеки відображає фундаментальні зміни як у ландшафті загроз, так і у вимогах до безпеки організацій. Одномодельні підходи дедалі більше намагаються відповідати вимогам, що ставляться до сучасних систем охорони праці (SOC).

Вирішення проблеми хибнопозитивних результатів

Команди безпеки стикаються з величезною кількістю сповіщень, причому традиційні системи генерують рівень хибнопозитивних спрацьовувань, який може перевищувати 90%. Аналітики відчувають втому від сповіщень, що змушує їх пропускати справжні загрози, приховані в шумі. Ансамблеві моделі значно зменшують кількість хибнопозитивних спрацьовувань, вимагаючи узгодження між кількома методологіями виявлення перед викликом високопріоритетних сповіщень. Коли система на основі правил позначає підозрілу активність, але статистичний аналіз показує, що поведінка відповідає

нормам для цього користувача, а оцінка LLM виявляє легітимний бізнес-контекст, ансамбль може впевнено знизити пріоритет сповіщення. Така багатоперспективна перевірка гарантує, що аналітики витрачають час на розслідування справжніх загроз, а не на пошук хибних слідів.

Виявлення нових та таких, що розвиваються, загроз

Розширені постійні загрози та атаки нульового дня не відповідають відомим сигнатурам, що робить чисте виявлення на основі правил неефективним. Статистичні моделі можуть виявляти аномалії, але їм часто бракує контексту, щоб відрізнити шкідливі відхилення від доброякісної незвичайної поведінки. LLM забезпечують контекстуальне розуміння, але їх можна обдурити складними методами обфускації.

Ансамблеві моделі чудово виявляють нові загрози, оскільки вони оцінюють підозрілу активність одночасно з кількох точок зору. Атака, яка уникає виявлення на основі правил, може викликати статистичні аномалії, тоді як LLM виявляє підозрілі мовні шаблони у пов'язаних комунікаціях. Таке поєднання виявляє загрози, які жодна окрема модель не виявила б.

Відповідність вимогам щодо пояснюваності

Рішення щодо безпеки часто потребують обґрунтування з міркувань відповідності, юридичних або операційних причин. Чисто нейронні мережеві підходи можуть бути непрозорими «чорними скриньками», що ускладнює пояснення того, чому було прийнято певне рішення. Ансамблеві моделі, що включають компоненти на основі правил, забезпечують пояснювальні ланцюжки міркувань, водночас використовуючи можливості передового штучного інтелекту.

Коли ансамблева модель позначає загрозу, вона може надати багатогранні пояснення: які правила були порушені, які статистичні аномалії були виявлені та які контекстуальні фактори визначила LLM. Така прозорість будує довіру з командами безпеки та задовольняє вимоги аудиту.

Стратегії впровадження ансамблевих моделей у сфері безпеки та штучного інтелекту

Розгортання ансамблевих моделей у виробничих середовищах безпеки вимагає ретельного планування та архітектурних рішень, які балансують продуктивність виявлення з операційними обмеженнями.

Вибір моделей компонентів для вашого ансамблю

Не всі сценарії безпеки мають однаковий ансамбльовий склад. Оптимальна комбінація залежить від конкретного профілю загроз вашої організації, джерел даних та операційних обмежень. Для організацій, які надають пріоритет вимогам до дотримання вимог та нормативних актів, ансамблі можуть надавати більшої ваги компонентам, що базуються на правилах, щоб забезпечити послідовне застосування політик. Компанії, що стикаються з передовими постійними загрозами, можуть наголосити на компонентах виявлення аномалій та LLM, які чудово виявляють малопомітні, складні атаки. Ключовим є відповідність архітектури ансамблю фактичним потребам безпеки, а не пошук універсальних рішень.

Архітектура конвеєра даних

Ансамблеві моделі вимагають надійної інфраструктури даних, яка може одночасно забезпечувати роботу кількох систем штучного інтелекту, зберігаючи при цьому низьку затримку для виявлення загроз у режимі реального часу. Зазвичай це включає:

– Нормалізоване отримання даних: перетворення різноманітних форматів журналів, сповіщень та сигналів безпеки на стандартизовані представлення, які можуть обробляти всі моделі компонентів.

– Паралельні конвеєри обробки: Забезпечення одночасного аналізу за допомогою різних типів моделей без створення вузьких місць

– Збагачення контексту: доповнення необроблених даних безпеки додатковим контекстом (ролі користувачів, критичність активів, розвідка про загрози), що покращує прийняття рішень у сукупності.

– Цикли зворотного зв'язку: фіксація рішень аналітиків для постійного покращення продуктивності моделі за допомогою контрольованого навчання.

Тренування та налаштування ансамблю

Ефективні ансамблеві моделі вимагають постійного навчання, яке виходить за рамки налаштування окремих компонентів. Логіка комбінацій на метарівні потребує оптимізації на основі реальної продуктивності у вашому конкретному середовищі.

Це включає створення наборів даних про підтверджені істинно позитивні та хибнопозитивні результати, а потім їх використання для оптимізації вагових коефіцієнтів ансамблю та стратегій комбінування. Багато організацій починають з консервативних ансамблів, які надають пріоритет точності (мало хибнопозитивних результатів) та поступово підвищують чутливість, оскільки вони формують довіру до системи та встановлюють механізми зворотного зв'язку.

Ансамблеві моделі в операціях AI SOC

Застосування ансамблевих моделей є значним прогресом у центрах операцій безпеки на базі штучного інтелекту, що дозволяє створювати можливості, що трансформують роботу команд безпеки.

Сортування та визначення пріоритетів за тривогою 1-го рівня

Ансамблеві моделі чудово виконують функцію первинного сортування сповіщень, яка традиційно споживає величезні ресурси аналітиків. Поєднуючи класифікацію на основі правил, статистичну оцінку ризиків та контекстний аналіз на основі LLM, ансамблі можуть точно категоризувати та визначати пріоритети сповіщень з мінімальним втручанням людини.

Таке автоматизоване сортування не просто зменшує обсяг, а й покращує якість, застосовуючи послідовні, багатовимірні критерії оцінки до кожного сповіщення. Служби безпеки отримують пріоритетні черги, де виявлення з високою достовірністю піднімаються на перший план, тоді як сповіщення з низьким пріоритетом та ймовірно хибнопозитивними результатами автоматично блокуються або перенаправляються до робочих процесів з нижчим пріоритетом.

Розширені розслідування 2-го та 3-го рівнів

Окрім базового сортування, ансамблеві моделі підтримують складніші

робочі процеси розслідування, які раніше вимагали досвіду старших аналітиків. Штучний інтелект революціонізує операції центрів захисту даних 2-го та 3-го рівнів, надаючи аналітикам багатоперспективні оцінки загроз, які поєднують кількісні показники ризику, контекстуальні пояснення та чітке вказівку на те, яка логіка виявлення спричинила тривогу.

Коли аналітики розслідують складні інциденти, ансамблеві моделі можуть пропонувати шляхи розслідування на основі схожих історичних випадків, виділяти відповідні дані про загрози та навіть складати попередні звіти про інциденти, які аналітики уточнюють, а не створюють з нуля. Таке доповнення дозволяє меншим командам безпеки обробляти навантаження інцидентами, що в іншому випадку вимагало б набагато більшого персоналу.

Безперервне навчання та адаптація

Ансамблеві архітектури сприяють постійному вдосконаленню завдяки численним механізмам навчання. Компоненти на основі правил оновлюються в міру появи нових даних про загрози. Статистичні моделі перенавчаються на основі останніх даних, щоб адаптуватися до базових рівнів, що змінюються. LLM точно налаштовуються на мову безпеки, специфічну для організації, та контекст.

Таке мультимодальне навчання означає, що ансамблеві моделі не стають застарілими та не потребують повного перенавчання, коли змінюється ландшафт загроз. Різні компоненти адаптуються з різною швидкістю, забезпечуючи стабільність, водночас враховуючи нові знання.

3.2 Розробка структурної схеми

Збір відповідних даних

Основою будь-якої ефективної системи виявлення загроз є високоякісні та релевантні дані. У кібербезпеці це часто передбачає збір структурованих журналів мережевого трафіку, поведінки користувачів або системної активності. Набори даних, такі як NSL-KDD, CICIDS2017 та UNSW-NB15, широко

використовуються та містять позначені записи, які розрізняють звичайну та шкідливу діяльність. Ці набори даних зазвичай включають такі характеристики, як IP-адреси, типи протоколів, тривалість з'єднання та статистика пакетів.

Наведено простий знімок мережевої активності, який можна використовувати для навчання моделі машинного навчання виявляти загрози безпеці. Кожен рядок представляє з'єднання між двома пристроями з такими деталями, як IP-адреси джерела та призначення, тип використовуваного протоколу (наприклад, TCP або UDP), тривалість з'єднання та кількість надісланих пакетів. Останній стовпець показує, чи була активність нормальною чи підозрілою. Наприклад, надзвичайно короткі з'єднання, які містять дуже мало пакетів, – такі як ті, що позначені як «Вторгнення», – можуть бути ознаками потенційної атаки. Тим часом довший та інтенсивніший трафік, такий як UDP-з'єднання тривалістю понад 300 секунд, позначається як нормальний. Навчаючись на таких позначених даних, модель може почати розпізнавати тонкі відмінності між повсякденною поведінкою мережі та чимось, що може бути небезпечним.

Розділення зразків трафіку та тесту

Для оцінки узагальнюваності моделі набір даних розділяється на навчальні та тестові підмножини. Зазвичай 80% даних використовується для навчання, а 20% резервується для тестування. Це гарантує, що моделі навчаються на значній частині даних, а потім оцінюються на невидимих прикладах.

Модельне навчання

На цьому етапі кілька моделей машинного навчання навчаються окремо на навчальних даних. Для цього дослідження використовуються три типи класифікаторів: Random Forest [17], SVM [18] та DNN [19]. Кожна модель навчається розпізнавати закономірності та поведінку, які зазвичай пов'язані з нормальною або шкідливою мережевою активністю. Використовуючи різні алгоритми, кожна модель пропонує унікальний спосіб розуміння даних, що додає різноманітності та потужності загальній системі.

Огляд підходу до ансамбевого навчання, розробленого для виявлення загроз у мережевому трафіку

Він починається з набору даних, який включає такі ознаки, як IP-адреси джерела та призначення, тип протоколу, тривалість та кількість пакетів, усі з яких позначені як «Нормальні» або «Вторгнення». Перед передачею даних класифікаторам виконується кілька етапів попередньої обробки, такі як одноразове кодування для категоріальних змінних, перетворення IP-адрес та масштабування значень тривалості та кількості для забезпечення однорідності. Потім уточнені дані одночасно передаються трьом різним класифікаторам: випадковому лісу, SVM та глибокій нейронній мережі (DNN). Кожен класифікатор незалежно навчається розрізняти нормальні шаблони від потенційних вторгнень, використовуючи свою унікальну методологію. Наприклад, випадковий ліс будує дерева рішень, SVM розділяє точки даних за допомогою гіперплощини, а DNN обробляє кілька нелінійних перетворень через приховані шари.

Після навчання цих моделей кожна з них робить власні прогнози на основі нових та раніше невідомих даних. Ці індивідуальні рішення потім агрегуються за допомогою механізму ансамблю голосування – по суті, системи «правил більшості» – де кінцевий результат базується на найпоширенішому прогнозі серед трьох класифікаторів. Цей спільний процес прийняття рішень підвищує надійність та стійкість системи виявлення загроз, балансуючи сильні та слабкі сторони кожного алгоритму [20-22]. Кінцевий результат чітко вказує на те, чи є спостережувана мережева активність нормальною, чи свідчить про вторгнення. Такий інтегрований підхід підвищує точність та узагальнюваність, роблячи систему ефективнішою у виявленні складних моделей атак у різних сценаріях даних.

Тестування моделей та виявлення загроз

Після навчання моделей їх тестують за допомогою тестового набору даних. Кожна модель робить власний прогноз щодо того, чи є певний запис даних нормальним, чи це вторгнення. Ці окремі прогнози потім об'єднуються за

допомогою ансамбльового методу – зазвичай за принципом голосування більшістю – для прийняття остаточного рішення [23-28]. Наприклад, якщо дві з трьох моделей стверджують, що з'єднання підозріле, система класифікує його як загрозу. Такий підхід допомагає зменшити кількість помилок, збалансувавши сильні сторони різних моделей, і призводить до більш точного та надійного виявлення потенційних загроз кібербезпеці.

Цей розділ починається з аналізу набору даних, що використовується для навчання та оцінки моделей виявлення загроз на основі ансамблю. Набір даних містить поєднання змодельованого нормального трафіку та трафіку вторгнень, що характеризується такими ознаками, як тривалість, кількість пакетів та тип протоколу. Ці атрибути фіксують поведінку мережевих потоків, дозволяючи моделям машинного навчання розрізняти доброякісну та шкідливу активність. Використовуючи статистичні візуалізації, такі як коробкові діаграми, можна чітко визначити відмінності між нормальним трафіком та трафіком вторгнень, особливо з точки зору тривалості з'єднання та обсягу пакетів. Це фундаментальне розуміння створює передумови для глибшої оцінки продуктивності моделі, де кілька класифікаторів тестуються окремо та в поєднанні для оцінки точності, надійності та узагальнення у виявленні загроз.

На графіку тривалості нормальний трафік відображає ширший діапазон та вищі середні значення, що вказує на те, що легітимні мережеві сеанси, як правило, тривають довше. І навпаки, спроби вторгнення зазвичай мають коротшу тривалість, що відображає швидку, часто автоматизовану поведінку атаки, таку як сканування портів або спроби грубої сили. Аналогічно, коробкова діаграма кількості пакетів показує, що нормальний трафік зазвичай включає передачу більшої кількості пакетів, тоді як трафік вторгнення характеризується меншою кількістю пакетів – що підтверджує припущення, що шкідлива діяльність часто передбачає мінімальний зв'язок, щоб уникнути виявлення. Ці візуальні шаблони підтверджують ідею про те, що ці дві характеристики є дуже дискримінативними, що робить їх цінними для навчання моделей машинного навчання розрізняти безпечну та підозрілу мережеву діяльність.

Результати оцінювання підкреслюють як сильні сторони, так і обмеження ансамблевого навчання порівняно з існуючими підходами. Логістична регресія досягла найвищої загальної точності (96,67%) та F1-балу (96,63%), показуючи, що окремі класифікатори іноді можуть перевершувати ансамблеві методи за точністю прогнозування. Ця висока продуктивність частково зумовлена відносно структурованою природою еталонних наборів даних, де логістична регресія може ефективно фіксувати лінійну роздільність. Однак така висока точність може не повністю узагальнюватися на більш складні або динамічні моделі трафіку. Випадковий ліс та градієнтне підвищення також показали конкурентні результати (обидва з точністю ~94,67%), виграючи від їхньої здатності моделювати нелінійні взаємодії ознак та обробляти шумні дані. Їхня продуктивність підкреслює цінність деревоподібних підходів у завданнях виявлення вторгнень, де гетерогенність ознак є високою. Тим не менш, обидві моделі демонстрували мінливість між складками, що свідчить про певну чутливість до розподілу даних.

На противагу цьому, метод ансамблю пропонує важливі досягнення, що базуються на існуючій роботі та розширюють її. Поєднуючи три гетерогенні класифікатори (SVM, Random Forest та DNN), ансамбль досягає найбільш збалансованого компромісу між точністю (95,10%) та повнотою (94,00%). Цей баланс особливо цінний у кібербезпеці, оскільки мінімізує хибні тривоги (точність), водночас гарантуючи виявлення більшості справжніх атак (повнотою). Вищий показник AUC (0,77) додатково демонструє здатність ансамблю відрізняти малопомітні типи атак від звичайного трафіку, навіть коли окремі класифікатори мають труднощі. Ця стійкість виникає завдяки взаємодоповнюючим сильним сторонам моделей: SVM сприяє ефективному виявленню меж для структурованих ознак, Random Forest забезпечує стабільність при обробці змішаних даних, а DNN фіксує складні нелінійні закономірності. У сукупності ці результати свідчать про те, що хоча окремі класифікатори, такі як логістична регресія, можуть досягати успіху в контрольованих умовах, ансамбль забезпечує сильніше узагальнення та

надійність у різних сценаріях. Цей глибший аналіз підкреслює практичний компроміс між моделями, орієнтованими на точність, та збалансованими, надійними стратегіями виявлення – важливий фактор для реального впровадження, де зменшення кількості хибнопозитивних результатів є таким же критичним, як і досягнення високої точності.

У цьому дослідженні розглянуто використання ансамбльового навчання для покращення виявлення загроз в системах інформаційної безпеки. Інтегруючи SVM, випадкові ліси та DNN у гетерогенний ансамбль, ми продемонстрували, що цей підхід досягає збалансованої продуктивності за кількома показниками. Зокрема, ансамбль забезпечив високу точність (95,10%) та повноту (94,00%), а також найвищий показник AUC (0,77) серед усіх оцінених моделей, що свідчить про чудову здатність розрізняти доброякісний та шкідливий трафік. Хоча логістична регресія перевершила ансамбль за чистою точністю, ансамбль запропонував більшу стійкість та узагальнюваність при тестуванні на трьох еталонних наборах даних (NSL-KDD, CICIDS2017 та UNSW-NB15).

Практичні наслідки: Ці результати свідчать про те, що ансамблеві моделі можуть слугувати надійнішими та адаптивнішими рішеннями для виявлення вторгнень у реальних умовах, де мінімізація хибних спрацьовувань та забезпечення стабільної роботи в різних середовищах є критично важливими. Організації, які впроваджують такі системи, можуть зміцнити свою інфраструктуру безпеки, зменшивши кількість пропущених атак, уникаючи при цьому експлуатаційних витрат, пов'язаних з надмірною кількістю хибних тривог.

Обмеження: Незважаючи на свої переваги, запропонований підхід має обмеження. Обчислювальна складність навчання та поєднання кількох класифікаторів може створювати проблеми у високошвидкісних мережевих середовищах. Крім того, використані набори даних, хоча й широко визнані, можуть не повністю відображати еволюціонуючу природу сучасних кібератак, таких як передові стійкі загрози або експлойти нульового дня.

Майбутні дослідження: Майбутня робота повинна бути зосереджена на оптимізації ефективності гетерогенних ансамблів для розгортання в системах

виявлення вторгнень у реальному часі. Включення методів штучного інтелекту (ШІ; XAI) з можливістю пояснення також може покращити прозорість прогнозів, підтримуючи довіру та прийняття рішень аналітиками безпеки. Крім того, розширення оцінювання на більш різноманітні та актуальні набори даних, а також застосування цієї структури до спеціалізованих середовищ, таких як Інтернет речей (IoT) та хмарні обчислення, додатково підтвердить її узагальнюваність та практичну корисність. Спираючись на пропозицію рецензента, майбутні дослідження також повинні досліджувати методи навчання без учителя та самостійного навчання, щоб зменшити залежність від маркованих наборів даних, створення яких часто є дорогим та трудомістким. Крім того, архітектури на основі трансформаторів пропонують значний потенціал для моделювання послідовних та контекстних залежностей у мережевому трафіку та повинні бути досліджені як частина систем виявлення вторгнень наступного покоління.

Це дослідження робить внесок у зростаючий обсяг знань про машинне навчання в кібербезпеці, демонструючи, як гетерогенна ансамблева структура може збалансувати точність виявлення, стійкість та узагальнюваність, пропонуючи надійний інструмент для сучасного виявлення загроз.

Структурна схема системи представлена на рис. 3.1.

Для забезпечення ефективного та стабільного функціонування комплексної системи нейромережевих експертів, призначеної для задач безпечної маршрутизації, першочерговим і критично важливим етапом є ретельна підготовка та глибока систематизація масивів даних, які слугуватимуть основою для навчання окремих нейронних компонентів.

Цю функцію виконує спеціалізований блок формування навчальної та тестової вибірки, завданням якого є підготовка, структуризація та впорядкування інформації таким чином, щоб зробити її повністю придатною для подальшої обробки сучасними нейромережевими технологіями.

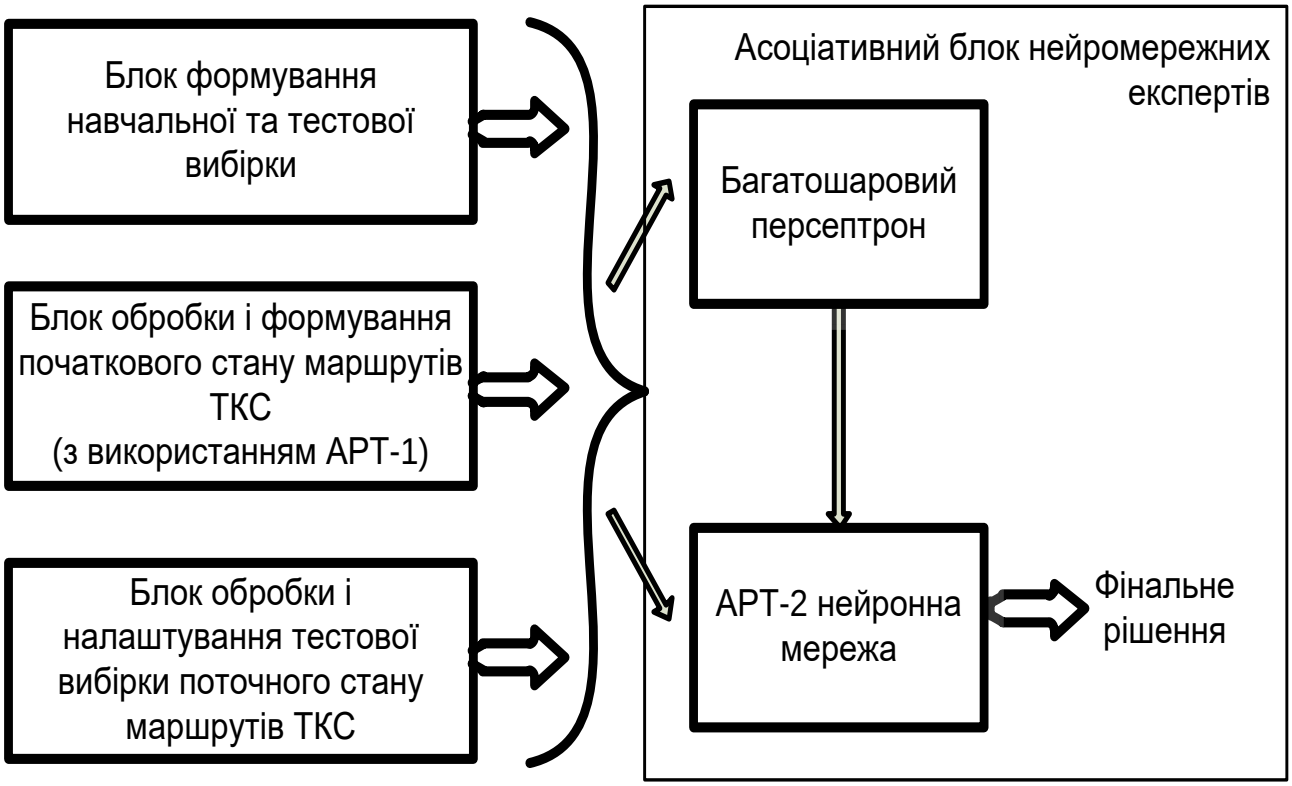


Рисунок 3.1 – Структурна схема системи

Цей етап алгоритму має ключове значення, оскільки саме він закладає фундамент для формування здатності сукупності нейронних мереж до ефективного узагальнення знань. Джерела вхідних даних, необхідних для роботи цього блока, а також методологія їх отримання для побудови навчальних і тестових множин асоціативної машини реалізуються відповідно до сформульованих раніше концептуальних принципів.

Не менш важливу роль відіграє блок обробки й формування початкового стану маршрутів телекомунікаційних систем (ТКС), який відповідає за визначення та встановлення початкових значень параметрів усієї архітектури ще до запуску процедури навчання. Логіка цього процесу полягає в тому, що якщо попередньо ініціалізувати змінні параметри системи значеннями, максимально близькими до оптимальних, то безпосередній процес навчання перетвориться з масштабного пошуку на процедуру тонкого «підстроювання» та оптимізації моделі. Відповідно, синтез оптимального алгоритму первинної ініціалізації

дозволяє суттєво скоротити часові витрати на навчання нейромережевих експертів.

Згідно з результатами аналізу фахової літератури [4, 8], для успішного розв'язання цієї задачі доцільно спиратися на напрацювання, наведені у джерелі [2]. Зокрема, як базовий алгоритм початкової установки параметрів там запропоновано використовувати кооперативний імунний алгоритм, який доповнено процедурою генетичного пошуку на базі нейронної мережі АРТ-1 (Adaptive Resonance Theory).

Зважаючи на те, що нейронні мережі типу АРТ належать до класу архітектур, що гармонійно поєднують у собі такі фундаментальні властивості, як пластичність і стабільність, до загальної структурної схеми блоку нейромережевих експертів раціонально інтегрувати додатковий блок обробки й налаштування тестової вибірки поточного стану маршрутів ТКС. Його призначення полягає в адаптації компонентів нейронної мережі безпосередньо під специфіку розв'язуваної проблеми. У межах виконання дипломної роботи процедура навчання для кожної з нейронних мереж реалізовувалася на основі алгоритмів, адаптованих до особливостей їхньої внутрішньої архітектури.

3.3 Розробка функціональної схеми

Розроблений у межах дипломного проєкту хмарний антивірус призначений для комплексного захисту комп'ютерних систем від шкідливого програмного забезпечення та кіберзагроз. Комплекс поєднує локальні механізми безпеки з хмарними обчисленнями та технологіями інтелектуального аналізу, що забезпечує високу ефективність виявлення аномалій при мінімальному навантаженні на апаратні ресурси ПК.

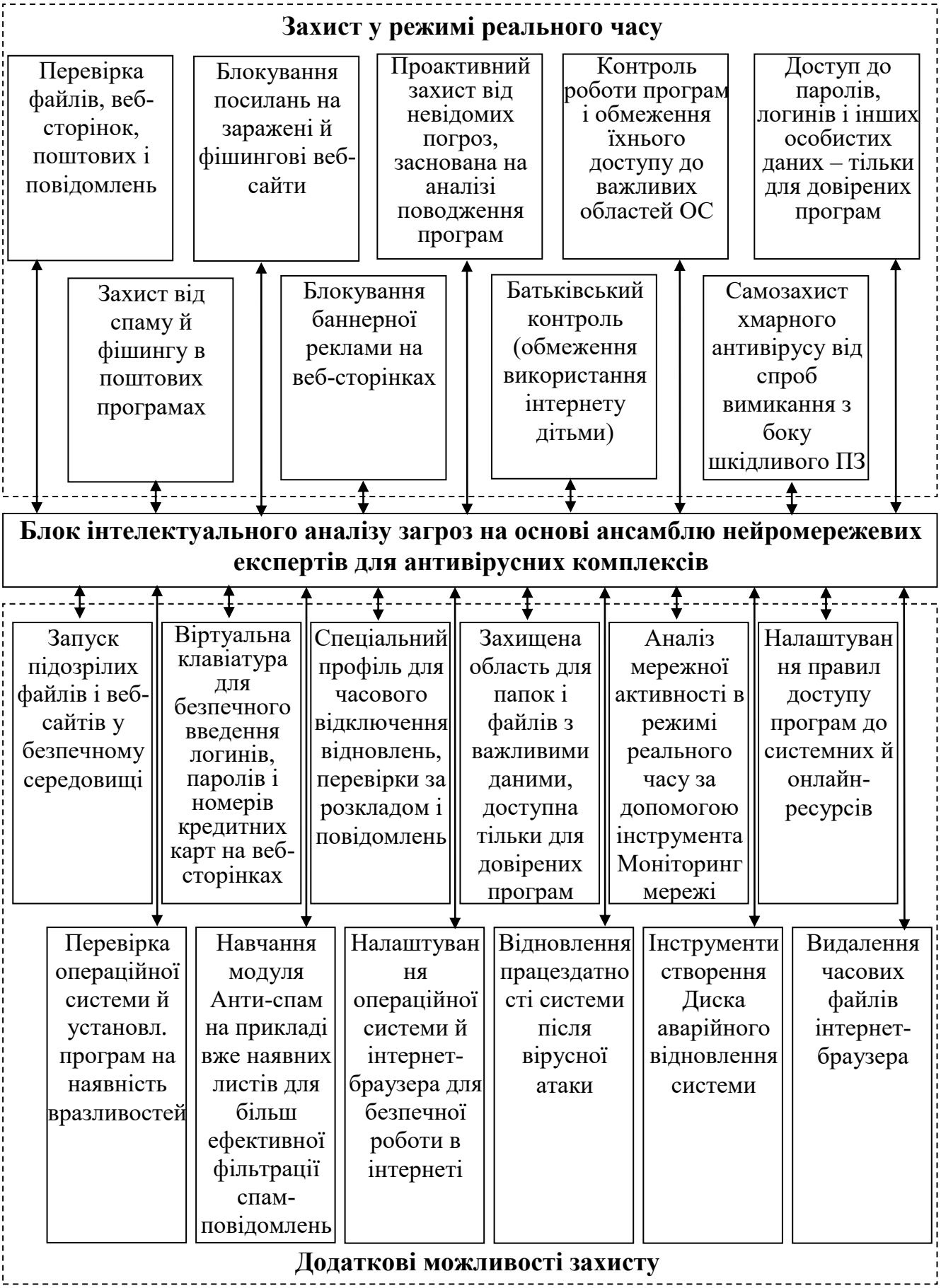


Рисунок 3.2 – Функціональна схема системи

Функціональна структура розробленого хмарного рішення охоплює такі основні можливості:

– Захист у реальному часі та проактивне виявлення: моніторинг операцій у реальному часі, поведінковий аналіз (проактивний захист нового покоління) для виявлення невідомих загроз і нульового дня (Zero-Day), а також системи миттєвого реагування для блокування шкідливих кодів.

– Мережева безпека та вебфільтрація: базовий захист при роботі в мережі Інтернет і з електронною поштою, перевірка вебсторінок, поштових і месенджер-повідомлень, а також спеціалізовані модулі блокування фішингових і заражених сайтів.

– Інформаційна безпека користувача: віртуальна клавіатура для захищеного введення конфіденційних даних (паролів, логінів, реквізитів платіжних карток).

– Системний аудит та відновлення: сканування операційної системи й встановленого ПЗ на наявність вразливостей, налаштування параметрів ОС і браузерів для безпечної роботи, очищення тимчасових файлів та відновлення працездатності системи після вірусних атак.

– Механізми самозахисту: вбудовані алгоритми попередження несанкціонованого вимикання або модифікації антивірусних компонентів з боку шкідливого ПЗ.

Для досягнення максимального рівня безпеки архітектура передбачає сумісність із міжмережевими екранами (файрволами) та характеризується інтуїтивно зрозумілим інтерфейсом.

На рисунку 3.2 зображена функціональна схема системи. Після детального розгляду всіх блоків функціональної схеми перейдемо до аналізу діаграми взаємодії процесів, які відбуваються у розробленому антивірусному комплексі.

3.4 Розробка діаграми процесів

Діаграма взаємодії процесів розробленої системи наведена на рисунку 3.3. Логіка інформаційного обміну та виконання функціональних завдань у межах хмарного антивірусного комплексу реалізує послідовність взаємопов'язаних процедур:

1. Ініціалізація та виведення системних ресурсів: базовий процес, який виконується першочергово при запуск програмного забезпечення та відображає поточний стан апаратних і хмарних ресурсів.

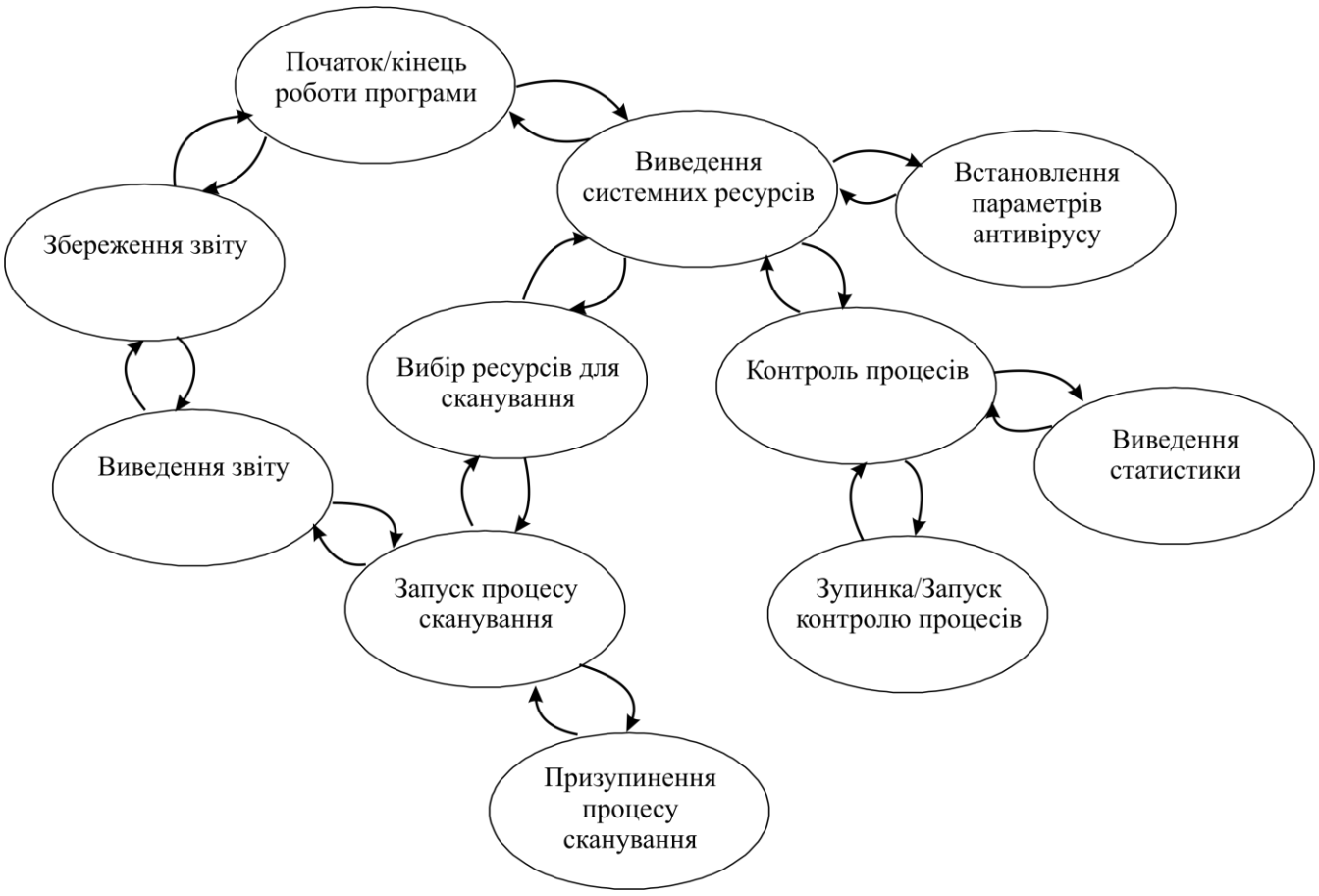


Рисунок 3.3 – Діаграма взаємодії процесів

2. Параметризація та моніторинг: після ініціалізації користувач може переходити до виконання трьох паралельних гілок процесів:

– встановлення параметрів хмарного антивірусу;

– контроль процесів;

– вибір ресурсів для сканування.

3. Керування процесами: підсистема контролю процесів безпосередньо взаємодіє з процедурами виведення статистики та керування станом моніторингу (зупинка або запуск контролю).

4. Процедура сканування: після вибору цільових ресурсів ініціюється процес запуску сканування, який тісно інтегрований із додатковими функціональними операціями:

– призупинення сканування;

– виведення звіту за результатами перевірки;

– збереження звіту в локальних або хмарних сховищах даних.

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

Функціонування системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів ґрунтується на багатокритеріальному дослідженні характеристик програмних об'єктів і виявленні ознак потенційно шкідливої поведінки. Основним призначенням алгоритмічного забезпечення є підвищення обґрунтованості рішень про небезпечність файлів шляхом поєднання результатів декількох спеціалізованих моделей машинного навчання. На відміну від класифікації за одним набором ознак, ансамблевий підхід дозволяє враховувати різні представлення програмного об'єкта, зокрема його двійкову структуру, характеристики виконуваного файлу та події, отримані під час контрольованого аналізу поведінки. Основну блок-схему функціонування програмного комплексу представлено на рисунку 4.1.

У межах запропонованого рішення аналіз загроз розглядається як послідовність взаємопов'язаних операцій. Спочатку система отримує програмний об'єкт або повідомлення про нього від антивірусного компонента. Далі визначаються тип файлу, допустимість його оброблення та наявність раніше отриманих результатів. Після первинної перевірки формується набір статичних характеристик. За необхідності до нього додаються відомості про поведінку об'єкта, отримані з ізольованого середовища або довіреного джерела телеметрії. Підготовлені дані передаються спеціалізованим нейромережевим експертам, результати яких об'єднуються для формування оцінки загрози.

Архітектура ансамблю передбачає використання декількох експертних моделей із різними інформаційними входами.

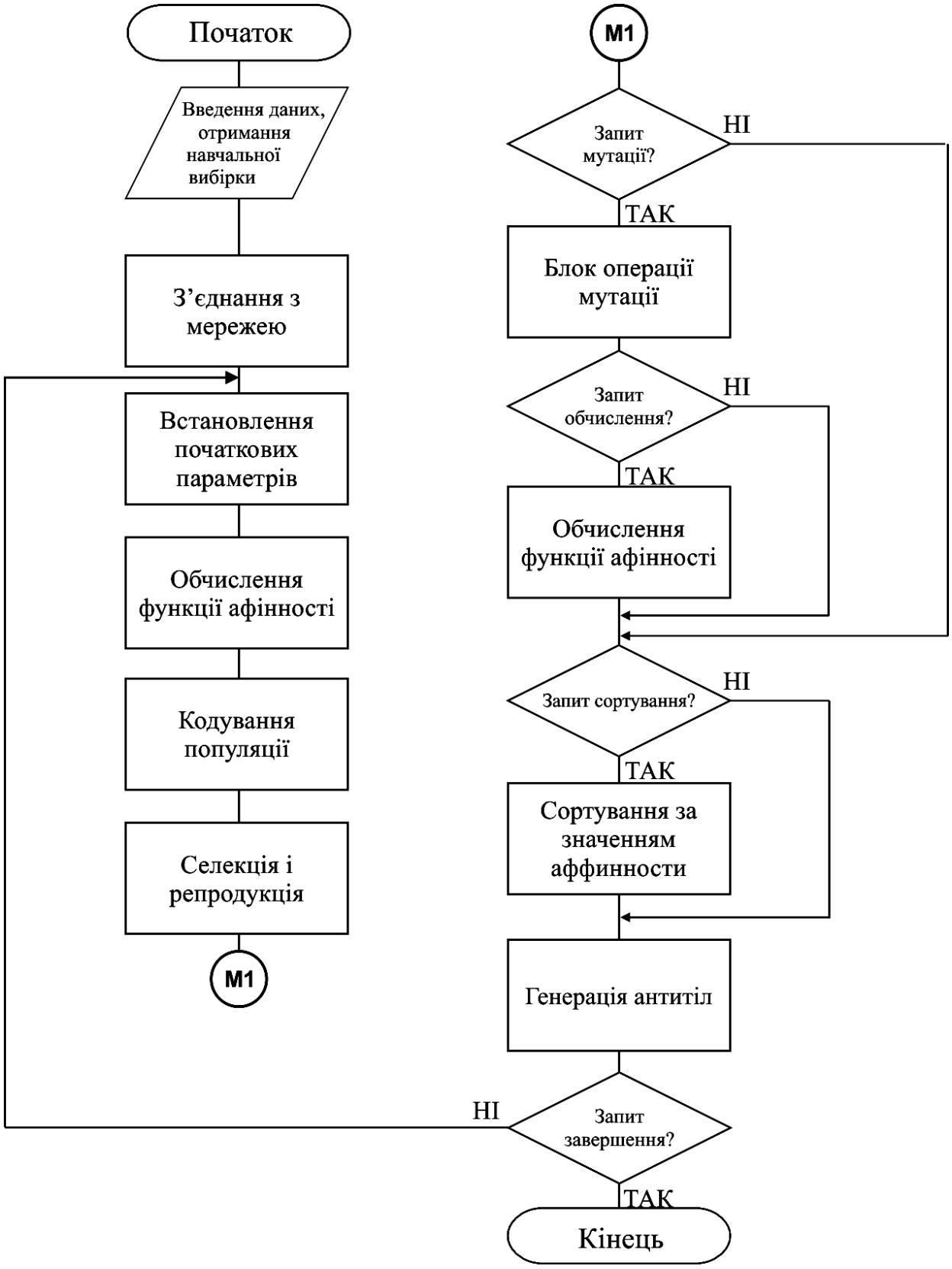


Рисунок 4.1 – Блок-схема основної програми

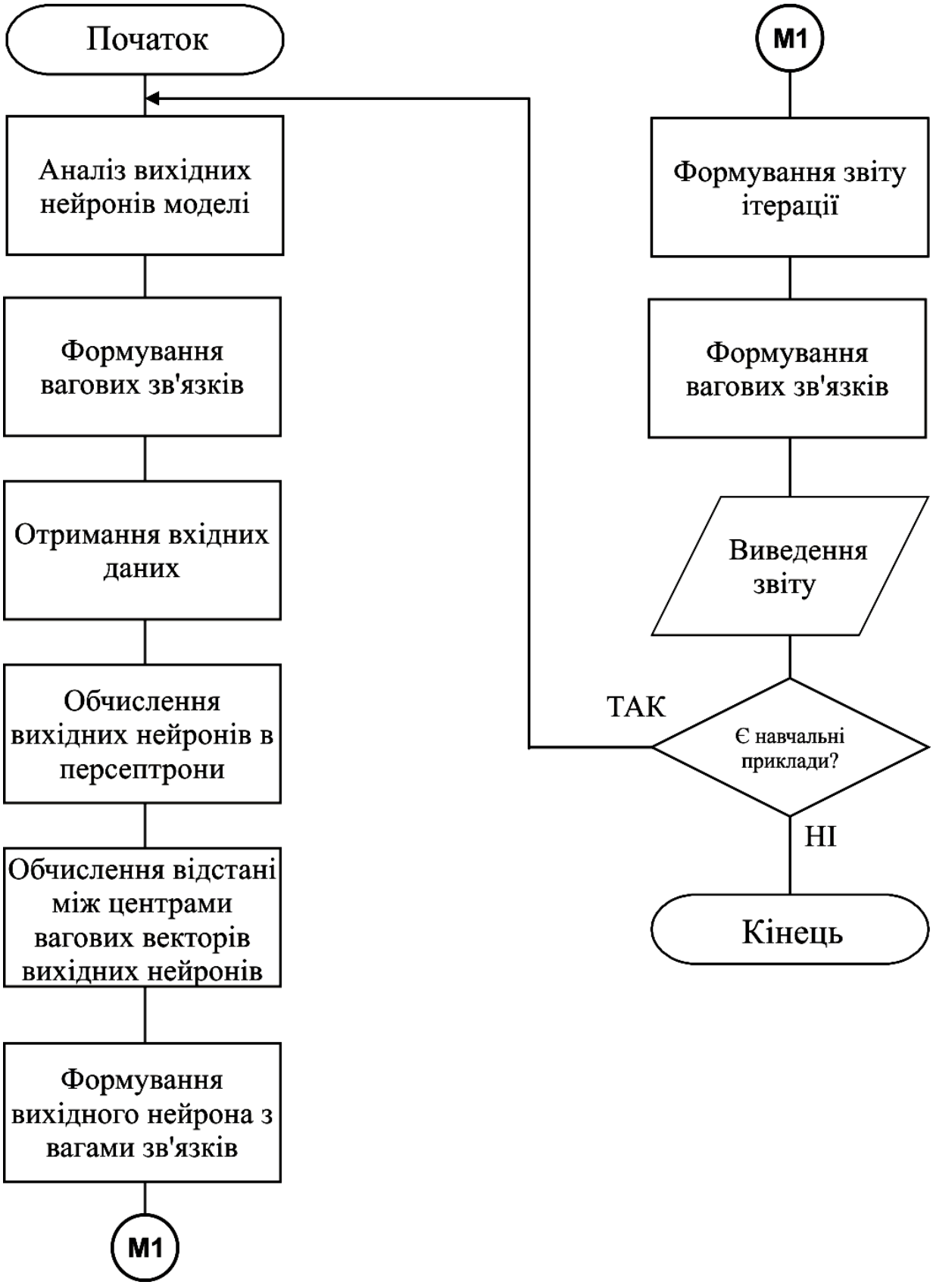


Рисунок 4.2 – Структурна схема підпрограми

Перший експерт аналізує послідовності байтів виконуваного файлу та виявляє характерні двійкові закономірності.

Другий досліджує структурні характеристики програмного об'єкта, зокрема параметри секцій, імпортованих функцій і метаданих. Третій експерт орієнтований на аналіз послідовностей поведінкових подій. Кожен компонент формує власну оцінку небезпечності. Окремий модуль інтеграції визначає відносну значущість доступних експертних висновків і формує підсумковий результат.

Важливою особливістю системи є підтримка неповних наборів ознак. Статичний аналіз можна виконувати без запуску досліджуваної програми. Поведінкові характеристики, навпаки, доступні лише за наявності відповідної телеметрії. Якщо динамічний аналіз не проводився, його результати не можна замінювати нульовими значеннями та трактувати як відсутність шкідливої поведінки. Для цього алгоритм об'єднання експертних оцінок повинен враховувати доступність кожного інформаційного каналу.

Центральним елементом системи є механізм адаптивного об'єднання результатів експертів. Він отримує числові оцінки моделей, перевіряє їхню коректність і визначає ваги відповідно до інформаційного контексту. При цьому необхідно враховувати якість вхідних даних, наявність поведінкової інформації та ступінь розбіжності експертних висновків. Якщо результати моделей суперечливі або недостатньо достовірні, система може ініціювати поглиблений аналіз замість негайної класифікації об'єкта. Послідовність функціонування відповідної підпрограми інтеграції нейромережевих оцінок відображено на рисунку 4.2.

Підсумкове рішення повинно враховувати не лише оцінку нейронної мережі, а й політику антивірусного комплексу. Високе значення оцінки загрози може бути підставою для додаткової перевірки, створення сповіщення або застосування обмежувальної дії. Проте автоматичне блокування легітимного програмного забезпечення здатне порушити роботу корпоративних систем. Тому необхідно розмежувати обчислення рівня ризику, прийняття рішення та фактичне

виконання захисної операції. Для останньої повинні застосовуватися окремі правила безпеки й авторизації.

Програмну реалізацію аналітичного ядра доцільно виконати мовою Python із використанням PyTorch для побудови та навчання нейромережевих моделей. Для оброблення числових даних може застосовуватися NumPy, для дослідження структури виконуваних файлів бібліотека LIEF або pefile, а для зберігання результатів реляційна база даних. Інтеграція з антивірусним комплексом може здійснюватися через локальний програмний інтерфейс або захищену серверну службу. Зазначена конфігурація характеризує технічно можливе проєктне рішення. Конкретний склад реалізованого програмного забезпечення та характеристики навчених моделей мають визначатися відповідно до фактичних матеріалів розробки.

Формування багатоканального конвеєра аналізу програмних об'єктів

Приймання програмного об'єкта є початковою операцією аналітичного конвеєра. Вхідними даними можуть бути файл із локальної файлової системи, об'єкт із карантинного сховища або структурований запит від антивірусного агента. Для кожного запиту формується унікальний ідентифікатор оброблення. Додатково фіксуються час надходження, походження об'єкта, його розмір та допустимі режими перевірки. Отримані відомості використовуються для маршрутизації завдання й контролю виконання.

На першому етапі необхідно перевірити відповідність об'єкта політиці аналізу. Система повинна обмежувати максимальний розмір файлу та відхиляти некоректні запити. Необхідно також контролювати кількість одночасно оброблюваних об'єктів. Для файлів невідомого формату допускається виконання базових перевірок, але спеціалізовані алгоритми розбору PE-структури не повинні застосовуватися до довільних двійкових даних як до коректних виконуваних файлів.

Після початкової перевірки обчислюється криптографічний ідентифікатор вмісту. Для цього доцільно використовувати SHA-256. Отримане значення дозволяє зіставляти однакові файли незалежно від їхньої назви або місця

розташування. Хеш може використовуватися як ключ пошуку попередніх результатів, проте не характеризує небезпечність об'єкта сам по собі. Відсутність ідентифікатора в базі відомих загроз не є доказом безпечності.

Алгоритм перевірки кешу повинен враховувати версію нейромережевої моделі, конфігурацію ознак і актуальність антивірусної політики. Результат аналізу, отриманий за допомогою попередньої версії ансамблю, не завжди придатний для безпосереднього повторного використання. Особливо це стосується випадків оновлення набору класів або параметрів калібрування. Тому ключ кешування доцільно формувати із хешу файлу та ідентифікатора версії аналітичного конвеєра.

Для початкової реалізації можна обмежити предметну область виконуваними файлами Windows у форматі Portable Executable. Цей формат визначає структуру заголовків, секцій, таблиць імпорту й інших елементів виконуваних файлів. Його специфікація може використовуватися під час побудови механізму структурного аналізу. Для документів, сценаріїв, архівів і файлів інших форматів потрібні окремі адаптери та набори експертних моделей.

У системі доцільно використовувати окремі стани оброблення. Після приймання завдання переходить до стану RECEIVED. Успішна перевірка формату переводить його до VALIDATED. Під час формування ознак використовується EXTRACTING, а на етапі нейромережевого аналізу INFERENCE. Після завершення об'єднання експертних оцінок формується ASSESSED. Якщо потрібна додаткова перевірка, використовується REVIEW_REQUIRED. Помилки оброблення реєструються окремо та не повинні автоматично позначатися як безпечний результат.

Особливе значення має безпечне поводження з підозрілими об'єктами. Статичний аналіз не повинен передбачати їхнього виконання. Файли необхідно обробляти в ізольованому середовищі з мінімальними правами доступу, обмеженнями використання ресурсів і контролем файлових операцій.

Якщо об'єкт передається на динамічний аналіз, для нього повинно використовуватися спеціалізоване ізольоване середовище, а не робочий сервер аналітичної системи.

Виділення двійкових ознак та структурних характеристик PE-файлів

Для роботи першого нейромережевого експерта необхідно сформувати числове представлення двійкового вмісту програми. Найпростішим способом є перетворення байтів на цілі числа в діапазоні від 0 до 255.

Отримана послідовність може використовуватися як вхід для нейромережі з шаром вкладень і згортковими операціями. Така модель здатна вивчати локальні закономірності двійкового представлення без ручного визначення кожної ознаки.

Обсяг виконуваних файлів може суттєво відрізнятися. Тому для нейромережевого аналізу необхідно визначити максимальну довжину вхідної послідовності. Просте використання лише початку файлу може призводити до втрати інформації з його інших частин.

Одним із можливих рішень є вибір декількох фрагментів, рівномірно розподілених за вмістом. Іншим варіантом є оброблення послідовності блоками з подальшим агрегуванням їхніх ознак. Вибір способу повинен відповідати архітектурі експерта й бути однаковим під час навчання та експлуатації. Окремий канал структурного аналізу призначений для виділення інформації, пов'язаної з організацією PE-файлу. До можливих ознак належать кількість секцій, їхні розміри, права доступу, характеристики імпорту, наявність окремих службових таблиць і статистичні показники вмісту. Такі дані можна перетворити на вектор фіксованої розмірності. Для ознак із великою кількістю категоріальних значень необхідно передбачити кодування або хешування в заданий ознаковий простір.

Одним із допоміжних показників є інформаційна ентропія байтового розподілу. Високе значення може бути характерним для стиснених або зашифрованих даних, але не є самостійним доказом шкідливості. Тому ентропію доцільно використовувати разом з іншими характеристиками.

Для початкового формування ознак можна реалізувати окремий модуль Python, який читає файл як двійковий об'єкт без виконання його вмісту.

Наведений приклад перевіряє основні сигнатури PE, обчислює SHA-256, формує частотний розподіл байтів та вибирає обмежену кількість фрагментів. Результат може використовуватися як вхід для подальшого формування ознак нейромережевого експерта.

```
from dataclasses import dataclass
from hashlib import sha256
from pathlib import Path
from math import log2
import struct
import numpy as np

@dataclass(frozen=True)
class BinaryFeatures:
    sha256_hash: str
    file_size: int
    entropy: float
    byte_histogram: np.ndarray
    sampled_bytes: np.ndarray

def extract_binary_features(
    file_path,
    max_size=64 * 1024 * 1024,
    sample_size=8192
):
    path = Path(file_path)
    # Обмеження розміру вхідного об'єкта
    if not path.is_file():
        raise FileNotFoundError(path)
    size = path.stat().st_size
    if size < 64 or size > max_size:
        raise ValueError("Недопустимий розмір файлу")
    if sample_size < 1:
        raise ValueError("Некоректний розмір вибірки")

    # Читання без виконання досліджуваного файлу
    data = path.read_bytes()

    # Перевірка початкових ознак PE-формату
    if data[:2] != b"MZ":
        raise ValueError("Відсутній заголовок MZ")
    pe_offset = struct.unpack_from("<I", data, 0x3C)[0]
    if pe_offset > len(data) - 4:
        raise ValueError("Некоректний PE-зсув")
    if data[pe_offset:pe_offset + 4] != b"PE\x00\x00":
        raise ValueError("Відсутня сигнатура PE")
    # Обчислення криптографічного хешу
    digest = sha256(data).hexdigest()
    # Нормалізований гістограмний опис
    values = np.frombuffer(data, dtype=np.uint8)
    counts = np.bincount(values, minlength=256)
    probabilities = counts / len(values)
    positive = probabilities[probabilities > 0]
    entropy = float(
        -np.sum(positive * np.log2(positive))
    )
    # Рівномірна вибірка байтів по всьому файлу
    positions = np.linspace(
        0, len(values) - 1,
        min(sample_size, len(values)),
```

```
        dtype=np.int64
    )
    sampled = values[positions].copy()
    return BinaryFeatures(
        sha256_hash=digest,
        file_size=len(values),
        entropy=entropy,
        byte_histogram=probabilities.astype(np.float32),
        sampled_bytes=sampled
    )
```

Наведений модуль формує базові статичні ознаки та перевіряє головні сигнатури PE-файлу. Він не замінює повноцінного розбору всіх структур виконуваного формату. Рівномірна вибірка байтів також не зберігає повну локальну послідовність, тому не повинна безпосередньо підставлятися до згорткової моделі, навченої на суміжних фрагментах. Для такої моделі необхідно реалізувати вибір суцільних блоків і узгодити відповідний спосіб із процедурою навчання.

Під час виділення структурних характеристик доцільно застосовувати бібліотеки, які підтримують перевірку меж секцій і коректність таблиць PE. У разі виявлення некоректного заголовка або пошкоджених структур система повинна повертати статус частково успішного аналізу. Сам факт помилки розбору може використовуватися як діагностична ознака, але не повинен автоматично трактуватися як підтвердження шкідливості.

Досвід відкритих дослідницьких наборів, зокрема EMBER, підтверджує доцільність використання наборів статичних PE-ознак для побудови класифікаторів. EMBER містить підготовлені характеристики виконуваних файлів і засоби відтворюваного навчання моделей. Водночас вихідний набір не містить самих виконуваних файлів. Тому він придатний для експериментів зі структурними ознаками, але не забезпечує безпосереднього навчання моделі на повних байтових послідовностях без додаткових даних.

Моделювання поведінкових ознак у контрольованому середовищі

Статичний аналіз дозволяє отримувати інформацію про програмний об'єкт без його запуску, проте не завжди відображає реальну поведінку. Частина небезпечних дій може виявлятися лише під час виконання програми. Тому в архітектурі ансамблю доцільно передбачити окремий поведінковий експерт. Його

вхідними даними є телеметричні записи, отримані під час контрольованого аналізу в ізольованому середовищі або від довіреного засобу захисту кінцевої точки.

До поведінкових характеристик можуть належати створення процесів, звернення до файлової системи, зміни параметрів операційної системи та встановлення мережевих з'єднань. Для кожного типу події визначаються часові позначки, ідентифікатор процесу, тип операції та нормалізовані характеристики її об'єкта. Такий набір відомостей узгоджується із загальними категоріями джерел даних, що використовуються для виявлення технік загроз у MITRE

Важливою умовою є ізоляція середовища динамічного аналізу. Досліджуваний файл не повинен запускатися на основному сервері антивірусної системи. Для отримання поведінкових даних необхідно використовувати спеціалізовану пісочницю з обмеженим доступом до мережі, контрольованими ресурсами та відновлюваним початковим станом. Об'єкти, які можуть містити конфіденційні дані, повинні аналізуватися відповідно до встановленої політики організації.

Алгоритм підготовки поведінкових даних починається з перевірки походження телеметрії. Повідомлення повинні бути пов'язані з конкретним об'єктом аналізу. Для цього використовується ідентифікатор завдання та криптографічний хеш файлу. Події, отримані від різних запусків або сторонніх процесів, не повинні безумовно об'єднуватися в одну послідовність. Після перевірки належності виконується нормалізація типів подій і впорядкування за часовими позначками.

Для нейромережевого аналізу подію можна представити як категоріальний токен та набір додаткових числових характеристик. Наприклад, створення процесу отримує один тип події, а встановлення мережевого з'єднання інший. За необхідності враховуються властивості відповідної операції. Для цього можуть застосовуватися векторні вкладення категоріальних значень та нормалізовані числові поля.

Для оброблення послідовностей подій доцільно використовувати рекурентну нейронну мережу з керованими вентилями GRU. Її прихований стан оновлюється під час надходження чергового елемента послідовності. Це дозволяє формувати представлення, яке залежить від порядку подій, а не лише від загальної кількості операцій. У PyTorch відповідний компонент реалізується класом torch.nn.GRU, який підтримує послідовності змінної довжини та пакетне оброблення.

Нехай поведінкова послідовність містить T подій $e_1, e_2, \dots, e_T$. Після формування векторних представлень x_t прихований стан рекурентного експерта визначається співвідношенням $h_t = \mathrm{GRU}(x_t, h_{(t-1)})$. Завершальний стан h_T може використовуватися як компактний опис спостереженої поведінки. На його основі формується експертна оцінка загрози. Для довгих послідовностей можуть застосовуватися механізми обмеження кількості подій, агрегування часових інтервалів або уваги до інформативних фрагментів.

Під час підготовки поведінкових ознак необхідно розрізняти відсутність події та відсутність даних. Якщо контрольований аналіз завершено успішно й певного типу дій не зафіксовано, це може бути допустимою ознакою. Якщо пісочниця завершила роботу з помилкою або телеметрію втрачено, такий результат не може трактуватися як нормальна поведінка. Для цих випадків вводиться ознака якості та повноти поведінкового спостереження.

Окрему проблему створює обмежений час динамічного аналізу. Деякі програмні дії можуть не проявитися протягом контрольного інтервалу. Тому поведінковий експерт оцінює лише фактично спостережені характеристики. Його негативний результат не підтверджує відсутність прихованої функціональності. Це обмеження необхідно враховувати під час об'єднання експертних оцінок.

Проєктування ансамблю нейромережевих експертів із контекстним зважуванням

Після формування окремих представлень виконується їхнє передавання експертним моделям. Кожен експерт повинен мати власний інтерфейс отримання даних і повертати числовий результат у визначеному форматі. Для двокласового

аналізу можна використовувати логіт, який після застосування сигмоїдної функції перетворюється на значення в інтервалі від нуля до одиниці. Однак інтерпретація такого значення як імовірності потребує перевірки калібрування моделі.

Ансамбль може використовувати просте усереднення експертних оцінок або складніший механізм із контекстно залежними вагами. Для досліджуваної системи доцільно розглядати другий варіант. Його перевага як проєктного підходу полягає в можливості враховувати різну інформативність експертів залежно від доступних даних. При цьому реальна користь контекстного зважування повинна підтверджуватися порівняльними експериментами, оскільки складніший механізм не гарантує кращих результатів.

Контекст керування вагами може містити тип програмного об'єкта, наявність окремих груп ознак, результат перевірки формату та характеристики якості телеметрії. Водночас недоцільно без додаткової перевірки включати до контексту змінні, які відображають лише особливості формування навчального набору. Це може призвести до ситуації, коли керуюча мережа запам'ятовує походження даних замість вивчення закономірностей загроз.

Для програмної реалізації ансамблю можна використати модульну структуру PyTorch. Наведений фрагмент демонструє принцип поєднання трьох експертів за допомогою навчуваного механізму зважування. Передбачається, що спеціалізовані модулі вже сформували вектори ознак фіксованої розмірності. Поведінковий вектор може надходити з рекурентної моделі, а статичні представлення з відповідних попередньо навчених компонентів.

```
import torch
from torch import nn

class ThreatExpertEnsemble(nn.Module):
    def __init__(
        self,
        byte_dim=128,
        structure_dim=64,
        behavior_dim=64
    ):
        super().__init__()
        dimensions = (
            byte_dim,
            structure_dim,
            behavior_dim
        )
        # Окремі класифікаційні голови експертів
```

```
        self.experts = nn.ModuleList([
            nn.Sequential(
                nn.Linear(dim, 32),
                nn.ReLU(),
                nn.Linear(32, 1)
            )
            for dim in dimensions
        ])

        # Керуюча мережа формує ваги експертів
        context_dim = sum(dimensions) + 3

        self.gate = nn.Sequential(
            nn.Linear(context_dim, 64),
            nn.ReLU(),
            nn.Linear(64, 3)
        )
    def forward(self, features, available):
        # features містить три тензори [batch, dim]
        if len(features) != 3:
            raise ValueError("Очікуються три групи ознак")

        if available.ndim != 2 or available.shape[1] != 3:
            raise ValueError("Некоректна маска доступності")

        mask = available.bool()

        if not torch.all(mask.any(dim=1)):
            raise ValueError("Немає доступних експертів")

        # Вхід відсутнього експерта занулюється
        masked_features = [
            x * mask[:, i:i + 1].to(dtype=x.dtype)
            for i, x in enumerate(features)
        ]

        logits = torch.cat([
            expert(x)
            for expert, x in zip(
                self.experts, masked_features
            )
        ], dim=1)

        # Додаємо маску до вхідного контексту
        context = torch.cat(
            masked_features +
            [mask.to(dtype=logits.dtype)],
            dim=1
        )

        gate_logits = self.gate(context)

        # Недоступні моделі не впливають на рішення
        gate_logits = gate_logits.masked_fill(
            ~mask, float("-inf")
        )
        weights = torch.softmax(gate_logits, dim=1)
        # Узгоджене об'єднання експертних логітів
        final_logit = (
            weights * logits
        ).sum(dim=1)
        return {
            "logit": final_logit,
            "score": torch.sigmoid(final_logit),
```

```
            "expert_weights": weights,
            "expert_logits": logits
        }
```

Наведений клас демонструє архітектуру об'єднання, а не готову навчену антивірусну модель. Перед експлуатацією необхідно виконати навчання класифікаційних компонентів та керуючої мережі. Особливого значення набуває правильність масок доступності під час навчання. Якщо модель завжди навчається на повних наборах ознак, а під час експлуатації часто отримує лише статичні характеристики, якість її роботи може суттєво змінитися. Тому до навчальних прикладів доцільно включати допустимі конфігурації відсутності окремих інформаційних каналів.

Для захисту від надмірної залежності від одного експерта може застосовуватися регуляризація керуючої мережі. Однак примусове вирівнювання ваг не завжди доцільне, оскільки інформативність джерел даних може об'єктивно відрізнятися. Необхідно дослідити, чи покращує адаптивний механізм якість класифікації порівняно з фіксованими вагами. Особливу увагу слід приділити випадкам, коли двійковий і структурний експерти використовують взаємозалежні ознаки одного файлу.

Додатково до підсумкової оцінки доцільно визначати ступінь узгодженості експертів. Для цього можна використовувати зважену дисперсію індивідуальних оцінок $p_k = \sigma(z_k)$ відносно їхнього середнього значення. Такий показник відображає розбіжність експертних висновків. Він не є повною мірою невизначеності нейронної мережі, але може використовуватися як ознака необхідності додаткового аналізу.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Впровадження системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів передбачає підготовку програмного середовища для автоматизованого дослідження потенційно небезпечних файлів та інтеграції результатів із засобами антивірусного захисту. Програмний комплекс призначений для отримання характеристик програмних об'єктів, виконання спеціалізованих нейромережевих моделей та формування узагальненої оцінки загрози. Аналіз може здійснюватися за двійковими, структурними та поведінковими ознаками. Результати використовуються для визначення необхідності додаткової перевірки або застосування захисної політики. Головне вікно програми показано на рисунку 5.1.



Рисунок 5.1 – Головне вікно програми

Для розгортання аналітичної підсистеми доцільно використовувати серверну операційну систему Linux або Windows із підтримкою Python та

необхідних бібліотек машинного навчання. Основою програмного середовища може бути PyTorch, який забезпечує виконання нейромережевих експертів і механізму об'єднання їхніх оцінок. Для чисельного оброблення ознак передбачається використання NumPy. Аналіз структури виконуваних файлів Windows може здійснюватися засобами LIEF або pefile. Конкретні версії компонентів повинні відповідати залежностям програмного проєкту та формату підготовлених моделей.

Апаратні вимоги визначаються складністю нейронних мереж, розмірами досліджуваних файлів та кількістю одночасних завдань. Для базового статичного аналізу може використовуватися центральний процесор із достатнім обсягом оперативної пам'яті. За необхідності прискорення нейромережевих обчислень доцільно передбачити графічний адаптер із підтримкою CUDA. Наявність GPU дозволяє розглядати паралельне виконання експертних моделей і пакетне оброблення ознак. Проте його використання потребує сумісних драйверів і відповідного варіанта PyTorch. Для зберігання підозрілих файлів необхідно передбачити окремий захищений дисковий простір.

Підготовка програмного середовища починається зі встановлення сумісного інтерпретатора Python. Для ізоляції залежностей доцільно створити окреме віртуальне середовище. Після його активації встановлюються бібліотеки чисельного аналізу, машинного навчання та оброблення виконуваних файлів. Далі перевіряється правильність завантаження модулів і доступність необхідного обчислювального пристрою. Якщо передбачається використання GPU, необхідно додатково підтвердити можливість виконання тензорних операцій на графічному прискорювачі.

Наступним етапом є підготовка файлів навчених нейромережевих моделей. Для кожного експерта необхідно визначити місце зберігання параметрів, формат вхідних ознак і структуру вихідного результату. Двійковий експерт повинен отримувати послідовності або блоки байтів відповідно до процедури навчання. Структурний експерт використовує вектор характеристик PE-файлу. Поведінкова модель приймає підготовлені послідовності подій. Перед початком експлуатації

необхідно перевірити узгодженість розмірностей, словників категоріальних ознак і параметрів нормалізації з відповідними моделями.

Окремої підготовки потребує модуль інтеграції експертних оцінок. Для його роботи необхідно завантажити параметри керуючої нейронної мережі та визначити порядок передавання результатів спеціалізованих експертів. Додатково налаштовуються правила оброблення відсутніх інформаційних каналів. Якщо поведінкова телеметрія недоступна, система повинна використовувати результати статичного аналізу без довільного заповнення відсутніх ознак. За відсутності всіх експертних результатів формується відповідний статус неможливості оцінювання.

Для зберігання результатів доцільно передбачити реляційну базу даних. Як можливе рішення може використовуватися PostgreSQL. У сховищі необхідно організувати облік завдань, криптографічних ідентифікаторів файлів, результатів експертного аналізу та версій моделей. Для кожного об'єкта доцільно зберігати SHA-256, час перевірки, доступні групи ознак та сформовану оцінку загрози. Окремо реєструється застосована політика реагування. Це дозволяє відтворювати обставини прийняття рішення та перевіряти правильність роботи ансамблю.

Перед підключенням антивірусного комплексу необхідно підготувати механізм отримання програмних об'єктів. Для цього може використовуватися локальний API або захищена серверна служба. Вхідні запити повинні проходити автентифікацію, перевірку допустимого розміру та контроль підтримуваного формату. Досліджувані файли необхідно розміщувати в ізольованому сховищі без дозволу на безпосереднє виконання. Права доступу до цього сховища повинні обмежуватися службовими процесами аналізу. Передавання файлів через мережу необхідно здійснювати захищеним каналом.

Для виконання поведінкового аналізу доцільно передбачити окреме ізольоване середовище. Воно може бути реалізоване на базі спеціалізованої пісочниці з підтримкою контрольованого запуску програм. Відповідне середовище повинно бути відокремлене від основного сервера аналітики та корпоративних робочих станцій. Необхідно встановити обмеження мережевої взаємодії, використання ресурсів і доступу до зовнішніх систем. Після

завершення дослідження отримані поведінкові події передаються до аналітичного модуля, а ізольоване середовище повертається до визначеного початкового стану.

Початкове налаштування системи включає встановлення параметрів класифікації та реагування. Для агрегованої оцінки визначаються пороги низького й високого ризику. Окремо задається допустимий рівень розбіжності між нейромережевими експертами. Значення цих параметрів повинні визначатися за результатами валідації моделей. За відсутності підтверджених експериментальних даних їх необхідно розглядати як попередні налаштування. Автоматичне блокування файлів не слід активувати до перевірки частоти помилкових спрацювань та правильності застосування захисної політики.

Рекомендована послідовність запуску передбачає початкову перевірку доступності сховищ і конфігураційних параметрів. Після цього ініціалізуються модулі статичного аналізу та завантажуються нейромережеві експерти. Наступним активується механізм об'єднання оцінок і перевіряється готовність обраного обчислювального пристрою. Далі запускається служба приймання завдань і компонент керування чергою. За наявності поведінкового аналізу додатково перевіряється доступність ізольованого середовища. Завершальним етапом активуються засоби взаємодії з антивірусним комплексом і користувацький інтерфейс.

Первинну перевірку працездатності доцільно виконувати на підготовленому наборі контрольних файлів. Спочатку перевіряється правильність обчислення SHA-256 та виділення структурних ознак PE. Після цього виконується нейромережевий аналіз зразків із відомими характеристиками. Необхідно підтвердити коректність вихідних розмірностей, допустимість числових оцінок та формування підсумкового статусу. Окремо перевіряються випадки відсутності поведінкових даних, пошкоджених файлів і непідтримуваних форматів. Для кожного випадку система повинна повертати визначений результат без аварійного завершення.

Перевірка інтеграції з антивірусним комплексом передбачає передавання контрольного завдання через підготовлений програмний інтерфейс. Після його

приймання необхідно перевірити правильність ідентифікації об'єкта, виконання аналітичного конвеєра та повернення структурованої відповіді. Результат повинен містити статус аналізу, агреговану оцінку та рекомендовану дію. Додатково перевіряється збереження запису в базі даних. На початковому етапі доцільно використовувати режим спостереження без автоматичного видалення або блокування файлів.

Для забезпечення ідентифікації програмного продукту необхідно передбачити відображення інформації про його розробника та належність до відповідної магістерської кваліфікаційної роботи. Авторські відомості доцільно розміщувати в окремому інформаційному розділі програми. Вони повинні бути відокремлені від конфіденційних параметрів антивірусного комплексу, службових облікових даних і характеристик досліджуваних файлів. Інформацію про авторство розробленого програмного забезпечення представлено на рисунку 5.2.

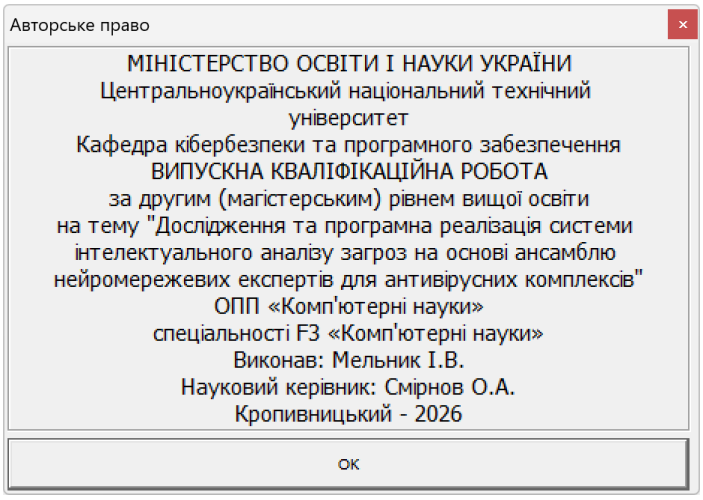


Рисунок 5.2 – Шаблона форма авторського права

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Метою розробки є дослідження та програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Об'єктом дослідження є процес інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Предметом дослідження є методи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Методи дослідження базуються на методах побудови нейронних мереж, методах математичної статистики, методах розробки програмного забезпечення.

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

– Удосконалено метод інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

– Розроблено вітчизняний продукт інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів, який має більш широкі можливості, на відміну від існуючих аналогів.

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

7.1 Вступ

Характерною ознакою сучасного науково-технічного прогресу практично у всіх сферах діяльності людини є широке застосування комп'ютерних технологій, заснованих на використанні електронно-обчислювальних машин (ЕОМ). Сьогодення, а тим більше, майбутнє, вже важко уявити без комп'ютерів та іншої електронної техніки. Адже саме завдяки їм стала можливою швидка обробка величезних обсягів інформації, виконання необхідних розрахунків та інших видів робіт, пов'язаних з обробкою текстових даних та ілюстраційних зображень, організація оперативного отримання та передачі інформації, збереження її значних обсягів електронним способом.

Стрімке впровадження комп'ютерів не тільки в сфері управління виробництвом, в банківській систему, бізнесі, системі освіти, але також на транспорті, сфері обслуговування призвело до того, що десятки мільйонів людей у всьому світі виявились втягнутими у взаємодію людини з комп'ютером. Природно виникає запитання: настільки безпечною є ця взаємодія для людини? Адже відома аксіома про те, що будь-яка взаємодія людини та засобів праці двостороння.

Людина впливає на удосконалення засобів праці, а останні –на працюючу людину. Отже, навіть сучасні технології та техніка, до яких безперечно, залежать комп'ютерні технології та ЕОМ несуть у собі певні потенційні небезпеки. У зв'язку з цим набуває актуальності адекватна оцінка конкретних умов і характеру праці, яка сприяє обґрунтованому розробленню та впровадженню комплексу заходів і засобів, спрямованих на збереження здоров’я і працездатності людини в процесі праці за рахунок поліпшення параметрів виробничого середовища, зменшення важкості, напруженості трудового процесу та збереження здоров'я працівників на комп'ютеризованих робочих місцях.

Законодавством України чітко врегульовано норми та вимоги до використання комп’ютерної техніки на підприємстві, безпосередньо й охорона праці на підприємстві при роботі за комп’ютером., зокрема «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями», затверджені наказом Мінсоцполітики від 14.02.2018 № 207 [1], «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-97. [2].

Загальні вимоги пожежної безпеки під час експлуатації комп’ютерної техніки визначають «Правила пожежної безпеки в Україні» (затверджені наказом МВС від 30.12.2014 № 1417) [3], комп’ютерних класів – пункт 3 розділу VIII «Правил пожежної безпеки для навчальних закладів та установ системи освіти України» (затверджені наказом МОН від 15.07.2016 № 974). [4] та інші державні стандарти, що регламентують експлуатування комп’ютерної техніки як радіоелектронної апаратури.

7.2 Шкідливі і небезпечні фактори при роботі з комп’ютером

Можна виділити наступні основні фактори, що впливають на стан здоров'я людей, які працюють за комп'ютером:

– сидяче положення на протязі тривалого періоду;

– вплив електромагнітного випромінювання монітора;

– втома очей, навантаження на зір;

– перевантаження суглобів кистей;

– стрес при втраті інформації або при виникненні критичних помилок.

У кожному з цих випадків ступінь ризику прямо пропорційний часу, що проводиться за комп’ютером і поблизу від нього. В сучасних умовах взаємодія людини з технікою значно ускладнилась, що вимагає комплексного підходу, який передбачає розгляд людини, технічних засобів праці та виробничого середовища, як взаємозв'язаних елементів єдиної системи. Все вищевказане в повній мірі відноситься й до системи «людина-комп'ютер-середовище».

Вагомий вплив на працездатність та здоров’я користувачів комп’ютерів здійснює виробниче середовище. Це середовище у виробничих приміщеннях (офісах), в основному, визначається мікрокліматом, освітленням, наявністю шкідливих речовин у повітрі, рівнем шуму та випромінювання.

Для того, щоб об’єктивно проаналізувати відповідність умов праці діючим нормативно-правовим актам та запропонувати заходи щодо зменшення негативного впливу комп’ютера на організм людини необхідно скласти санітарно-гігієнічну характеристику умов праці співробітника, який працює з програмним продуктом.

7.3 Аналіз санітарно-гігієнічних умов праці на робочому місці користувача ПК

Розглянемо приміщення в якому працює користувач ПК з програмним продуктом.

Приміщення має одностороннє природне освітлення і загальне штучне освітлення. Стіни і стеля обклеєні світлими шпалерами, підлога вкрита темним ламінатом. У приміщенні відсутні сильні вібрації та шкідливі речовини. Склад повітря відповідає нормі. У кімнаті знаходиться ПК з 4-ядерним процесором і 23-дюймовим IPS-монітором, а також меблі.

Приміщення має довжину 4м, ширину 3,5м, висоту стелі 2,7м. Кількість робочих місць – одне. Площа – 14 $м^2$, об'єм – 37,8 $м^3$. Виходячи з цього, отримано дані, наведені в таблиці 7.1.

Таблиця 7.1 – Фактичні та нормативні значення параметрів приміщення

Параметр	Норма *	Реальні параметри
Площа, S	не менше 6 $м^2$	14 $м^2$
Об’єм, V	не менше 20 $м^3$	37,8 $м^3$

*Згідно ДСанПіН 3.3.2.007-98 (Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин).

За даними, які наведено у табл. 7.1, можна зробити висновок, що отримані показники, площа та об’єм приміщення у розрахунку на одно робоче місце користувача ПК відповідає чинним нормам і вимогам.

Щодо мікроклімату, то згідно з ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» [5] роботу з ПК можна віднести до категорії легка – 1а. Джерелами тепла в цьому приміщенні є люди, електроустаткування, освітлювальні прилади в темний час доби і система опалювання взимку. Оператором виділяється до 120 ккал теплової енергії за годину. Оптимальні та фактичні значення параметрів мікроклімату приведені в таблиці 7.2.

Таблиця 7.2 – Значення параметрів мікроклімату

Період року	Параметр	Оптимальний*	Фактичний
Теплий	Температура	23 – 25 ^{0} С	24^0 С
	Вологість	40 – 60%	50%
	Швидкість повітря	< 0,1м/с	
Холодний	Температура	22 – 24^0 С	23^0 С
	Вологість	40 – 60%	55%
	Швидкість повітря	< 0,1м/с	

*ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень»

За отриманими замірами параметрів мікроклімату можна зробити висновок, що всі показники задовольняють вимогам, зазначеним для робіт категорії праці легка 1а і є задовільними для здоров'я людини.

Щодо освітлення, то згідно з ДБН В.2.5-28:2006 «Природне і штучне освітлення» [6] ця робота відноситься до Va розряду зорових робіт. Передбачається використання природного, штучного і змішаного освітлення.

Природне освітлення здійснюється за допомогою вікна, площа якого складає S' = 1,8х1,5 = 2,7 м^2 і є бічним освітленням. У світильниках місцевого і загального освітлення використовуються світлодіодні лампи потужністю 20 Вт

із світловим потоком однієї лампи 900 лм. Згідно замірів рівень освітлення в даному приміщенні і на робочому місці складає в межах 350-500 лк, що відповідає нормованому значенню.

Джерелом шуму в приміщенні є комп'ютер. Вентилятори (кулери) системного блоку, процесора, відеокарти і блоку живлення є сучасними і мають низький рівень шуму. Згідно з технічною документацією шум, зумовлений кулером в блоці живлення складає 25 дБ, кулером процесора – 30 дБ, загальний – 34 дБ. Враховуючи незначний рівень шуму від персонального комп'ютера і незначний рівень фонового шуму від іншого устаткування, можна стверджувати, що сумарний рівень шумового забруднення приміщення не перевищує максимально допустимий рівень коригованої звукової потужності і складає не більше 50 дБА, що відповідає рівню шуму для приміщень з комп’ютерною технікою згідно Державних санітарних правил і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-97.

У приміщенні відсутні джерела інфрачервоного, ультрафіолетового і електромагнітного випромінювання, бо монітор ПК вироблений на основі рідкокристалічної матриці, підсвітка якої здійснюється неоновою лампою, які не мають сильного електромагнітного випромінювання і сертифіковані в Україні.

Блок живлення є екранованим і не випускає вищезазначених видів випромінювання.

7.4 Розробка заходів з умов поліпшення охорони праці

Перерахуємо проведені заходи щодо забезпечення умов праці на робочому місці користувача ПК.

З точки зору забезпечення електробезпеки до цих заходів можна віднести: устаткування розподільних щитів спеціальними розетками з заземлюючими контактами; організація заземлення всіх приладів і пристроїв;

періодична перевірка всіх приладів і пристроїв; щорічна здача іспитів з охорони праці.

З точки зору забезпечення оптимальних умов мікроклімату, рівня звуку і освітленості до цих заходів можна віднести: організацію природної вентиляції, за допомогою дефлектора, для забезпечення необхідного повітрообміну в приміщенні вузла; організацію системи центрального опалювання, для підтримки оптимальної температури в холодний період року; організацію штучного загального освітлення, для забезпечення необхідних умов зорової роботи, що відповідають, оформлення паспорта на приміщення вузла, з занесенням в нього вимірювань освітленості і рівня звуку, проведених відділом охорони праці.

Крім рекомендацій щодо конкретного приміщення, де було проведено дослідження умов праці, існують загальні вимоги, які зарекомендовані відповідними нормативними документами.

Правильна організація робочих місць запобігає передчасній втомлюваності користувача і сприяє збереженню здоров'я. Організація робочого місця передбачає:

- правильне розміщення робочого місця у виробничому приміщенні;
- вибір ергономічного обґрунтованого робочого положення, виробничих меблів з урахуванням характеристик людини;.
- раціональне компонування обладнання на робочих місцях;
- урахування характеру й особливостей трудової діяльності. Стосовно робочих місць користувача ВДТ, то організація робочого має забезпечуватися відповідно до ДСанПіН 3.3.2-007-97. Для запобігання перевтомленню необхідно виконувати вправи для очей та дотримуватись розпорядку роботи та відпочинку. На робочому місці реалізовувався режим відпочинку: кожні дві години – перерва для виконання фізичних вправ для м‘язів очей.

7.5 Протипожежний захист

Пожежі в приміщеннях з оргтехнікою становлять особливу небезпеку, бо поєднані з великими матеріальними збитками. Пожежа може виникнути при взаємодії горючих речовин і джерел запалювання. Горючими речовинами є будівельні та опоряджувальні матеріали, пластмасові корпуси техніки, шнури тощо. Джерелами запалювання можуть бути електронні схеми комп'ютерів, принтерів, пристроїв електроживлення, де внаслідок різних порушень виникає перегрівання елементів, утворюються електричні іскри та дуги, здатні спричинити займання горючих матеріалів.

При обслуговуванні, ремонтних та профілактичних роботах використовуються різні легкозаймисті рідини, прокладаються тимчасові електропровідники, здійснюється паяння. Виникає додаткова пожежна небезпека, яка потребує відповідних заходів пожежного захисту.

До засобів гасіння пожежі, призначених для локалізації невеликих займань, належать вогнегасники, сухий пісок, азбестові ковдри. Приміщення, в якому встановлено комп'ютери і де немає необхідності влаштування систем автоматичного пожежогасіння, необхідно оснащувати переносними вуглекислотними вогнегасниками з розрахунку 2 шт. на кожні 20 $м^2$ в приміщеннях.

Звуковбирне облицювання стін, стель приміщень треба виконувати з негорючих та важко горючих матеріалів.

З метою виявлення початкової стадії займання необхідно використовувати пристрої систем автоматичного пожежогасіння там, де цього вимагають Правила пожежної безпеки.

З точки зору забезпечення пожежної безпеки до цих заходів можна віднести наявність схеми евакуації з приміщення у випадку пожежі, прикріплену на вхідні двері.

7.6 Розрахункова частина

В приміщенні (де відсутні джерела виділення шкідливих речовин) працює одна людина. Робота пов’язана з використанням ПЕОМ. Розміри приміщення: А = 4 м, В = 3.5 м, Н = 2.8 м, устаткування займає 15% об’єму. Визначимо найменшу необхідну кількість повітря для вентиляції.

Для приміщень, в яких відсутні виділення шкідливих речовин у повітрі, розрахунок вентиляції здійснюється залежно від кількості працюючих.

Необхідна кількість повітря (м^3/год.), яка забезпечує відповідність параметрів повітря робочої зони нормованим значенням, визначається за наступною формулою:

$$L = L' \cdot N,$$

де

L' – нормативна кількість повітря на одного працюючого, яка залежить від питомого об’єму приміщення, м^3/(год.-люд.);

N – кількість працюючих.

Питомий об’єм приміщення $V_п$, (м^3 /люд.), визначається за формулою:

$$V_n = V/N,$$

де V – об’єм приміщення, м^3.

Визначаємо вільний об’єм приміщення

$$V = A \cdot B \cdot H \cdot 0{,}85 = 4 \cdot 3{,}5 \cdot 2{,}8 \cdot 0{,}85 = 33{,}3 \text{ м}^3.$$

Питомий вільний об’єм складає

$$V' = V / N = 33{,}2 / 1 = 33{,}2 \text{ м}^3/\text{люд.} > 20 \text{ м}^3/\text{люд.}$$

Нормована кількість повітря на одну людину при V' > 20 м^3 /люд. становить 30 м^3/(год.·люд.).

Висновки до розділу

У даному розділі магістерської роботи проведено аналіз умов працівника робота якого пов’язана з комп’ютерною технікою. Проведено аналіз основних санітарно – гігієнічних показників в заданому приміщені , де працівник зайнятий постійною роботою за комп’ютером.. Створені умови повинні забезпечувати

комфортну роботу. На підставі вивченої літератури з даної проблеми, були зазначені оптимальні параметри мікроклімату, освітлення, допустимі рівні шуму та іонізуючого випромінювання при роботі з ПЕОМ, а також розраховано найменшу необхідну кількість повітря для вентиляції.

Дотримання умов, що визначають оптимальну організацію робочих місць працівників, дозволить зберегти гарну працездатність протягом усього робочого дня, підвищить як в кількісному, так і в якісному відносинах продуктивність їх праці.

8 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

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 інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

– Досліджена система інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

– На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів.

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.

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.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мельник І.В. Дослідження та програмна реалізація системи інтелектуального аналізу загроз на основі ансамблю нейромережевих експертів для антивірусних комплексів // Збірник праць молодих науковців ЦНТУ. – Вип. 17. – Кропивницький: ЦНТУ, 2027.

2. Knuth D. The Art of Computer Programming, Vol. 1: Fundamental Algorithms, 3rd Edition 3rd Edition. – Addison-Wesley Professional, 2019. – 672 p.

3. Mattmann C. Machine Learning with TensorFlow, Second Edition. – Manning, 2020. – 1124 p.

4. Mueller J.P., Massaron L. Machine Learning For Dummies. – Wiley, 2016. – 714 p.

5. Teofili T. Deep Learning for Search. – Manning, 2019. – 695 p.

6. Rungta K. TensorFlow in 1 Day: Make your own Neural Network. – Publishdrive, 2019. – 587 p.

7. Weidman S. Deep Learning from Scratch: Building with Python from First Principles. – O'Reilly. 2019. – 252 p.

8. Rajasekaran S., Vijayalakshmi Pai G.A. Neural networks, fuzzy logic, and genetic algorithms: synthesis and applications (with cd-rom) Kindle Edition. – PHI, 2013. – 628 p.

9. Богаченко, С., Смірнов, О., Козірова, Н., Смірнова, Т., Константинова, Л., Смірнов, С. «Методи зменшення обчислювальної складності легковагових нейронних мереж із використанням баз даних для мобільних та edge-платформ». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, т. 3 № 35, С.110-118.

10. Vintenko, B., Myronets, I., Smirnov, O., Smirnova, T. «Enhancing the Reliability of Input Data for Nuclear Power Plant Operator Support Systems». *International Conference on Sensors, Devices and Systems. SDaS 2025. Lecture Notes in Electrical Engineering*, 2026. vol 1617. pp 3-12 Springer, Cham.

11. Богаченко, С., Смірнов, О., Буравченко, К., Смірнова, Т., Конопліцька-Слободенюк, О., Якименко, Н., Смірнов, С. «Обмеження ресурсів мобільних та edge-платформ при розробці програмного забезпечення для реалізації та оптимізації моделей машинного навчання». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, т. 2 № 34, С. 677-686.

12. Смірнов, О., Ткачук, Р., Козірова, Н., Константинова, Л., Конопліцька-Слободенюк, О., Якименко, Н., Смірнов, С.. «Дослідження застосування векторних баз даних у генеративному штучному інтелекті». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, Том 1 № 33, 667-682.

13. Вінтенко Б.Ю., Смірнова Т.В., Миронець І.В., Смірнов О.А., Буравченко К.О. «Метод оцінки функціональної стійкості комп'ютерно-орієнтованих процедур системи підтримки оперативного персоналу АЕС». *Системи управління, навігації та зв'язку*, 2026, вип. 2(84), С. 62-69.

14. Смірнов О., Заріцкий В., Буравченко К., Конопліцька-Слободенюк О., Константинова Л., Якименко Н., Смірнов С. «Оптимізація розпізнавання облич за допомогою CUDA прискореної бібліотеки dlib». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, Том 4, № 32, С. 573-582.

15. Лисенко, І., Минайленко, Р., Смірнов, С., Буравченко, К., Якименко, Н., Смірнов, О. «Дослідження інструментів штучного інтелекту для інтелектуального аналізу даних». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2025, № 3(31), С. 227–241.

16. Kuznetsov O., Frontoni E., Arnesano M., Smirnov O., Khruskov B. «Biometric Authentication in TinyML: Opportunities and Challenges». *Tiny Machine Learning: Design Principles and Applications*, 2026, pp. 587-633.

17. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61.

18. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». *Кібербезпека: освіта, наука, техніка*. 2025. Том 2 № 30. С. 413-427, 2025.

19. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». *Кібербезпека: освіта, наука, техніка*. 2025. Том 2 № 30. С.195-208, 2025.

20. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704–716, 2025

21. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.

22. Kuznetsov, O., Smirnov, O., Akhmetov, B., Alimseitova, Z., Imoize, A.L. «Deep Learning Frontiers in Copy-Move Forgery Detection: Advances, Challenges, and Future Directions». *Advancements in Cybersecurity Next Generation Systems and Applications*, 2025. 202-229.

23. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.

24. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп’ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». *Центральноукраїнський науковий вісник. Технічні науки.* 2025. Вип. 11(42), ч. ІІ. С.52-62.

25. Смірнов, О.А., Константинова, Л.В., Конопліцька-Слободенюк, О.К., Козірова, Н.В, Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». *Кібербезпека: освіта, наука, техніка.* 2025. №3(27), С. 429–448.

26. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.

27. Smirnov O., Fedorov E., Neskorodieva A., Neskorodieva T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». *CEUR Workshop Proceedings* Volume 3664, 2024, Pages 11-23.

28. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.

29. Malyukov V., Bebeshko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale Process of Digital Currencies Under Fuzzy Conditions». *Lecture Notes in Networks and Systems*, 2023, 729 LNNS, pp. 104–112.

30. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.

31. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.

32. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-

56.

33. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». CEUR Workshop Proceedings, Volume 3312, 2022, pp. 47-58.

34. 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, pp. 1-12.

35. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.

36. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.

37. Kuznetsov, A., Oleshko, I., Chernov, K., Bagmut, M., Smirnova, T. «Biometric authentication using convolutional neural networks». Lecture Notes in Networks and Systems. Volume 152, 2021, Pages 85-98.

38. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w.

39. Smirnov O., Neskorodieva T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». CEUR Workshop Proceedings Volume 3101, 2021, Pages 192-207.

40. 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.

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

42. 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.

43. 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.

44. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.

45. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.

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. 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.

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. Smirnov, S., Bulekbaeva, G., Kikvidze, O.G., Lakhno, V., Brzhanov, R., Tabylov, A. «Computer simulation in the MathCAD package of plastic deformation of the deposited layer on the flat surface of the part». Journal of Theoretical and Applied

Information Technology Volume 97, Issue 20, 2019, Pages 2467-2484.

56. Smirnov A.A., Kuzne tsov 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.

57. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95

58. Смірнов, О.А., Усік П.С., Полігенько О.О., Одарченко Р.С., Терещенко Л.Ю. «Інформаційна технологія та програмне забезпечення для підвищення ефективності планування підсистеми базових станцій стільникового зв'язку». Проблеми телекомунікацій. № 1(26). С. 83-96. 2020.

59. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» Вісник Черкаського державного технологічного університету. Технічні науки. №4. С. 103-110. 2020.

60. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.

61. Смірнов, С.А., Смірнова, Т.В., Минайленко, Р.М., Доренський, О.П., Сисоєнко С.В. «Хмарна автоматизована система інтелектуальної підтримки прийняття рішень для технологічних процесів». Вісник Черкаського державного технологічного університету. Технічні науки. №4, 2020, С. 84-92.