Центральноукраїнський національний технічний університет
Центр заочної та дистанційної освіти
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 оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання”

Виконав здобувач вищої освіти
ІІ курсу, групи КН-25МЗ
ОПП «Комп’ютерні науки»
спеціальності F3 «Комп’ютерні науки»
_____ Швидкий Ю.Ю.
«____» _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Марченко К.М.
«____» _____ 2026 р.

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

Рецензент _____
_____

Підписано КЕП
Центральноукраїнський національний технічний університет
Швидкий Юрій Юрійович
Сертифікат: 514B5C86A1E5DA110400000044CC200054E8A005
Дійсний з 22.04.2026 02:28:21 по 22.04.2027 02:28:20

Центральноукраїнський національний технічний університет
Центр *Заочної та дистанційної освіти*
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

Швидкому Юрію Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження та програмна реалізація системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання*

2. Керівник роботи *Марченко Костянтин Миколайович, кандидат технічних наук, доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 44-13 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 оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання*

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

Швидкий Ю.Ю. Дослідження та програмна реалізація системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання. 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 оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Метою розробки є дослідження та програмна реалізація системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Об'єктом дослідження є процес оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Предметом дослідження є методи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Методи дослідження базуються на методах машинного навчання, методи захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

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, машинне навчання, оцінка ризиків, безпека, виявлення аномалій, конфігурації міжмережевих екранів

ABSTRACT

Shvydkyi Yu.Yu. Research and Software Implementation of a System for Assessing Security Risks and Detecting Anomalies in Firewall Configurations Using Machine Learning. F3 Computer Science. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification thesis for the second (master's) level of higher education, software has been developed for a system designed to assess security risks and detect anomalies in firewall configurations using machine learning.

The objective of this development is to research and implement a software system for assessing security risks and detecting anomalies in firewall configurations using machine learning.

The object of the research is the process of assessing security risks and detecting anomalies in firewall configurations using machine learning.

The subject of the research consists of methods for assessing security risks and detecting anomalies in firewall configurations using machine learning.

The research methodology is based on machine learning techniques, information security methods, mathematical statistics, and software development practices.

The outcome of the work is a software implementation of a system for assessing security risks and detecting anomalies in firewall configurations using machine learning.

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 using the software are provided.

The software can be used on PCs running the Windows 10/11 operating system.

The software was developed in the Python environment.

Keywords: computer science, machine learning, risk assessment, security, anomaly detection, firewall configurations

ВІДОМІСТЬ ПРОЕКТУ

		Текстові документи			
1	А4	Пояснювальна записка	91	–	
2	А4	Робоча програма	22	–	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 10
ВСТУП..... 11
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ 14
1.1 Призначення системи..... 14
1.2 Область застосування 14
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ 16
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти..... 16
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування 24
2.3 Розгорнута постановка завдання 25
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ 26
3.1 Опис функціонування системи 26
3.2 Розробка структурної схеми..... 31
3.3 Розробка функціональної схеми 47
3.4 Розробка діаграми процесів 49
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ 51
4.1 Розробка блок-схем та опис алгоритмів функціонування системи 51
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ..... 66
6 НАУКОВА НОВИЗНА 72

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ 73
7.1 Вступ 73
7.2 Аналіз умов праці на робочому місці ІТ-фахівця 74
7.3 Пропозиції щодо підвищення працездатності ІТ – фахівців 77
7.4 Розрахункова частина 79
7.5 Висновки до розділу 81
8 ОСНОВНІ ВИСНОВКИ 82
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 84

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЛОМ	–	локальна обчислювальна мережа
MME	–	міжмережні екрани
ATM	–	асинхронний режим передачі
BSD	–	адаптована для Internet реалізація операційної системи UNIX
ICMP	–	міжмережний протокол управляючих повідомлень
IP	–	Internet Protocol – міжмережний протокол
NFS	–	мережна файлова система
PPP	–	протокол передачі від точки до точки
RFC	–	опис набору протоколів Internet
RPC	–	віддалений виклик процедури
SLIP	–	міжмережний протокол для послідовного каналу
SMTP	–	Simple Mail Transfer Protocol – простий протокол передачі пошти
TCP	–	Transmission Control Protocol – протокол управління передачею
UDP	–	User Datagram Protocol – протокол користувальницьких датаграм
UNIX	–	багатозадачна операційна система
UTP	–	незахищена вита пара
URL	–	уніфікований покажчик інформаційного ресурсу

ВСТУП

Актуальність теми. Зі швидким розвитком цифрових комунікацій та ескалацією кіберзагроз, традиційні системи брандмауерів стали принципово недостатніми через їхню виключну залежність від статичних правил та методів виявлення на основі сигнатур. Ці традиційні системи не здатні адаптуватися до нових, раніше не бачених моделей атак і потребують постійного ручного оновлення. У даній магістерській роботі представлено проектування та комплексне впровадження інтелектуальної системи брандмауера на основі штучного інтелекту, яка принципово підвищує безпеку мережі шляхом інтеграції передових алгоритмів машинного навчання, архітектур глибокого навчання та аналізу поведінки в реальному часі. Запропонована система здатна безперервно аналізувати великі обсяги мережевого трафіку, виявляти складні моделі та автономно виявляти як відомі, так і невідомі загрози, включаючи атаки нульового дня, розширені постійні загрози (APT), програми-вимагачі та внутрішні загрози. Завдяки постійному навчанню на основі історичних даних про трафік та живих мережевих сеансів, брандмауер динамічно адаптується до кіберзагроз, що розвиваються, забезпечуючи суттєво підвищену точність виявлення та значне зниження рівня хибнопозитивних результатів. Механізм роботи охоплює збір даних з гетерогенних мережевих джерел, багатоетапну попередню обробку, навчання моделей штучного інтелекту з використанням контрольованих та неконтрольованих парадигм, моніторинг трафіку в реальному часі, автоматизовану класифікацію загроз та інтелектуальне прийняття рішень з миттєвою реакцією. Система додатково включає модуль біометричного розпізнавання облич, реалізований за допомогою каскадного класифікатора Хаара від OpenCV, що забезпечує додатковий рівень контролю фізичного доступу до критичної мережевої інфраструктури. Експериментальна оцінка демонструє точність класифікації 90-98%, зниження кількості хибних спрацьовувань на понад 60% порівняно з системами на основі правил та

затримку реагування на загрози в режимі реального часу менше однієї секунди. Цей підхід забезпечує проактивне, інтелектуальне та адаптивне рішення безпеки, придатне для сучасних мережевих середовищ, включаючи хмарні платформи, корпоративні мережі, екосистеми Інтернету речей (IoT) та великомасштабні веб-додатки.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

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

– Огляд існуючих систем оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

– Дослідження системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

– Програмна реалізація системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Об'єктом дослідження є процес оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Предметом дослідження є методи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Методи дослідження базуються на методах машинного навчання, методи захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

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

– Удосконалено метод оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

– Розроблено вітчизняний продукт оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

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 оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання, 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

Інтелектуальні брандмауери на основі штучного інтелекту (ШІ) представляють собою наступне покоління інфраструктури мережевої безпеки, розробленої для захисту цифрових середовищ від постійно зростаючого та дедалі складнішого ландшафту кіберзагроз. Зростаюча складність сучасних кібератак вимагає систем безпеки, здатних навчатися, адаптуватися та реагувати автономно – можливостей, які принципово перевищують конструктивні параметри традиційних технологій брандмауерів.

Традиційні брандмауери працюють на основі статичних наборів правил, визначених адміністратором, та попередньо скомпільованих баз даних сигнатур. Така архітектура дозволяє ефективно блокувати розпізнані загрози, але за своєю суттю є реактивною: загрозу необхідно ідентифікувати, проаналізувати та задокументувати, перш ніж захист можна буде розгорнути. В епоху, коли щодня з'являються нові варіанти шкідливого програмного забезпечення, експлойти нульового дня та складні постійні загрози, ця реактивна парадигма залишає критичні вікна вразливості, які зловмисники активно використовують.

1.2 Область застосування

Розумні брандмауери на основі штучного інтелекту долають ці фундаментальні обмеження, використовуючи моделі машинного навчання, які вивчають статистичні характеристики як нормальної поведінки мережі, так і відомої шкідливої активності. Після навчання ці моделі можуть оцінювати новий мережевий трафік у режимі реального часу, порівнюючи спостережувану поведінку з вивченими базовими показниками та позначаючи аномальні закономірності, які суттєво відхиляються від очікуваних норм. Ця можливість дозволяє виявляти загрози, з якими ніколи раніше не стикалися, включаючи експлойти нульового дня, для яких не існує сигнатур.

Проблеми безпеки, що розглядаються в цьому дослідженні, є суттєвими та багатовимірними. Атаки нульового дня використовують раніше невідомі вразливості та не можуть бути виявлені системами на основі сигнатур. Розширені постійні загрози (APT) включають тривалі, приховані кампанії вторгнення, які поступово вилучають конфіденційні дані протягом тривалих періодів. Програми-вимагачі шифрують організаційні дані та вимагають оплату за ключі розшифрування. Розподілені атаки відмови в обслуговуванні (DDoS) перевантажують мережеву інфраструктуру, заповнюючи її трафіком від тисяч скомпрометованих хостів. Внутрішні загрози походять від авторизованих користувачів, чиї облікові дані були скомпрометовані або які діють зловмисно. Усі ці категорії загроз вимагають адаптивних можливостей виявлення поведінки, які статичні системи на основі правил не можуть забезпечити.

Дана магістерська робота робить наступний основний внесок у галузь інтелектуальної мережевої безпеки. По-перше, вона представляє комплексну багатомодельну архітектуру штучного інтелекту, яка поєднує навчання з учителем для класифікації відомих загроз, виявлення аномалій без учителя для ідентифікації загроз нульового дня та навчання з підкріпленням для адаптивної оптимізації політик. По-друге, вона представляє інтегрований модуль біометричного контролю доступу, що використовує класифікатор Хаара Каскад від OpenCV для розпізнавання облич, забезпечуючи додатковий рівень фізичної безпеки. По-третє, вона представляє механізм безперервного навчання та зворотного зв'язку, який дозволяє системі покращувати свої можливості виявлення з часом без ручного втручання. По-четверте, вона надає експериментальну оцінку, що демонструє суттєве покращення продуктивності порівняно з традиційними підходами до брандмауерів.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання, 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

Check Point

Check Point ставить мережеву безпеку під основою запобігання, єдиного управління та аналізу загроз у режимі реального часу. Для середовищ Інтернету речей такий підхід корисний, коли організаціям потрібна узгоджена політика в штаб-квартирі, філіях, хмарно-підключених сайтах та операційних місцях, не керуючи кожним середовищем як окремим островом безпеки.

Брандмауери Check Point на базі штучного інтелекту поєднують у собі запобігання загрозам на основі штучного інтелекту, запобігання вторгненням, контроль програм, перевірку зашифрованого трафіку та централізоване управління політиками. Check Point також робить акцент на виявленні та захисті пристроїв Інтернету речей завдяки своїй ширшій архітектурі мережевої безпеки, допомагаючи командам виявляти некеровані пристрої, класифікувати ризики та застосовувати засоби контролю без встановлення агентів на самі пристрої.

Практичною перевагою є зв'язок між забезпеченням брандмауера та аналітикою ThreatCloud AI. Якщо шкідлива інфраструктура, поведінка шкідливого програмного забезпечення або новий шаблон експлойту виявлені в іншому місці, ці дані можуть допомогти у запобіганні на рівні шлюзу. Це важливо в IoT-інфраструктурах, де пристрої може бути важко швидко виправити, і де блокування експлойту на мережевому рівні може бути безпечнішим, ніж очікування на виправлення на рівні пристрою.

Check Point чудово підходить для гібридних підприємств, яким потрібна єдина система політик для центрів обробки даних, філіалів, хмарних середовищ та сегментів Інтернету речей. Під час оцінювання покупці повинні перевірити

точність класифікації пристроїв, автоматизацію політик, продуктивність зашифрованого трафіку та те, наскільки легко команди безпеки можуть відокремити трафік Інтернету речей від трафіку користувачів та серверів, не створюючи некерованої бази правил.

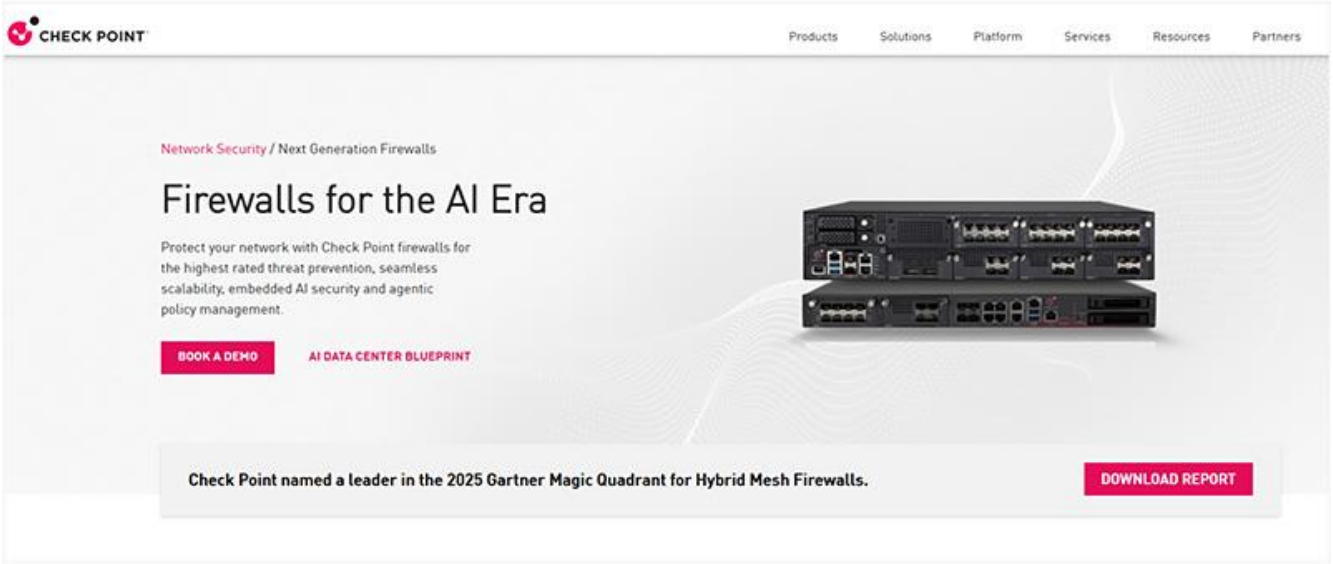

Рисунок 2.1 – Інтерфейс користувача Check Point

Ключові можливості:

– Запобігання загрозам та захист «нульового дня» на основі штучного інтелекту.

– Централізована політика в розподілених середовищах.

– Видимість пристроїв Інтернету речей та безагентне забезпечення виконання.

– Сегментація мережі та елементи керування, що відповідають вимогам програм.

– Варіанти високої доступності та масштабованих шлюзів.

Fortinet

Найсильніша позиція Fortinet у сфері Інтернету речей полягає в поєднанні безпеки та мережевої безпеки у філіях, кампусах, центрах обробки даних та

операційних середовищах. Брандмауери FortiGate входять до складу Fortinet Security Fabric та можуть працювати разом із засобами безпеки комутації, бездротового зв'язку, SD-WAN, кінцевих точок та операційних технологій.

Брандмауери Fortinet на базі штучного інтелекту використовують служби безпеки FortiGuard на базі штучного інтелекту для запобігання вторгненням, виявлення шкідливого програмного забезпечення, веб-фільтрації та аналізу загроз. Для розгортання Інтернету речей Fortinet може забезпечити видимість підключених пристроїв та забезпечити сегментацію на межі мережі, тоді як його мережевий портфель може допомогти організаціям застосовувати політику ближче до місць підключення пристроїв.

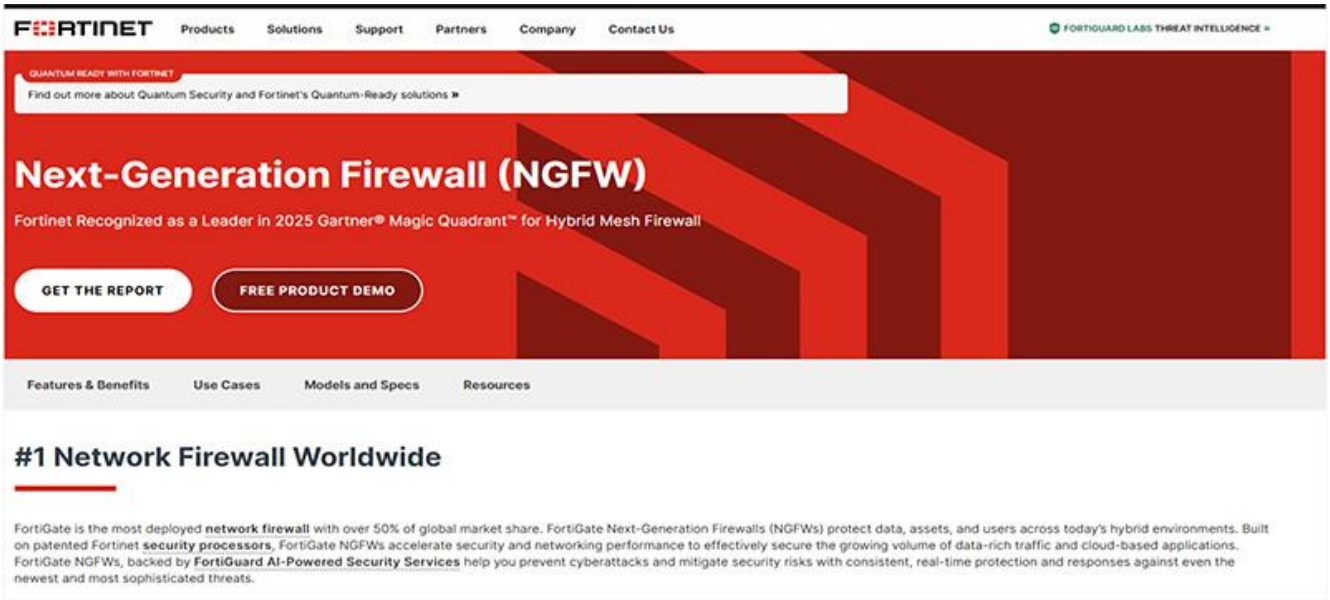

Рисунок 2.2 – Інтерфейс користувача Fortinet

Така конвергенція корисна для роздрібних торговців, виробників, постачальників логістичних послуг та розподілених підприємств, які керують багатьма об'єктами з обмеженим штатом місцевих IT-фахівців. Брандмауер філії, який також підтримує SD-WAN, комутацію та політику бездротового зв'язку, може зменшити кількість окремих пристроїв та систем управління, необхідних у кожному місці розташування.

Fortinet – це сильний вибір, коли продуктивність, розподілене розгортання та операційні технології є основними пріоритетами. Покупці повинні підтвердити, як інвентаризація пристроїв, політика брандмауера, керування комутаторним доступом та видимість OT працюють разом у тій самій архітектурі, яку вони планують розгорнути, оскільки глибина інтеграції може відрізнятися залежно від продукту та ліцензії.

Ключові можливості:

– Сервіси запобігання загрозам FortiGuard на базі штучного інтелекту.

– Потужна інтеграція філій, кампусів та SD-WAN.

– Сегментація в мережевих середовищах та середовищах підключених пристроїв.

– Широка підтримка для OT та промислового використання.

– Високопродуктивне обладнання та централізоване управління.

Cisco

Cisco розглядає безпеку брандмауера як частину ширшої екосистеми мереж та безпеки. Це може бути цінним для середовищ Інтернету речей, оскільки підключення пристроїв часто залежить від тієї ж комутаційної, бездротової, SD-WAN та периферійної інфраструктури, якою Cisco вже керує.

Брандмауери Cisco на базі штучного інтелекту поєднують захист від загроз Secure Firewall з аналітикою на основі штучного інтелекту та централізованим керуванням через Cisco Security Cloud Control. Деякі платформи брандмауерів також роблять акцент на підключенні філій та підтримці пристроїв Інтернету речей, що робить портфоліо актуальним для організацій, які хочуть, щоб безпека та мережеві операції мали більший спільний контекст.

Перевага Cisco є найбільшою, коли підприємство вже використовує мережеві, ідентифікаційні та сегментаційні технології Cisco. Контекст пристроїв із ширшого середовища може допомогти командам розробляти політики щодо того, хто або що підключається, звідки виникає з'єднання та які ресурси мають бути доступними.

Cisco найкраще підходить для великих підприємств, які цінують інтеграцію екосистеми та мають операційну зрілість для координації мережевих команд та команд безпеки. Покупцям слід перевірити узгодженість управління моделями брандмауерів, управлінням хмарою, політикою ідентифікації та інфраструктурою філій, особливо якщо середовище включає застарілі розгортання Cisco.

Ключові можливості:

– Безпечний брандмауер з операційною аналітикою на основі штучного інтелекту.

– Інтеграція з мережевими системами Cisco та засобами контролю ідентифікації.

– Сильна релевантність філії та кампусу.

– Централізоване управління та оркестрація політик.

– Підтримка сегментації в розподіленому середовищі.

Palo Alto Networks

Компанія Palo Alto Networks давно наголошує на обізнаності про програми, контексті пристроїв та політиці нульової довіри. Її портфоліо брандмауерів особливо актуальне для підприємств, яким потрібна детальна інформація про те, які пристрої взаємодіють між собою, які програми використовуються та чи відповідає поведінка трафіку очікуваній ролі пристрою.

Брандмауери Palo Alto Networks на базі штучного інтелекту використовують машинне навчання всередині брандмауера та спираються на хмарні служби безпеки для аналізу шкідливих програм, безпеки DNS, фільтрації URL-адрес та аналізу загроз. У середовищах Інтернету речей можливості компанії щодо безпеки Інтернету речей можуть додавати профілювання пристроїв та поведінковий контекст, що дозволяє базувати політики на ідентифікації та ризику пристрою, а не лише на IP-адресах чи розташуванні мережі.

Це цінно в лікарнях, кампусах, на заводах та у великих офісах, де тисячі пристроїв можуть використовувати схожі сегменти мережі, але виконувати дуже

різні функції. Підключений інфузійний насос, зчитувач бейджів та датчик навколишнього середовища не повинні отримувати однаковий доступ лише тому, що вони знаходяться в одній підмережі.

Palo Alto Networks найкраще підходить для організацій, які бажають глибокої прозорості та готові інвестувати в ширшу операційну модель Zero Trust. Платформа може бути потужною, але покупцям слід врахувати складність ліцензування, оперативний персонал та зусилля, необхідні для перетворення детальної аналітики пристроїв у політику підтримки.

Ключові можливості:

– Брандмауер наступного покоління на базі машинного навчання.

– Висока видимість програм і пристроїв.

– Профілювання пристроїв Інтернету речей та політика на основі поведінки.

– Сегментація Zero Trust за користувачами, програмами та пристроями.

– Інтеграція з ширшими робочими процесами Cortex та хмарної безпеки.

Sophos

Sophos орієнтований на організації, яким потрібен потужний брандмауер з простішим керуванням та тісною інтеграцією між мережею та безпекою кінцевих точок. Його лінійка брандмауерів XGS поєднує глибоку перевірку пакетів, запобігання вторгненням, контроль програм, веб-захист та можливості виявлення на базі штучного інтелекту.

Брандмауери Sophos на базі штучного інтелекту використовують штучний інтелект та машинне навчання для аналізу трафіку та файлів, а Sophos виділяє інтегроване виявлення та реагування в мережі. Для середовищ малого та середнього розміру з високим рівнем Інтернету речей це може допомогти виявити підозрілу поведінку некерованих пристроїв, які не можуть запускати програмне забезпечення для кінцевих точок.

Sophos особливо актуальний для шкіл, медичних закладів, виробників та багатосайтових компаній, яким потрібен централізований контроль без великої спеціалізованої команди брандмауерів. Синхронізована безпека також може

поєднувати контекст кінцевих точок та брандмауерів, хоча самі пристрої Інтернету речей залишаються без агентів і повинні контролюватися за допомогою мережевої політики.

Sophos – це ідеальний вибір, коли простота експлуатації важливіша за побудову максимально широкої архітектури корпоративної безпеки. Покупці повинні перевірити масштабованість, глибину класифікації пристроїв, вимоги до високої доступності та підтримку складних ОТ або дуже великих середовищ з кількома сайтами.

Ключові можливості:

– Виявлення загроз за допомогою штучного інтелекту та машинного навчання.

– Інтегроване виявлення та реагування на мережу.

– Централізоване управління хмарою.

– Зручність використання для середніх організацій.

– Координація між брандмауером та безпекою кінцевих точок.

Як вибрати брандмауер на базі штучного інтелекту для Інтернету речей

Почніть з видимості. Попросіть кожного постачальника ідентифікувати пристрої в репрезентативній мережі, не покладаючись виключно на існуючий інвентар. Тест має включати некеровані камери, датчики, шлюзи, принтери, системи будівлі та спеціалізовані операційні пристрої. Порівняйте точність класифікації, час виявлення та обсяг необхідного ручного виправлення.

Далі перевірте сегментацію. Створіть політики, які дозволять кожному пристрою групувати лише ті сервіси, які йому дійсно потрібні. Потужна платформа повинна забезпечити практичне розділення категорій пристроїв, сайтів та програм без створення тисяч крихких правил. Рекомендації щодо політик можуть бути корисними, але кожна рекомендація має бути пояснимою та такою, що підлягає перегляду.

Потім перевірте операційну поведінку. Виміряйте затримку, перевірку зашифрованого трафіку, перемикання на резервний архів, реєстрацію та

продуктивність управління за реального обсягу сеансів. У чутливих середовищах Інтернету речей та ОТ засіб контролю безпеки, який викликає нестабільність, може створювати стільки ж бізнес-ризиків, скільки й загроза, яку він має зупинити.

Зрештою, оцініть відповідність екосистемі. Брандмауери стають ефективнішими, коли вони спільно використовують контекст з інструментами ідентифікації, комутації, бездротового зв'язку, кінцевих точок, хмари та безпеки операцій. Найкращим вибором часто є платформа, яка зменшує сліпі зони та операційну передачу в середовищі, а не обов'язково та, що має найдовший список функцій.

Чому брандмауери на базі штучного інтелекту важливіші для Інтернету речей

Середовища Інтернету речей виявляють структурну слабкість традиційних моделей безпеки: багато пристроїв важко виправити, неможливо інструментально налаштувати, і очікується, що вони будуть постійно залишатися онлайн. Зловмисники можуть використовувати слабкі облікові дані, застаріле програмне забезпечення, вразливі сервіси або довірений доступ до мережі, а потім використовувати пристрій як плацдарм для горизонтального просування.

Аналіз на основі штучного інтелекту може допомогти виявити незвичайні схеми зв'язку, раніше невидимі загрози та відхилення політик у великих групах пристроїв. Однак брандмауер залишається точкою забезпечення дотримання правил. Ефективний захист все ще залежить від точної інвентаризації, сегментації з найменшими привілеями, безпечної конфігурації пристроїв та дисциплінованого управління змінами.

Для підприємств у 2026 році метою є не купувати термін «ШІ». Мета полягає у використанні ШІ там, де він покращує виявлення, пріоритезацію та операції, зберігаючи при цьому чіткі та тестовані засоби контролю над тим, як взаємодіють пристрої Інтернету речей.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Для реалізації програмного забезпечення системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів (файрволів) було обрано мову програмування Python. Вибір цього інструментарію зумовлений високою продуктивністю розробки, гнучкістю обробки структурованих даних, наявністю потужних бібліотек машинного навчання та можливістю ефективного аналізу великих масивів правил і логів безпеки.

Python є динамічною високорівневою інтерпретованою мовою програмування загального призначення з лаконічним і зрозумілим синтаксисом.

У контексті розробки систем аудиту безпеки мережевих екранів ключовими перевагами Python є:

– Розвинена екосистема для машинного навчання та аналізу даних: наявність спеціалізованих бібліотек (Scikit-learn, Pandas, NumPy) дозволяє ефективно реалізовувати алгоритми виявлення аномалій, класифікації конфігураційних помилок та прогнозування ризиків несанкціонованого доступу.

– Ефективність обробки текстових і мережевих даних: вбудовані структури даних та потужні інструменти роботи з рядками й регулярними виразами забезпечують швидкий парсинг правил фільтрації пакетів, таблиць маршрутизації та журналів подій (log-файлів).

– Гнучкість розширення: можливість інтеграції з модулями, написаними на низькорівневих мовах (C/C++), дозволяє оптимізувати виконання ресурсомістких обчислень при аналізі великих обсягів мережевого трафіку.

Завдяки своїй універсальності, надійній стандартній бібліотеці та кросплатформовості, Python забезпечує створення ефективного, масштабованого та гнучкого програмного середовища для автоматизованого виявлення вразливостей і аномалій у політиках безпеки розподілених мережевих екранів.

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 оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

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

У цьому розділі розглядаються найбільш актуальні та впливові внески, що складають основу запропонованої системи.

Системи прийняття рішень брандмауером на основі машинного навчання

У дослідженні, проведеному у 2021 році, було представлено систему машинного навчання з керуванням для автоматизації рішень щодо класифікації пакетів брандмауера [1]. До цієї роботи адміністраторам брандмауерів доводилося вручну визначати та підтримувати великі набори правил, що було як трудомістким, так і схильним до помилок. Запропонований підхід навчав моделі класифікації на позначених наборах даних мережевого трафіку, класифікуючи пакети за класами рішень «дозволити», «заборонити» або «відхилити».

У дослідженні оцінювалися три класичні алгоритми машинного навчання: дерева рішень, випадковий ліс та метод опорних векторів (SVM). Експериментальні результати показали, що класифікатор випадкового лісу досяг найвищої точності, значно перевершуючи традиційні системи на основі правил на еталонних наборах даних. Основним виявленим обмеженням була залежність від якості та репрезентативності маркованих навчальних даних, оскільки моделі, навчені на обмежених наборах даних, демонстрували знижену узагальненість на шаблони трафіку з різних мережевих середовищ.

Аналіз журналів брандмауера за допомогою глибокого навчання

Комплексне дослідження 2022 року розглядало проблему аналізу великомасштабних даних журналів брандмауера з використанням як класичних архітектур машинного навчання, так і глибокого навчання [2]. Дослідження було мотивоване спостереженням, що журнали брандмауера містять багату часову та контекстну інформацію, яку моделі поверхневого навчання не можуть повною

мірою використати. Набір даних включав кілька класів мережевої активності, що охоплюють нормальні операції, різні категорії атак та аномальні моделі поведінки.

Архітектури глибокого навчання, включаючи штучні нейронні мережі (ANN) та мережі довгої короткочасної пам'яті (LSTM), були застосовані як до необроблених векторів ознак, так і до часових послідовностей ознак, отриманих з даних журналів. Мережі LSTM продемонстрували особливу силу у фіксації послідовних залежностей у потоках трафіку, що дозволило виявляти багатоетапні шаблони атак, які розгортаються з часом. Цей підхід ефективно обробляв великомасштабні дані та успішно визначав складні моделі поведінки атак. Визнані обмеження включали високі вимоги до обчислювальних ресурсів та необхідність суттєвих розмічених навчальних наборів даних.

Порівняльне дослідження брандмауерів штучного інтелекту наступного покоління

У знаковому порівняльному дослідженні 2023 року систематично проаналізовано різноманітні архітектури брандмауерів на основі штучного інтелекту та оцінено їхню відносну продуктивність за допомогою комплексного набору показників, включаючи точність, прецизійність, повноту, F1-оцінку та коефіцієнт хибнопозитивних результатів [3]. У дослідженні розглянуто системи, починаючи від одномодельних класифікаторів і закінчуючи ансамблевими підходами та гібридними архітектурами, що поєднують кілька парадигм штучного інтелекту.

Порівняльний аналіз переконливо продемонстрував, що брандмауери на основі штучного інтелекту перевершують традиційні системи за всіма оцінюваними показниками, особливо для виявлення невідомих та поліморфних загроз. Дослідження також виявило, що ансамблеві методи, що поєднують кілька базових класифікаторів, послідовно досягають вищої точності, ніж підходи на основі однієї моделі. Ключова рекомендація полягала в тому, що майбутні системи повинні надавати пріоритет адаптивним архітектурам, здатним розвиватися разом із новими методологіями атак.

Високопродуктивні обчислення та хмарна безпека

У дослідженні, опублікованому в 2024 році, розглядалися підходи на основі штучного інтелекту до вдосконалення правил брандмауера в мережевих середовищах високопродуктивних обчислень (HPC) [4]. Мережі HPC створюють унікальні проблеми безпеки через свій масштаб, вимоги до продуктивності та чутливість даних, які вони обробляють. Запропонована система використовувала машинне навчання для автоматичного виявлення та усунення надлишкових або конфліктуючих правил брандмауера, зменшуючи складність бази правил, зберігаючи або покращуючи охоплення безпеки.

Окреме дослідження 2024 року було спеціально присвячене адаптивним брандмауерам на основі машинного навчання для безпеки хмарних технологій у реальному часі [5]. Хмарні середовища запроваджують динамічні зміни топології, еластичний розподіл ресурсів та багатокористувацьку оренду, що робить статичну безпеку на основі правил особливо неадекватною. Запропонований адаптивний брандмауер постійно оновлював свої моделі в міру надходження нових даних про трафік, демонструючи, що системи на основі штучного інтелекту можуть підтримувати високу точність виявлення навіть за умови швидкого розвитку захищеного мережевого середовища.

Навчання з підкріпленням та покращена безпека за допомогою LLM

Передові дослідження 2025 року досліджували архітектури брандмауерів на основі навчання з підкріпленням (RL), доповнені моделями великих мов (LLM) [7]. У цій парадигмі брандмауер моделюється як RL-агент, який вивчає оптимальні політики дозволу/блокування, отримуючи сигнали винагороди на основі точності своїх рішень. LLM використовуються для інтерпретації складних звітів про загрози та перетворення їх на дієві оновлення політик, що дозволяє брандмауеру включати якісні знання про загрози разом із кількісним аналізом трафіку.

Додаткова робота над динамічними брандмауерами на основі штучного інтелекту для зменшення загроз у реальному часі продемонструвала, що поєднання реактивних та проактивних компонентів штучного інтелекту дає

кращі результати порівняно з використанням будь-якого з цих підходів окремо [6]. Реактивний компонент негайно реагує на виявлені загрози, тоді як проактивний компонент постійно аналізує тенденції трафіку, щоб передбачити нові моделі атак до їх прояву.

Розпізнавання облич у системах безпеки

Розпізнавання облич на основі комп'ютерного зору широко вивчалося як компонент систем фізичної безпеки. Алгоритм Віоли-Джонса, реалізований у класифікаторі Haar Cascade від OpenCV [9], залишається фундаментальною методикою завдяки своїй обчислювальній ефективності та продуктивності в режимі реального часу. Сучасні підходи глибокого навчання, включаючи MTCNN та RetinaFace, досягають вищої точності, але з більшими обчислювальними витратами. Для інтеграції з інфраструктурою мережевої безпеки, де розпізнавання облич служить рівнем контролю доступу, підхід Haar Cascade забезпечує відповідний баланс точності та ефективності.

Моделі машинного навчання для виявлення вторгнень

Окрім досліджень, що стосуються лише брандмауерів, ширша галузь виявлення мережевих вторгнень дала відповідні результати. Набір даних NSL-KDD [11], отриманий з оригінального набору даних DARPA KDD Cup 1999, став стандартним еталоном для оцінки систем виявлення вторгнень. Набір даних CICIDS2017 [12] пропонує більш сучасний еталон, що включає сучасні типи атак, зокрема веб-атаки, інфільтрацію та трафік ботнетів. Набір даних UNSW-NB15 [13] пропонує комплексну колекцію, що охоплює дев'ять категорій атак за 49 мережевими функціями.

Дослідження, що застосовують ансамблеві методи до цих наборів даних, послідовно демонструють перевершувальну продуктивність порівняно з одномодельними підходами. Випадковий ліс [16] став особливо ефективним базовим класифікатором завдяки своїй стійкості до перенавчання та здатності обробляти багатовимірні простори ознак. Мережі LSTM [15] забезпечують додаткові можливості часового моделювання, фіксуючи послідовні шаблони атак, які розгортаються через кілька пакетів або сеансів. Поєднання цих підходів

за допомогою ансамбевого голосування, як запропоновано в даній магістерській роботі, використовує додаткові сильні сторони кожного типу моделі.

Прогалини в існуючій роботі

Незважаючи на значний прогрес у цих дослідницьких галузях, кілька критичних прогалин залишаються невирішеними:

По-перше, більшість існуючих систем розглядають безпеку на рівні мережі та контроль фізичного доступу як абсолютно окремі питання, що втрачає можливості для інтегрованого багаторівневого захисту.

По-друге, мало які системи забезпечують єдину архітектуру, яка одночасно враховує класифікацію відомих загроз, виявлення нульового дня за допомогою аналізу аномалій та безперервне адаптивне навчання в рамках однієї розгорнутої системи.

По-третє, поєднання біометричної автентифікації з поведінковим мережевим аналізом являє собою значною мірою недосліджений напрямок досліджень, якому присвячена дана магістерська робота.

По-четверте, в існуючій літературі рідко розглядаються операційні аспекти розгортання брандмауера штучного інтелекту, включаючи планування перенавчання моделей, моніторинг продуктивності та інтеграцію робочих процесів аналітиків. Розгорнута система безпеки, яка досягає високої точності контрольних показників, але накладає нестійкі операційні накладні витрати, має обмежену практичну цінність. Запропонований дизайн системи чітко вирішує ці операційні проблеми за допомогою автоматизованого безперервного навчання, управління сповіщеннями, орієнтованого на аналітиків, та панелей моніторингу продуктивності.

По-п'яте, відтворюваність отриманих результатів була обмежена непослідовними експериментальними методологіями та приватними наборами даних.

У даній роботі використовуються загальнодоступні набори даних для контрольних показників та повідомляється про комплексні показники оцінки для забезпечення відтворюваності.

3.2 Розробка структурної схеми

Поточні розгортання мережевої безпеки переважно спираються на традиційні архітектури брандмауерів, що базуються на фільтрації пакетів, перевірці стану та виявленні вторгнень на основі сигнатур. Ці системи працюють, підтримуючи таблиці правил, які визначають, які пакети слід дозволяти, забороняти або реєструвати на основі критеріїв, включаючи IP-адреси джерела та призначення, номери портів, типи протоколів та відомі сигнатури шкідливого корисного навантаження.

Хоча традиційні брандмауери ефективні проти відомих та каталогізованих загроз, вони демонструють фундаментальні архітектурні обмеження, які значно знижують їхню ефективність у сучасних середовищах загроз. Бази даних сигнатур потребують постійного ручного оновлення, щоб залишатися актуальними, створюючи вікна вразливості між появою нових загроз та розгортанням відповідних сигнатур. Статичні набори правил не можуть адаптуватися до змін поведінки в захищеній мережі, що призводить як до надмірної кількості хибнопозитивних результатів, які блокують легітимний трафік, так і до хибнонегативних результатів, які дозволяють шкідливому трафіку проходити непоміченим.

Брандмауери наступного покоління (NGFW) являють собою поступове вдосконалення, включаючи перевірку на рівні додатків, розшифрування SSL та обмежені можливості виявлення аномалій. Однак навіть NGFW фундаментально залежать від попередньо визначених сигнатур та політик, не маючи можливості навчатися на поведінці мережі та виявляти справді нові моделі атак без постійного втручання адміністратора.

Робота, виконана в існуючих системах

Попередні дослідження з великим успіхом стосувалися конкретних аспектів розробки інтелектуальних брандмауерів. Класифікатори машинного навчання застосовувалися до мережевих даних на рівні пакетів та потоків, демонструючи, що автоматизована класифікація може зрівнятися або

перевершити підходи на основі правил, налаштовані людиною, для відомих категорій трафіку. Моделі глибокого навчання, зокрема LSTM та згорткові нейронні мережі, продемонстрували високу продуктивність на наборах даних для виявлення мережевих вторгнень, включаючи NSL-KDD, CICIDS2017 та UNSW-NB15.

Дослідження виявлення аномалій продемонстрували, що статистичні моделі нормальної поведінки мережі можуть бути створені та використані для позначення відхилень, які можуть свідчити про атаки. Такі методи, як ізоляційні ліси, автокодери та однокласова SVM, були успішно застосовані для виявлення аномалій мережевого трафіку. Навчання з підкріпленням було застосовано для оптимізації політики брандмауера, коли агенти навчаються балансувати цілі безпеки та продуктивності через взаємодію з мережевими симуляторами.

Проблеми в існуючій системі

Існуючі системи демонструють кілька критичних обмежень, що мотивують запропоновану роботу. Погане узагальнення є найсуттєвішою проблемою: моделі, навчені на певних наборах даних для порівняння, часто дають збій при розгортанні у виробничих середовищах з різними характеристиками трафіку. Високі обчислювальні вимоги обмежують розгортання складних моделей глибокого навчання в середовищах з обмеженими ресурсами. Більшість існуючих систем аналізують лише одну модальність даних безпеки, не отримуючи додаткової інформації, доступної в результаті поєднання даних мережевого та фізичного контролю доступу.

Відсутність механізмів безперервного навчання означає, що розгорнуті моделі поступово застарівають у міру розвитку мережевих середовищ та методологій атак. Ручне перенавчання є трудомістким та дорогим, створюючи прогалини в безпеці під час циклів оновлення. Крім того, більшість систем забезпечують обмежену інтерпретацію, видаючи результати класифікації без пояснень конкретних характеристик, які сприяли прийняттю кожного рішення, що ускладнює процеси перевірки та аудиту аналітиками безпеки.

Запропоноване рішення

Запропонований інтелектуальний брандмауер на основі штучного інтелекту вирішує ці обмеження за допомогою багатопарадигмальної архітектури, яка поєднує навчання з учителем для виявлення відомих загроз, виявлення аномалій без учителя для ідентифікації загроз нульового дня, навчання з підкріпленням для адаптивної оптимізації політик та розпізнавання облич на основі комп'ютерного зору для контролю фізичного доступу. Система реалізує безперервне онлайн-навчання, яке автоматично включає нові виявлені загрози в оновлені моделі без необхідності ручного перенавчання. Модульна конструкція гарантує, що окремі компоненти можна оновлювати незалежно, коли стають доступними вдосконалені алгоритми.

Запропонована система

Запропонований інтелектуальний брандмауер на основі штучного інтелекту – це комплексна багаторівнева платформа мережевої безпеки, яка інтегрує технології штучного інтелекту, машинного навчання, глибокого навчання та комп'ютерного зору в єдину, розгортану систему. Архітектура спеціально розроблена для подолання фундаментальних обмежень традиційних брандмауерів на основі правил, забезпечуючи автоматизовані, адаптивні та інтелектуальні можливості виявлення та реагування на загрози.

Система побудована навколо центрального механізму штучного інтелекту, який безперервно оцінює мережевий трафік за допомогою ансамблевих моделей, навчених на різноманітних наборах даних, що представляють нормальну поведінку та різні категорії атак. Це ядро оточують спеціалізовані модулі для збору даних, попередньої обробки, встановлення базової поведінки, класифікації загроз, автоматизованого реагування, біометричного контролю доступу та безперервного навчання. Усі модулі взаємодіють через стандартизований внутрішній API, що дозволяє здійснювати незалежну розробку та оновлення кожного компонента.

Огляд архітектури системи

Повна архітектура системи складається з восьми основних компонентів, організованих у три функціональні рівні. Рівень даних охоплює модуль збору даних та модуль попередньої обробки, які разом збирають, нормалізують та готують дані мережевого трафіку для аналізу. Рівень інтелектуального аналізу містить підсистему навчання моделі штучного інтелекту,

Механізм базової поведінки, модуль виявлення та класифікації загроз і модуль розпізнавання облич. Рівень реагування включає модуль автоматизованого реагування та систему безперервного навчання зі зворотним зв'язком.

Мережевий трафік надходить у систему через рівень даних, де він фіксується на рівні мережевого інтерфейсу за допомогою бібліотек захоплення пакетів, нормалізується у стандартизовані вектори ознак та пересилається на рівень інтелектуального аналізу. Механізм виведення на основі штучного інтелекту оцінює кожен потік трафіку та створює мітку класифікації з відповідним показником достовірності. Якщо показник достовірності перевищує поріг класифікації зловмисника, запускається модуль автоматизованого реагування для виконання відповідних контрзаходів.

Парадигми навчання штучного інтелекту

Система використовує три взаємодоповнюючі парадигми машинного навчання, які разом забезпечують комплексне охоплення проблеми виявлення загроз. Навчання з учителем працює на маркованих наборах даних, що містять приклади як звичайного мережевого трафіку, так і специфічних категорій атак. Моделі класифікації, навчені за допомогою цього підходу, вивчають розпізнавальні ознаки, які відрізняють шкідливий трафік від доброякісного, і можуть класифікувати новий трафік з високою точністю, коли він нагадує раніше виявлені шаблони.

Неконтрольоване виявлення аномалій вирішує проблему виявлення нульового дня, вивчаючи статистичну модель нормальної поведінки мережі без необхідності позначених прикладів атак. Система постійно оновлює цю модель

у міру спостереження нового нормального трафіку, підтримуючи точне відображення очікуваної поведінки. Трафік, який суттєво відхиляється від цього вивченого нормального профілю, позначається як аномальний, незалежно від того, чи відповідає він будь-якій відомій сигнатурі атаки. Ця можливість є критично важливою для виявлення нових варіантів атак, які раніше ніколи не спостерігалися.

Навчання з підкріпленням забезпечує рівень оптимізації політик, навчаючи агента приймати оптимальні рішення щодо дозволу/блокування в контексті поточного мережевого середовища. RL-агент отримує сигнали винагороди на основі точності своїх рішень – позитивні винагороди за правильні класифікації та негативні винагороди як за хибнопозитивні, так і за хибнонегативні результати – і поступово вивчає політики, які максимізують загальну безпеку, мінімізуючи законні перебої в трафіку.

Механізм поведінкового аналізу

Механізм поведінкового аналізу встановлює та підтримує базові профілі нормальної поведінки мережі з кількома рівнями деталізації: для кожного користувача, для кожного пристрою, для кожної програми та для кожної підмережі. Ці профілі фіксують статистичні характеристики звичайних моделей трафіку, включаючи типові обсяги передачі даних, поширених партнерів зв'язку, звичайні години активності, характерні розподіли протоколів та очікувану тривалість сеансів. Відхилення від встановлених базових рівнів запускають сповіщення, які пересилаються до механізму класифікації для більш детального аналізу.

Базовий механізм використовує експоненціально зважені ковзні середні для підтримки профілів, які поступово адаптуються до законних змін у поведінці мережі, залишаючись чутливими до раптових аномальних відхилень. Окремі пороги підтримуються для різних типів поведінкових показників, з більш чутливими порогами для поведінки з високим рівнем ризику, такої як активність привілейованих облікових записів та доступ до конфіденційних сховищ даних.

Розпізнавання облич та біометричний контроль доступу

Біометричний рівень контролю доступу використовує каскадний класифікатор Хаара від OpenCV для виконання розпізнавання облич у режимі реального часу на фізичних точках доступу до мережевої інфраструктури. Цей модуль взаємодіє з камерами безпеки, розташованими біля входів до серверних кімнат, точок доступу до центрів мережевих операцій та критично важливих місць розташування обладнання. Коли персонал наближається до цих зон, система розпізнавання облич ідентифікує та реєструє виявлені обличчя, зіставляючи їх з базою даних авторизованого персоналу.

Для цього застосування обрано підхід Каскаду Хаара завдяки його чудовому балансу точності виявлення та обчислювальної ефективності. Класифікатор застосовує алгоритм Віоли-Джонса, використовуючи каскад дедалі складніших оцінювачів ознак, що дозволяє швидко відкидати області зображення, що не належать до обличчя, та ефективно фокусуватися на розташуваннях облич-кандидатів. Цей підхід забезпечує продуктивність у режимі реального часу на стандартному обладнанні, що є критично важливою вимогою для системи контролю доступу, яка не повинна перешкоджати роботі уповноваженого персоналу.

Реалізація

Технологічний стек

Реалізація системи використовує Python 3.10 як основну мову програмування, використовуючи його розгалужену екосистему бібліотек машинного навчання, комп'ютерного зору та мережевого аналізу. Конвеєр машинного навчання використовує scikitlearn для класичних алгоритмів, включаючи випадковий ліс, метод опорних векторів та ізоляційний ліс. Компоненти глибокого навчання реалізовані за допомогою TensorFlow 2.x та Keras, що забезпечує доступ до мереж LSTM та згорткових архітектур. Модуль навчання з підкріпленням використовує Stable Baselines3, побудований на PyTorch.

Для захоплення та аналізу мережевого трафіку використовується Scapy для операцій на рівні пакетів та PyShark для аналізу потоків вищого рівня.

Вилучення ознак із необроблених пакетів виконується за допомогою спеціального конвеєра, який обчислює 41 статистичну ознаку для кожного мережевого потоку, сумісного з форматом набору даних NSL-KDD для полегшення порівняння з опублікованими результатами. Модуль розпізнавання облич використовує OpenCV 4.8.x з попередньо навченою моделлю haarcascade_frontalface_default.xml. Панель керування реалізована як веб-застосунок Flask з фронтендом React.js, що забезпечує візуалізацію мережевого трафіку, сповіщень про загрози та показників продуктивності системи в режимі реального часу.

Збір та попередня обробка даних

Модуль збору даних фіксує мережевий трафік на рівні інтерфейсу за допомогою захоплення пакетів на основі libpcap. Пакети обробляються в режимі реального часу з використанням методу ковзного вікна, при цьому характеристики рівня потоку обчислюються для кожного двонаправленого мережевого сеансу. Конвеєр видобування ознак обчислює 41 ознаку для кожного потоку, включаючи тривалість, тип протоколу, тип служби, прапорець, байти джерела та призначення, землю, неправильний фрагмент, терміновий, гарячий, невдалі входи, стан входу в систему, кількість скомпрометованих подій, доступ до кореневої оболонки, спроби su, кількість root-доступів, кількість створених файлів, кількість оболонок, кількість файлів доступу, кількість вихідних команд, вхід до хоста, вхід до гостя, кількість, кількість srv, коефіцієнт помилок, коефіцієнт помилок srv, коефіцієнт помилок srv, коефіцієнт помилок srv, той самий коефіцієнт srv, коефіцієнт різниці srv, коефіцієнт різниці хостів, кількість хостів призначення, кількість srv хостів призначення, той самий коефіцієнт srv хоста призначення, коефіцієнт різниці srv хоста призначення, коефіцієнт порту src хоста призначення, коефіцієнт srv хоста призначення, коефіцієнт помилок хоста призначення, коефіцієнт помилок srv хоста призначення, коефіцієнт помилок хоста призначення та коефіцієнт помилок srv хоста призначення.

Попередня обробка застосовує нормалізацію z-оцінки до безперервних ознак та одноразове кодування до категоріальних ознак, включаючи тип протоколу, сервіс та прапорець. Дисбаланс класів між зразками нормального та шкідливого трафіку вирішується за допомогою SMOTE (техніка синтетичної меншості надмірної вибірки) для навчального набору даних. Ознаки з майже нульовою дисперсією в навчальному наборі видаляються для зменшення розмірності та підвищення ефективності навчання моделі.

Реалізація розпізнавання облич

Модуль розпізнавання облич ініціалізує каскадний класифікатор Хаара, завантажуючи попередньо скомпільовану модель фронтального обличчя OpenCV: face_cascade = cv2.CascadeClassifier(cv2.data.haarcascades + 'haarcascade_frontalface_default.xml'). Вхідні зображення отримуються з USB- або IP-камер безпеки зі швидкістю 30 кадрів на секунду. Кожен кадр спочатку перевіряється на успішне захоплення, а потім перетворюється з колірного простору BGR, що використовується OpenCV, у градації сірого за допомогою cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY). Перетворення у градації сірого зменшує вхідні дані до одного каналу, видаляючи інформацію про колір, яка не потрібна для розпізнавання обличчя, та підвищуючи швидкість обробки.

Розпізнавання облич виконується за допомогою функції detectMultiScale(), яка застосовує класифікатор у кількох масштабах зображення для виявлення облич різного розміру. Функція налаштована з коефіцієнтом масштабування 1,1, що призводить до збільшення розміру вікна виявлення на 10% на кожному кроці масштабування. Параметр minNeighbors встановлено на 5, що вимагає, щоб п'ять сусідніх вікон виявлення погодилися щодо наявності обличчя, перш ніж виявлення буде підтверджено, що ефективно усуває хибнопозитивні результати. Мінімальний розмір виявлення 30x30 пікселів виключає дуже маленькі області, які навряд чи представляють реальні обличчя.

Для кожного виявленого обличчя модуль малює прямокутну обмежувальну рамку за допомогою cv2.rectangle() з фіолетовим кольором (255, 0, 255) та товщиною лінії 2 пікселі. Виявлені області обличчя обрізаються,

змінюються на розмір до стандартного формату 128x128 пікселів та передаються до модуля розпізнавання облич для перевірки особи в базі даних авторизованого персоналу. Рішення щодо контролю доступу реєструються з позначкою часу, місцезнаходженням камери, виявленим зображенням обличчя та результатом розпізнавання.

Навчання моделей машинного навчання

Модель контрольованої класифікації використовує ансамбль випадкового лісу з 200 дерев рішень, кожне з яких навчається на випадковій підмножині навчальних вибірок та ознак. Випадковий ліс обрано як основний класифікатор через його стійкість до перенавчання, здатність обробляти багатовимірні простори ознак та вбудовану підтримку оцінки важливості ознак. Модель навчається на об'єднаному наборі даних, отриманому з NSL-KDD, CICIDS2017 та UNSW-NB15, що включає різноманітні типи трафіку та категорії атак.

Компонент глибокого навчання LSTM обробляє послідовні дані трафіку для фіксації часових шаблонів атак. Архітектура мережі складається з двох шарів LSTM зі 128 та 64 одиницями відповідно, за якими йдуть два повністю зв'язані шари з активацією ReLU та вихідний шар softmax для класифікації загроз для кількох класів. Шари відсіву з коефіцієнтом 0,3 застосовуються після кожного шару LSTM для запобігання перенавчанню. Модель навчається за допомогою оптимізатора Adam з початковим коефіцієнтом навчання 0,001 та розміром пакету 256 протягом 50 епох.

Компонент виявлення аномалій використовує Ізоляційний ліс із 200 дерев, навчених виключно на звичайних зразках трафіку. Параметр забруднення встановлено на 0,05, що вказує на очікуваний рівень аномалій 5% у тестових даних. Ця модель позначає зразки трафіку, які ізольовані випадковим лісом у меншій кількості розщеплень, ніж типові звичайні зразки, що вказує на те, що вони займають області з низькою щільністю простору ознак, характерних для аномальної поведінки.

Інтеграція та голосування ансамблю

Трикомпонентні моделі – класифікатор випадкового лісу, класифікатор LSTM та детектор аномалій ізоляційного лісу – інтегровані за допомогою механізму зваженого голосування. Для кожного зразка трафіку кожна модель створює мітку класифікації загрози та коефіцієнт достовірності. Моделі випадкового лісу та LSTM вносять 40% ваги в остаточне рішення, тоді як детектор аномалій ізоляційного лісу вносить 20%. Ця вага відображає вищу точність класифікації моделей під наглядом, зберігаючи при цьому внесок детектора аномалій у виявлення нульового дня.

Остаточне рішення щодо класифікації приймається шляхом обчислення зваженої суми балів достовірності для кожного класу за всіма трьома моделями. Якщо зважений бал достовірності зловмисності перевищує 0,5, трафік класифікується як зловмисний; якщо він падає нижче 0,3, трафік класифікується як легітимний; значення від 0,3 до 0,5 запускають підозрілу класифікацію, яка спрямовує трафік до середовища honeypot для подальшого аналізу, дозволяючи при цьому продовжувати початковий сеанс під посиленим моніторингом.

До вихідних балів необробленої моделі застосовується етап пост-обробки калібрування з використанням масштабування Платта [10], перетворюючи некалібровані оцінки ймовірності на добре калібровані значення достовірності. Добре калібровані показники достовірності є важливими для багаторівневої системи реагування, яка залежить від порогів достовірності для вибору відповідних рівнів реагування. Калібрування виконується з використанням витриманого набору даних для перевірки та оновлюється під час кожного циклу перенавчання.

Оптимізація політики навчання з підкріпленням

Компонент навчання з підкріпленням моделює рішення брандмауера про дозвіл/блокування як процес прийняття рішень Маркова (MDP). Простір станів відображає поточні умови мережі, включаючи останній обсяг трафіку, кількість активних з'єднань, частоту виявлених загроз та характеристики часу доби. Простір дій включає чотири окремі дії: дозвіл, блокування, обмеження

швидкості та перенаправлення на приманку. Функція винагороди призначає позитивні винагороди за правильну класифікацію загроз та правильний дозвіл легітимного трафіку, а також негативні винагороди за хибнопозитивні результати, які порушують роботу легітимних користувачів, та хибнонегативні результати, які дозволяють продовжувати атаки.

Агент RL навчається за допомогою Proximal Policy.

Оптимізація (PPO) – алгоритм градієнта політики, який забезпечує стабільне навчання за допомогою обмежених оновлень політики. Навчання проводиться в середовищі мережевого моделювання з використанням записаних трас трафіку, що дозволяє ретельно дослідити простір дій без впливу на робочу мережу. Навчена політика потім розгортається як додатковий рівень прийняття рішень, який може замінити або доповнити рекомендації класифікатора ансамблю, коли умови мережі вказують на необхідність коригування порогових значень.

Автоматизована система реагування

Модуль автоматизованого реагування реалізує багаторівневу політику реагування на основі рівня серйозності загрози, пов’язаного з кожним виявленим типом загрози. Реакції 1-го рівня, що застосовуються до класифікацій підозрілого трафіку, включають розширене ведення журналу, обмеження швидкості з’єднань та сповіщення аналітиків безпеки. Реакції 2-го рівня, що застосовуються до підтверджених класифікацій шкідливого трафіку з помірною впевненістю, включають негайне блокування з’єднання, додавання вихідної IP-адреси до тимчасового списку блокування, дійсного протягом 24 годин, та генерацію сповіщень у режимі реального часу. Реакції 3-го рівня, що застосовуються до класифікацій шкідливого трафіку з високою впевненістю, що включають критичні типи атак, такі як DDoS, ескалація привілеїв або витік даних, включають повне блокування вихідної підмережі, ізоляцію уражених кінцевих пристроїв, екстрене сповіщення старшого персоналу безпеки та автоматичне створення звітів про інциденти.

Дії реагування реалізуються шляхом інтеграції з API мережевої інфраструктури. Для керованих комутаторів та маршрутизаторів, що підтримують API NETCONF або REST, система безпосередньо програмує записи списку контролю доступу для блокування шкідливого трафіку на межі мережі. Для середовищ без програмованої мережевої інфраструктури дії реагування застосовуються за допомогою правил iptables, що застосовуються на хості брандмауера. Усі дії реагування реєструються з повною контекстною інформацією та можуть бути переглянуті, змінені або скасовані через панель керування.

Опис модуля

Модуль введення даних

Модуль введення даних слугує основним інтерфейсом між живим мережевим середовищем та аналітичним конвеєром системи безпеки. Модуль працює на рівні мережевого інтерфейсу, фіксуючи весь вхідний, вихідний та внутрішній трафік, що проходить через контрольовані сегменти мережі. Він підтримує кілька режимів захоплення, включаючи змішаний режим для повного огляду трафіку, інтеграцію дзеркалювання портів для розгортання на керованих мережевих комутаторах та вбудований режим для активної перевірки та блокування трафіку.

Модуль реалізує агрегацію трафіку на основі потоку, об'єднуючи окремі пакети, що належать до одного мережевого сеансу, в єдині записи потоку. Записи потоку зберігаються в хеш-таблиці, індексованій за п'ятикортежем: вихідна IP-адреса, вихідна IP-адреса призначення, вихідний порт, порт призначення та протокол, з параметрами тайм-ауту простою та активного тайм-ауту, що контролюють закінчення терміну дії потоку. Завершені записи потоку пересилаються до конвеєра попередньої обробки для вилучення ознак.

Модуль попередньої обробки

Модуль попередньої обробки перетворює необроблені записи потоку на нормалізовані вектори ознак, придатні для введення в моделі класифікації ШІ. Модуль застосовує повний конвеєр вилучення ознак 41, описаний у розділі VB,

обчислюючи статистичні агрегації вимірювань на рівні пакетів для кожного потоку. Нормалізація ознак за допомогою стандартизації zscore застосовується з використанням статистики, обчисленої з навчального набору даних, що гарантує узгодженість параметрів нормалізації між навчанням та висновком.

Модуль попередньої обробки також реалізує кешування ознак для потоків, що надходять кількома пакетами, зберігаючи часткові вектори ознак для активних потоків та завершуючи їх після закінчення терміну дії потоків. Такий підхід дозволяє системі проводити попередні оцінки загроз на основі даних часткового потоку, що підтримує раннє виявлення атак, які мають шкідливі характеристики в початкових пакетах сеансу.

Модуль моніторингу трафіку

Модуль моніторингу трафіку забезпечує перегляд моделей мережевого трафіку та продуктивності системи в режимі реального часу через веб-інтерфейс панелі керування. Модуль агрегує статистику трафіку через налаштовувані інтервали часу, створюючи часові ряди даних, які візуалізуються за допомогою інтерактивних діаграм, що показують обсяг трафіку за протоколом, найбільш поширених промовців за споживанням пропускної здатності, географічний розподіл зовнішніх підключень та частоту виявлення загроз.

Функція керування сповіщеннями дозволяє аналітикам безпеки переглядати, підтверджувати, ескалювати та вирішувати виявлені загрози. Кожне сповіщення містить вичерпну контекстуальну інформацію, зокрема деталі потоку трафіку, конкретні характеристики моделі, які вплинули на рішення про класифікацію, оцінку достовірності кожного компонента моделі та вжиті автоматизовані дії реагування. Аналітики можуть ігнорувати автоматизовані рішення реагування та надавати зворотний зв'язок, який враховується в системі безперервного навчання.

Модуль класифікації загроз

Модуль класифікації загроз реалізує конвеєр ансамблю логічного виводу, описаний у розділі VE, застосовуючи навчені моделі випадкового лісу, LSTM та ізоляційного лісу до кожного обробленого запису потоку. Модуль оптимізовано

для логічного виводу з низькою затримкою, орієнтуючись на затримку класифікації менше 50 мілісекунд на потік для підтримки аналізу трафіку в режимі реального часу на швидкості лінії.

Багатокласова класифікація підтримує 23 різні категорії загроз, включаючи «Звичайний», варіанти DoS (DoS slowhttptest, DoS Hulk, DoS GoldenEye, DoS Slowloris) та варіанти DDoS (DDoS HOIC, DDoS LOIC-HTTP, DDoS LOIC-UDP), варіанти сканування портів, груба сила (FTP-Patator, SSH-Patator), веб-атаки (XSS, SQL-ін'єкції, груба сила), інфільтрація, ботнет та Heartbleed. Дрібнозерниста багатокласова класифікація забезпечує більш цілеспрямовані та відповідні автоматизовані відповіді порівняно з бінарною класифікацією шкідливих/доброякісних атак.

Модуль безперервного навчання

Модуль безперервного навчання реалізує онлайн-конвеєр навчання, який періодично перенавчає моделі класифікації, використовуючи нові накопичені дані про трафік. Конвеєр перенавчання працює за розкладом, зазвичай кожні 24 години в періоди низького трафіку, включаючи підтверджені класифікації загроз з огляду аналітиків та нові зразки звичайного трафіку з поточного операційного середовища.

Методи активного навчання використовуються для визначення пріоритетів вибірок даних для розгляду аналітиками, зосереджуючись на вибірках поблизу меж рішень щодо класифікації, де зворотний зв'язок аналітиків забезпечує найбільше покращення точності моделі. Вибірки з високою невизначеністю – ті, де моделі ансамблю суттєво розходяться – позначаються як такі, що мають високий пріоритет для розгляду. Система моніторингу ефективності моделі постійно відстежує точність класифікації, рівень хибнопозитивних та рівень хибнонегативних результатів на затриманому наборі даних для перевірки, запускаючи сповіщення, якщо показники ефективності знижуються нижче визначених порогових значень.

Модуль управління сповіщеннями та звітності

Модуль керування сповіщеннями забезпечує структурований робочий процес для аналізу виявлених загроз аналітиками безпеки. Сповіщенням присвоюється пріоритетність за допомогою багатофакторної системи оцінювання, яка враховує серйозність загрози, оцінку достовірності, критичність активів цільового мережевого ресурсу та час з моменту останнього подібного сповіщення. Сповіщення з високим пріоритетом відображаються негайно через push-сповіщення, тоді як сповіщення з нижчим пріоритетом ставляться в чергу для періодичного перегляду.

Кожен запис сповіщення містить вичерпну контекстну інформацію: повний ідентифікатор потоку з п'яти кортежів, усі 41 витягнуті ознаки потоку, окремі оцінки достовірності моделі з кожного компонента ансамблю, конкретні ознаки, які найбільше сприяли прийняттю рішення про класифікацію (обчислені за допомогою значень SHAP для інтерпретації), автоматизовані дії реагування та посилання на відповідні звіти про розвідку загроз. Цей контекст дозволяє аналітикам приймати обґрунтовані рішення щодо того, чи приймати, ігнорувати або ескалювати відповідь системи.

Модуль звітності генерує заплановані та на вимогу звіти про безпеку, включаючи короткий виклад обсягів та категорій виявлених загроз, аналіз тенденцій, що порівнює поточні моделі загроз з історичними базовими показниками, відстеження рівня хибнопозитивних та хибнонегативних результатів з плином часу, а також показники продуктивності системи, включаючи затримку класифікації та пропускну здатність. Звіти генеруються у форматах PDF та HTML і можуть бути автоматично розповсюджені зацікавленим сторонам електронною поштою.

Модуль біометричної інтеграції

Модуль біометричної інтеграції керує інтерфейсом між системою розпізнавання облич OpenCV та ширшою платформою безпеки. Коли модуль розпізнавання облич ідентифікує особу в контрольованій точці доступу, модуль біометричної інтеграції виконує пошук ідентифікаційних даних у базі даних

авторизованого персоналу, порівнює позначку часу виявлення з графіками доступу, оцінює, чи дозволяє рівень доступу виявленої особи вхід до певного місця, та реєструє подію доступу із зображенням обличчя, впевненістю розпізнавання та рішенням про доступ.

Інтеграція з компонентами мережевої безпеки дозволяє здійснювати кореляційний аналіз подій фізичного та логічного доступу. Незвичайні комбінації фізичного та логічного доступу, такі як використання мережевих облікових даних користувача, коли фізична присутність цього користувача не може бути підтверджена на відповідній робочій станції, викликають підвищені сповіщення безпеки, які можуть свідчити про крадіжку облікових даних або компрометацію облікового запису. Така міжмодальна кореляція є значною перевагою можливостей порівняно з традиційними одномодальними системами безпеки.

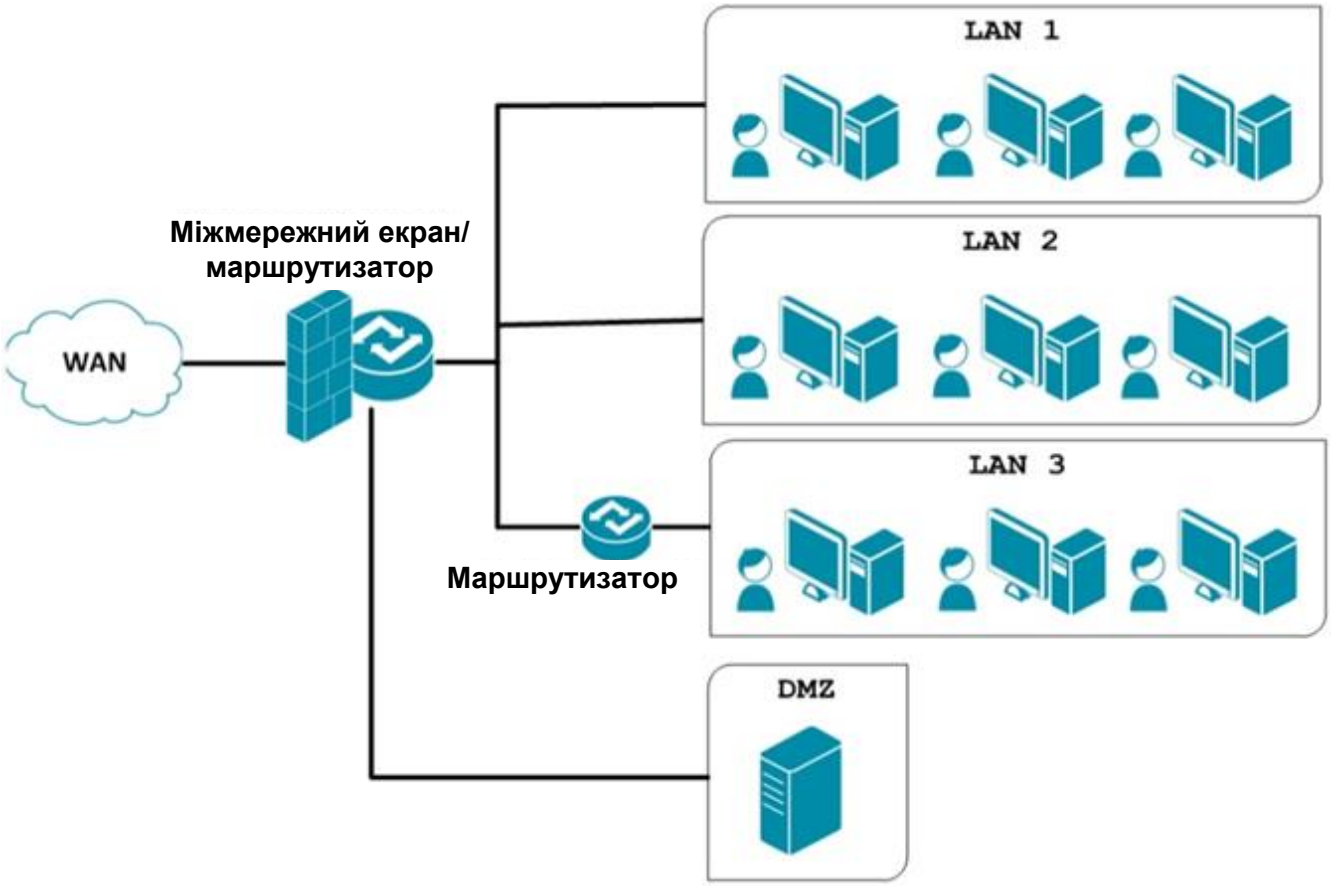

Рисунок 3.1 – Структурна схема системи

Структурна схема розробленої системи зображена на рисунку 3.1. Зовнішній інтернет-трафік проходить крізь міжмережевий екран (фаєрвол) і спрямовується або до захищеного внутрішнього сегмента мережі, або до демілітаризованої зони (DMZ). Будь-який трафік між внутрішніми системами та вузлами в DMZ також контролюється брандмауером згідно із заданими правилами безпеки. Більшість мереж мають ієрархічну структуру: єдиний вхідний канал ззовні розгалужується на кілька внутрішніх гілок. Найефективніше встановлювати міжмережевий екран саме в точці такого розгалуження – це відразу знімає питання про те, де «зовнішній», а де «внутрішній» периметр. Проте іноді фаєрволи розміщують і всередині мережі – наприклад, щоб ізолювати одну групу комп'ютерів від іншої.

Якщо ж мережа не має чіткої ієрархії, єдині політики безпеки мають застосовуватися до абсолютно всіх точок доступу. Поширена помилка – встановити захист лише на головному вході й забути про інші, через що зловмисний трафік може легко обійти блокування та проникнути в мережу альтернативними шляхами.

3.3 Розробка функціональної схеми

На рисунку 3.2 наведено функціональну схему розробленої системи. Сучасні пристрої домашніх та корпоративних мереж, зокрема інтегровані маршрутизатори, зазвичай містять багатофункціональні програмні міжмережні екрани (Firewalls). Такі рішення реалізують трансляцію мережевих адрес (NAT), динамічний інспекційний аналіз пакетів (SPI), а також фільтрацію трафіку за IP-адресами, прикладними протоколами та вебдолученнями, додатково підтримуючи механізми демілітаризованої зони (DMZ).

Конфігурація та обмеження DMZ

Інтегрований маршрутизатор дає змогу налаштовувати примітивну DMZ для забезпечення доступу до внутрішнього сервера із зовнішніх мережевих вузлів. Для цього захищений сервер повинен мати статичну IP-адресу, яка

вказується в параметрах конфігурації. Мережевий пристрій ізолює трафік, спрямовуючи його виключно на зазначений порт комутатора, до якого підключено сервер, тоді як на інші вузли поширюються стандартні правила фільтрації міжмережевого екрана.

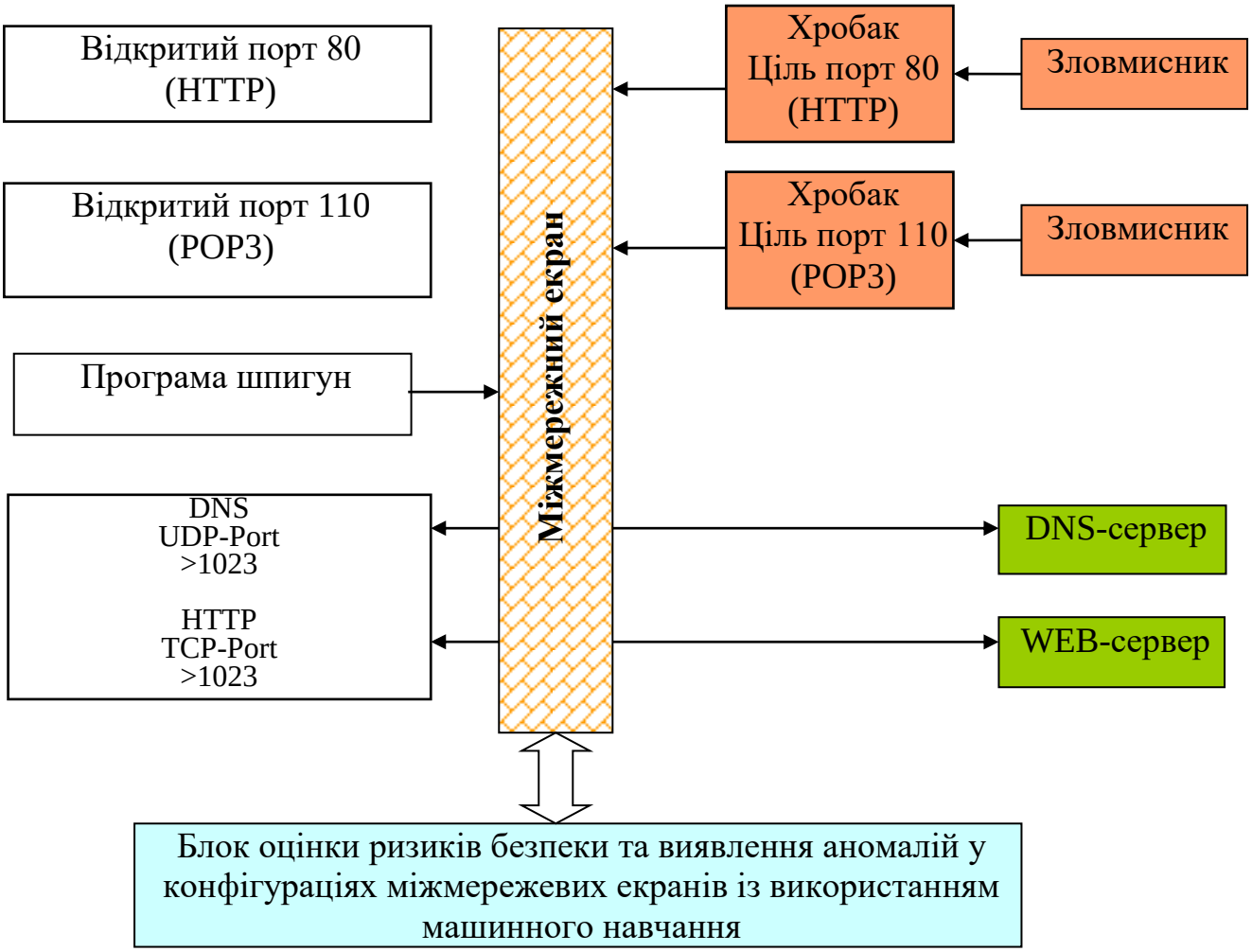

Рисунок 3.2 – Функціональна схема системи

У найпростішому режимі активації DMZ зовнішні користувачі отримують потенційний доступ до всіх портів сервера (наприклад, 80 для HTTP, 21 для FTP, 110 для POP3). З метою підвищення рівня безпеки застосовується функція переадресації портів (Port Forwarding), що дозволяє реалізувати більш жорстку конфігурацію: трафік пропускається виключно через чітко визначені порти, тоді як усі інші запити блокуються.

Ризики безпеки бездротових точок доступу

Особливу увагу в контексті аналізу ризиків слід приділяти бездротовим точкам доступу, які входять до складу інтегрованих маршрутизаторів і розглядаються як частина внутрішньої мережі. Робота точки доступу в незахищеному режимі створює критичну вразливість: неавторизовані користувачі отримують прямий доступ до захищеного внутрішнього сегмента мережі, минаючи рівні перевірки міжмережевого екрана, що створює передумови для реалізації атак та несанкціонованого перехоплення даних.

Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

Діаграма процесів розробленої системи зображена на рисунку 3.3. При детальному її розгляді можна побачити як саме проходе взаємодія у розробленій системі.

Діаграми взаємодії процесів застосовуються для наочної візуалізації процедур обробки даних у межах структурного проєктування інформаційних систем. Традиційний підхід до розробки програмних комплексів передбачає першочергову побудову контекстної діаграми потоків даних, яка ілюструє загальну взаємодію розроблюваної системи оцінки ризиків безпеки та виявлення аномалій із зовнішнім середовищем (мережевими адміністраторами, джерелами логів трафіку, міжмережевими екранами та зовнішніми базами вразливостей). У подальшому ця концептуальна модель підлягає послідовній декомпозиції шляхом деталізації окремих процесів і потоків даних з метою повного та всебічного відображення архітектури комплексу, що створюється.

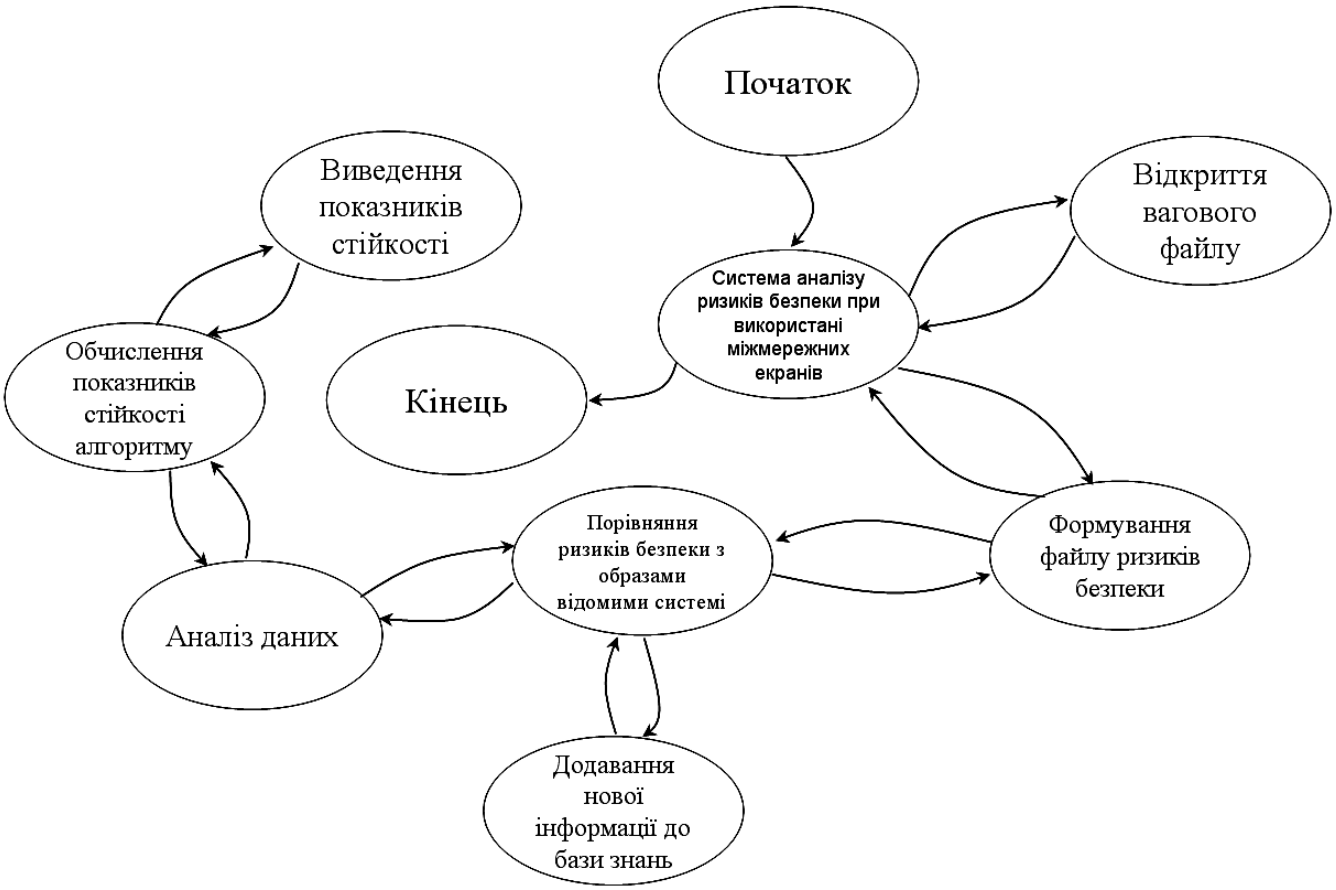

Рисунок 3.3 – Діаграма взаємодії процесів

Таким чином, розглянувши опис системи, структурну, функціональну схеми системи, та діаграму взаємодії процесів перейдемо до опису блок-схем основної програми, та підпрограм, які використовуються, для реалізації системи.

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

4.1 Блок-схеми та опис алгоритмів функціонування системи

Алгоритмічне забезпечення системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання призначене для автоматизованого дослідження правил фільтрації мережевого трафіку, визначення потенційно небезпечних конфігураційних рішень і формування рекомендацій щодо їхнього вдосконалення.

Основу системи становить поєднання детермінованого аналізу мережевих політик із методами машинного навчання.

Алгоритми перевірки правил дозволяють визначати структурні суперечності, надлишкові дозволи та недосяжні правила. Інтелектуальний компонент використовується для виявлення нетипових конфігураційних характеристик, які потребують додаткового дослідження.

Результатом роботи є оцінка ризику окремих правил і конфігурації загалом із визначенням причин формування відповідних висновків.

Загальну послідовність функціонування програмного комплексу відображено на рисунку 4.1.

Після ініціалізації системи виконується отримання конфігурації міжмережевого екрана з файлу або підтримуваного інтерфейсу керування.

Далі здійснюється синтаксичний розбір і перетворення правил до уніфікованого представлення. На основі отриманих даних формується модель політики фільтрації.

Після цього виконуються перевірка коректності правил, пошук структурних аномалій та визначення потенційно небезпечних дозволів.

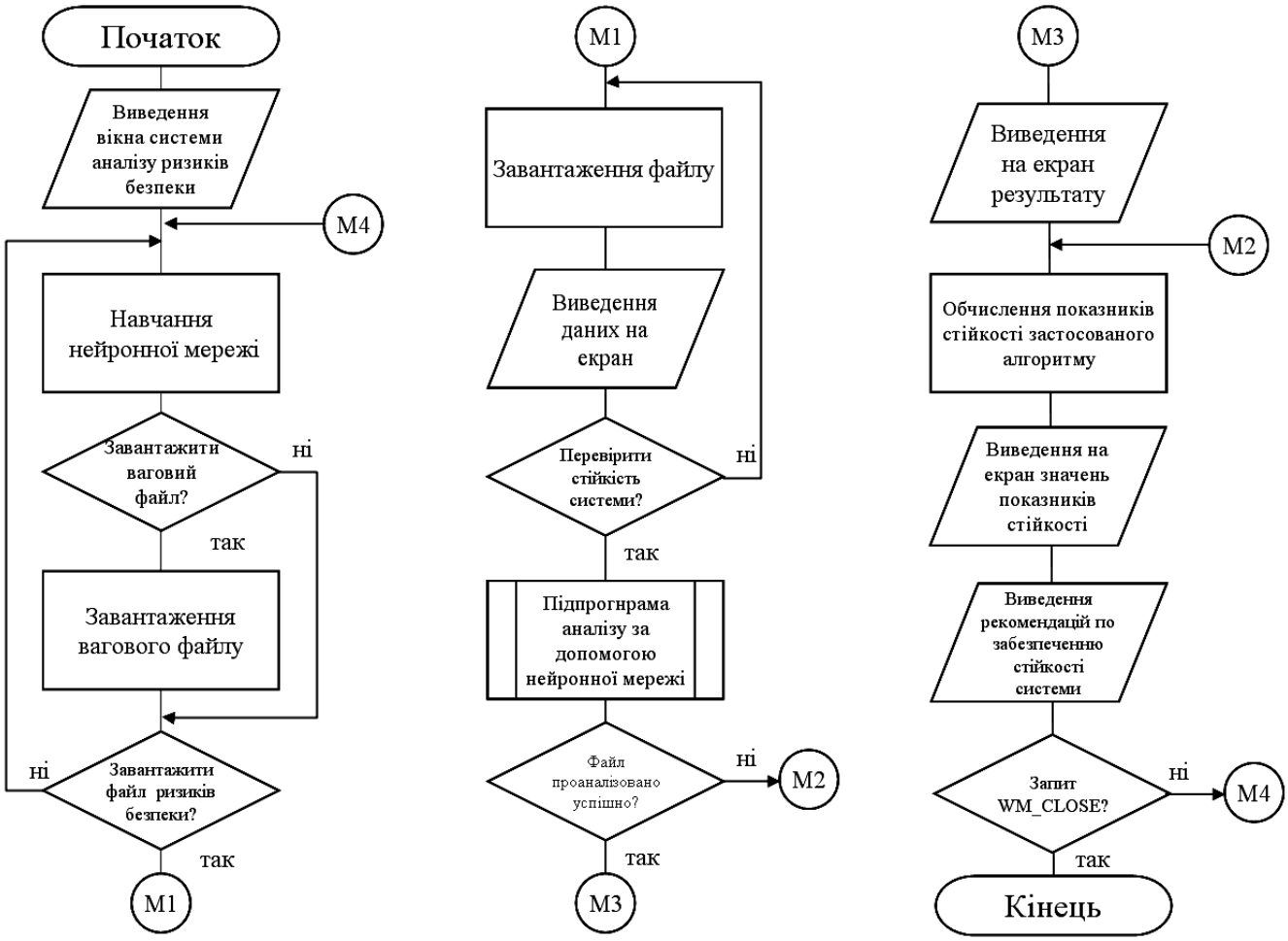

Рисунок 4.1 – Блок-схема основної програми

Наступним етапом є формування набору ознак для машинного навчання. Результати інтелектуального аналізу поєднуються з оцінками конфігураційних ризиків. Завершується оброблення формуванням аналітичного звіту з поясненнями та рекомендаціями.

Для реалізації запропонованого підходу доцільно використовувати модульну архітектуру.

Компонент імпорту забезпечує отримання конфігурацій із підтримуваних джерел. Підсистема нормалізації перетворює різні формати правил до єдиної структури. Статичний аналізатор визначає конфлікти, дублювання та потенційно неефективні правила.

Модуль оцінювання ризиків враховує характер дозволеного трафіку та значущість захищених ресурсів. Підсистема машинного навчання визначає статистичні відхилення у характеристиках правил.

Окремий компонент формує результати для користувацького інтерфейсу та зберігає історію виконаних перевірок.

Особливістю конфігурацій міжмережевих екранів є залежність результату фільтрації від порядку перевірки правил і конкретної платформи. У традиційних послідовних списках керування доступом може застосовуватися принцип першого відповідного правила.

Однак цей принцип не можна безумовно поширювати на всі міжмережеві екрани. Наприклад, у nftables результат проходження пакетів може залежати від декількох базових ланцюгів і пріоритетів оброблення. Тому перед аналізом необхідно визначати фактичну семантику відповідного механізму фільтрації.

Особливості роботи підпрограми виявлення конфліктів і визначення ризикових характеристик правил доцільно представити окремим алгоритмом на рисунку 4.2. Підпрограма отримує нормалізований набір правил, їхню послідовність і параметри політики безпеки. На першому етапі перевіряється належність правил до спільного контексту оброблення. Далі аналізуються перетини адресних діапазонів, протоколів і портів. Після встановлення відношень між правилами визначається тип потенційної аномалії. Окремо перевіряється широта дозволеного доступу. Отримані результати використовуються для розрахунку ризику та формування пояснення виявленого відхилення.

Запропонована система повинна розмежовувати конфігураційні помилки та статистичні аномалії. Конфігураційна помилка встановлюється на основі формально визначеного правила перевірки. Наприклад, за певної моделі послідовної фільтрації повністю перекрите правило може бути недосяжним. Статистична аномалія означає, що характеристики правила відрізняються від типових конфігурацій. Вона не доводить наявності вразливості. Рідкісне правило може бути технічно обґрунтованим, а поширене налаштування може створювати суттєвий ризик.

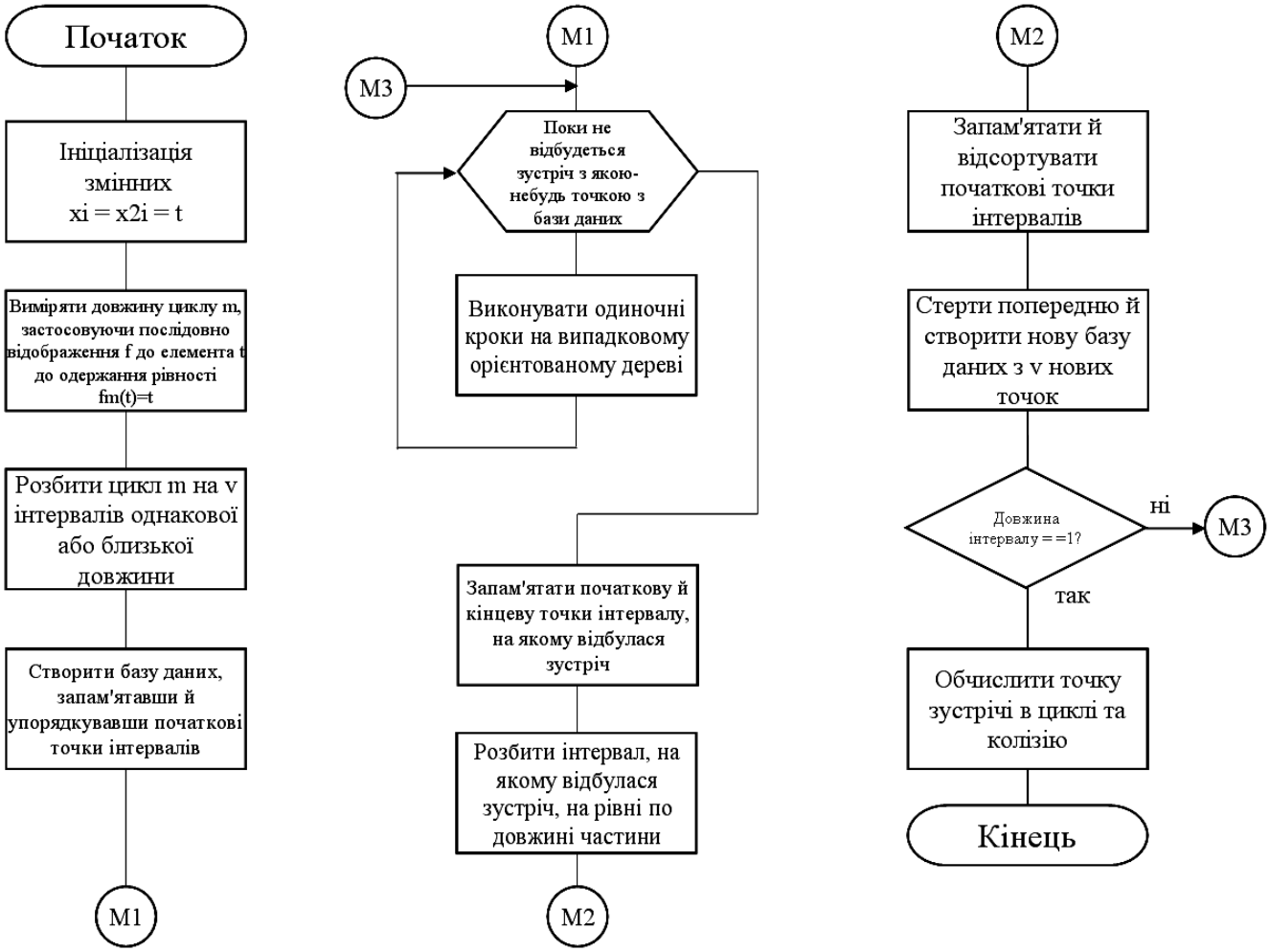

Рисунок 4.2 – Блок-схема роботи підпрограми

Для коректного аналізу необхідно враховувати призначення міжмережевого екрана. Правило, допустиме для ізольованого тестового сегмента, може бути неприйнятним для продукційної мережі з критичними серверами.

Тому до конфігураційних даних доцільно додавати інформацію про мережеві зони, категорії ресурсів, допустимі сервіси та встановлену політику доступу. За відсутності таких відомостей система повинна формувати технічні спостереження, не видаючи їх за підтверджені порушення вимог безпеки.

Важливим обмеженням є відокремлення аналізу конфігурації від фактичного тестування мережевої доступності. Наявність дозволяючого правила не гарантує проходження трафіку через відповідний пристрій.

На кінцевий результат також впливають маршрутизація, трансляція адрес, стан з'єднань, інші міжмережеві екрани та локальні політики вузлів. Отже, оцінювання ефективної доступності потребує ширшої моделі мережі.

Для безпечного використання програмного комплексу необхідно передбачити переважно пасивний режим роботи. Система отримує конфігурацію, аналізує її та формує рекомендації без автоматичного внесення змін до міжмережевого екрана. Застосування нової політики повинно виконуватися лише після перевірки запропонованих змін і підтвердження відповідальним адміністратором.

Формалізація семантики застосування мережевої політики

Для правильного визначення конфліктів необхідно знати порядок, у якому міжмережевий екран обробляє правила.

У найпростішому випадку використовується впорядкована послідовність, в якій рішення приймається за першим правилом, що відповідає параметрам пакета.

Проте інші платформи можуть підтримувати декілька етапів оброблення, вкладені ланцюги, виклики підпрограм, трансляцію адрес і контекстні перевірки.

Тому адаптер повинен задавати формальну модель виконання. Вона визначає порядок проходження правил і значення можливих дій.

Для nftables важливо враховувати, що рішення accept в одному базовому ланцюзі не обов'язково завершує оброблення пакета іншими базовими ланцюгами того самого оброблювального шляху. На відміну від цього, відповідне рішення drop припиняє подальше проходження пакета.

Якщо така семантика не відображена в моделі аналізу, висновки про недосяжність або ефективний дозвіл можуть бути помилковими.

Результатом є визначений контекст виконання, в межах якого можна застосовувати відповідні алгоритми перевірки.

Математична модель області дії правила

Для формального аналізу необхідно визначити множину пакетів, які відповідають умовам конкретного правила.

У спрощеній моделі правило (r_i) можна представити набором

$$r_i = (S_i, D_i, P_i, Q_i, A_i),$$

де (S_i) визначає множину адрес джерел, (D_i) характеризує адреси призначення, (P_i) задає протоколи, (Q_i) містить допустимі значення портів, а (A_i) визначає дію.

Область відповідності правила може бути представлена як

$$M_i = S_i \times D_i \times P_i \times Q_i$$

Наведена модель стосується визначеного класу пакетної фільтрації. Для державних і приватних мереж, складних протоколів і платформ із додатковими умовами необхідно враховувати інші атрибути.

Порівняння правил виконується через операції над множинами. Для визначення повного перекриття перевіряється відношення включення. Для часткового конфлікту використовується перетин.

Математичний підхід до виявлення аномалій у політиках фільтрації розглянуто в дослідженні Ehab S. Al-Shaer та Hazem H. Hamed «Discovery of Policy Anomalies in Distributed Firewalls», представленому на IEEE INFOCOM 2004.

Результатом є формальна основа для алгоритмічного визначення відношень між правилами.

Аналіз часткових конфліктів і перетинів

Не всі суперечності виникають через повне перекриття. Часто два правила мають лише спільну частину адресного простору або діапазону портів.

У такому випадку необхідно визначити перетин їхніх областей відповідності

$$M_{(ij)} = M_i \cap M_j$$

Якщо перетин порожній, правила не впливають на однакові пакети в межах обраної моделі. Якщо перетин непорожній, перевіряються порядок та дії відповідних правил.

Наприклад, перше правило може дозволяти TCP-з'єднання до визначеної підмережі, а друге забороняти доступ до окремого сервера цієї підмережі.

У послідовній політиці результат для спільної частини визначається правилом, яке має вищий пріоритет. Таке співвідношення не завжди свідчить про помилку. Воно може бути результатом навмисного проєктування політики.

Тому програмний комплекс повинен відображати точні умови перетину та виявлену залежність, не змінюючи автоматично конфігурацію.

Результатом є перелік часткових конфліктів, які потребують оцінювання відповідно до політики безпеки.

Математична модель оцінювання конфігураційного ризику

Для формування інтегральної оцінки доцільно використовувати декілька груп характеристик.

До них належать широта дозволеного доступу, критичність ресурсу, невідповідність встановленій політиці та статистична аномальність правила.

Узагальнену оцінку можна представити як

$$R_i = w_e E_i + w_c C_i + w_p P_i + w_a A_i,$$

де (E_i) характеризує експозицію доступу, (C_i) відображає критичність ресурсу, (P_i) визначає відхилення від політики, а (A_i) є нормалізованою оцінкою аномальності.

Коефіцієнти (w_e), (w_c), (w_p) та (w_a) встановлюють значущість відповідних складових. Для обчислення показники приводяться до спільного діапазону.

Необхідно враховувати, що значення (R_i) не є безпосередньою ймовірністю компрометації. Воно призначене для порівняння правил і визначення порядку їхнього аналізу.

Для критичних порушень формально встановленої політики може застосовуватися окреме обов'язкове правило пріоритету, незалежне від інтегрального бала.

Результатом є пояснювана оцінка ризику з визначеним внеском окремих критеріїв.

Обґрунтування застосування Isolation Forest

Для виявлення нетипових правил може застосовуватися Isolation Forest. Цей алгоритм не потребує обов'язкової наявності розмітки кожного спостереження.

Його принцип полягає у випадковому розділенні простору ознак. Спостереження, які значно відрізняються від більшості, зазвичай ізолюються меншою кількістю розбиттів.

На початковому етапі формується матриця числових характеристик. Далі виконується навчання набору дерев.

Після цього для кожного правила обчислюється оцінка аномальності.

У бібліотеці scikit-learn модель IsolationForest може використовувати метод decision_function, за яким нижчі значення відповідають більш аномальним спостереженням відносно визначеної межі.

Результат необхідно інтерпретувати як статистичне відхилення, а не як безпосередню оцінку вразливості міжмережевого екрана.

Особливу увагу слід приділити параметрам навчання, складу ознак та очікуваній частці аномальних записів.

Результатом є модель, яка визначає правила з незвичними комбінаціями конфігураційних характеристик.

Програмний приклад виявлення затінених правил

Для пояснення принципу формального аналізу можна використати програмний алгоритм мовою Python. Він демонструє пошук правил, які повністю перекриваються попередніми записами.

Приклад розглядає впорядковані IPv4-правила з протоколами TCP та UDP. Для кожного правила враховуються адреси джерела й призначення, діапазон портів, дія та контекст виконання.

Наведена реалізація призначена для ілюстрації методу.

Вона не є універсальним аналізатором усіх типів міжмережевих екранів і не підтверджує використання саме такого коду в програмному комплексі.

```
from dataclasses import dataclass
from ipaddress import IPv4Network, ip_network

@dataclass(frozen=True)
class FirewallRule:
    # Унікальний ідентифікатор правила
    rule_id: str

    # Контекст послідовного застосування правил
    chain: str
    direction: str
    zone: str

    # Адресні діапазони джерела та призначення
    source: IPv4Network
    destination: IPv4Network

    # Тип протоколу та інтервал портів призначення
    protocol: str
    port_start: int
    port_end: int

    # Дозвіл або заборона передавання
    action: str

    # Ознака активності правила
    enabled: bool = True


def validate_rule(rule: FirewallRule) -> bool:
    """Перевірка базових характеристик правила."""

    if not rule.rule_id or not rule.chain:
        return False

    if not rule.direction or not rule.zone:
        return False

    # Приклад обмежено протоколами TCP та UDP
    if rule.protocol not in {"tcp", "udp"}:
        return False

    if rule.action not in {"allow", "deny"}:
        return False

    # Порт призначення повинен належати допустимому діапазону
    if not 0 <= rule.port_start <= rule.port_end <= 65535:
        return False

    return True

def same_context(first: FirewallRule,
                 second: FirewallRule) -> bool:
    """Перевірка спільного контексту фільтрації."""

    return (
        first.chain == second.chain
        and first.direction == second.direction
        and first.zone == second.zone
        and first.protocol == second.protocol
    )


def covers(previous: FirewallRule,
```

```
        current: FirewallRule) -> bool:
    """Перевірка повного охоплення наступного правила."""
    if not same_context(previous, current):
        return False

    # Попередня адресна множина повинна охоплювати наступну
    source_covered = current.source.subnet_of(
        previous.source
    )

    destination_covered = current.destination.subnet_of(
        previous.destination
    )
    # Діапазон портів також повинен бути повністю охоплений
    ports_covered = (
        previous.port_start <= current.port_start
        and previous.port_end >= current.port_end
    )

    return (
        source_covered
        and destination_covered
        and ports_covered
    )


def analyze_shadowing(rules: list[FirewallRule]) -> list[dict]:
    """Пошук затінення в послідовній політиці first-match."""

    findings = []
    # Перевіряємо коректність усіх правил перед аналізом
    for rule in rules:
        if not validate_rule(rule):
            raise ValueError(
                f"Некоректне правило: {rule.rule_id}"
            )

    for current_index, current in enumerate(rules):
        if not current.enabled:
            continue

        # Досліджуємо лише попередні активні правила
        for previous in rules[:current_index]:
            if not previous.enabled:
                continue

            if not covers(previous, current):
                continue

            # Дія визначає тип виявленого затінення
            if previous.action == current.action:
                finding_type = "SAME_ACTION_SHADOWING"
            else:
                finding_type = "CONFLICTING_SHADOWING"

            findings.append({
                "rule_id": current.rule_id,
                "covered_by": previous.rule_id,
                "finding_type": finding_type,
                "status": "REQUIRES_REVIEW"
            })
            # Для демонстрації достатньо першого підтвердження
            break
```

```
    return findings
# Демонстраційний набір правил однієї політики
rules = [
    FirewallRule(
        rule_id="ALLOW_INTERNAL",
        chain="forward",
        direction="outbound",
        zone="internal",
        source=ip_network("10.0.0.0/8"),
        destination=ip_network("192.168.10.0/24"),
        protocol="tcp",
        port_start=1,
        port_end=65535,
        action="allow"
    ),
    FirewallRule(
        rule_id="DENY_SSH",
        chain="forward",
        direction="outbound",
        zone="internal",
        source=ip_network("10.12.0.0/16"),
        destination=ip_network("192.168.10.20/32"),
        protocol="tcp",
        port_start=22,
        port_end=22,
        action="deny"
    )
]

results = analyze_shadowing(rules)

for finding in results:
    print(finding)
```

У наведеному фрагменті використовується структура FirewallRule, яка описує параметри нормалізованого правила. Для адресних діапазонів застосовується стандартний модуль Python ipaddress.

Функція validate_rule перевіряє допустимість основних характеристик. Вона обмежує аналіз підтримуваними протоколами та діями.

Функція same_context визначає належність двох правил до одного контексту фільтрації. Це необхідно, оскільки правила різних ланцюгів або напрямів не можна довільно порівнювати як послідовні записи.

Функція covers перевіряє повне включення адресних діапазонів і портів наступного правила до області попереднього.

Після цього процедура analyze_shadowing послідовно досліджує активні правила. Якщо попередній запис повністю перекриває наступний, формується відповідний результат.

У демонстраційному наборі широке дозволяюче правило охоплює пізніше правило заборони SSH до окремого сервера. За умови саме такої семантики першого збігу пізніше правило не може заборонити відповідний трафік.

Необхідно враховувати обмеження програмного прикладу. Він не аналізує IPv6, NAT, стан з'єднань, заперечення умов, динамічні адресні об'єкти та взаємодію декількох ланцюгів.

Крім того, алгоритм визначає лише затінення окремим попереднім правилом. Для аналізу перекриття сукупністю правил необхідно використовувати операції над об'єднаннями множин або інше відповідне формальне представлення.

Результатом прикладу є перелік конфігураційних відхилень із зазначенням правил, що беруть участь у відповідній ситуації.

Особливості контролю безпечного застосування змін

Видалення або перестановка правил може суттєво вплинути на доступність мережевих сервісів. Тому зміни необхідно перевіряти до їхнього застосування.

Для цього доцільно використовувати окрему модель проєктованої конфігурації.

На початковому етапі створюється копія поточного набору правил. До неї вносяться запропоновані зміни.

Після цього виконується повторний статичний аналіз. Окремо порівнюється результат фільтрації для визначених контрольних класів трафіку.

Якщо система підтримує формальне моделювання політики, можна визначити множини пакетів, для яких рішення змінилося.

Після перевірки формується звіт про можливий вплив.

Для продукційної інфраструктури доцільно передбачити резервну копію конфігурації та процедуру відновлення.

Результатом є перевірений сценарій модифікації, який може бути переданий адміністратору для затвердження.

Оброблення неповних і некоректних конфігурацій

Під час імпорту можливі помилки синтаксису, відсутність пов'язаних об'єктів, невідомі дії та непідтримувані конструкції.

Для кожної категорії необхідно визначити відповідну реакцію.

Якщо конфігурація містить синтаксично некоректний запис, система повинна зафіксувати його позицію та причину відхилення.

У випадку невизначеного адресного об'єкта необхідно позначити залежні правила як неповні.

Якщо адаптер не підтримує певну особливість платформи, відповідне правило не повинно автоматично перетворюватися на універсальний дозвіл.

Окремо слід контролювати помилки машинного навчання. За відсутності сумісної моделі або необхідного набору ознак статистичний етап не виконується.

При цьому результати детермінованих перевірок можуть залишатися доступними.

Результатом є оброблення помилок із чітким розмежуванням виконаних та пропущених перевірок.

Методика функціональної перевірки проєктних рішень

Для підтвердження правильності роботи системи необхідно сформувати набір контрольованих конфігурацій міжмережевих екранів.

На початковому етапі перевіряється синтаксичний імпорт. Для цього використовуються конфігурації з відомими правилами, адресними об'єктами та сервісними групами.

Далі досліджується правильність нормалізації. Отримані внутрішні записи порівнюються з початковими параметрами.

Окремо необхідно перевірити правила з IPv4 та IPv6, різними протоколами й діапазонами портів.

Для виявлення затінення формуються сценарії, у яких одне правило повністю перекриває інше. Результат порівнюється з очікуваним висновком.

Наступним етапом є перевірка часткових перетинів. Для цього використовуються правила з різними діями та спільними адресними областями.

Окремо перевіряються незалежні правила, які не повинні класифікуватися як конфліктні.

Для дослідження надлишковості формуються конфігурації з однаковими умовами й діями. Результати повинні враховувати можливі відмінності побічних операцій.

Результатом є методика перевірки функціональної коректності статичного аналізатора.

Експериментальне дослідження виявлення конфігураційних аномалій

Для оцінювання інтелектуального компонента необхідно підготувати тестовий набір правил із достовірною розміткою.

До нього можуть включатися звичайні конфігураційні записи, контрольовані надмірні дозволи, рідкісні протокольні комбінації та інші визначені типи відхилень.

Важливо розділяти статистичну нетиповість і підтверджений ризик.

Наприклад, правило, яке використовує рідкісний порт, може бути нормальним для спеціалізованої системи. Водночас типовий дозвіл широкого доступу може суперечити встановленій політиці.

Тому експериментальна розмітка повинна містити окремі характеристики статистичної аномальності й конфігураційного порушення.

Після підготовки набору виконується навчання моделі та формування передбачень.

Для порівняння доцільно використовувати окрему базову стратегію, яка спирається лише на статичні ознаки.

Результатом експерименту має бути оцінка додаткової користі машинного навчання порівняно з детермінованими перевірками.

Оцінювання продуктивності аналізатора правил

Час оброблення конфігурації залежить від кількості правил, складності їхніх умов і структури адресних об'єктів.

Для простого попарного аналізу (n) правил верхня оцінка кількості порівнянь має порядок $O(n^2)$.

За збільшення розміру конфігурації такий підхід може потребувати значних обчислювальних ресурсів.

Для покращення ефективності доцільно попередньо групувати правила за контекстом, протоколом і напрямом. Для адресних діапазонів можуть застосовуватися префіксні дерева або інші структури, які прискорюють пошук відповідних мереж.

Для портових інтервалів можливе використання відповідних індексів перетину. Окремо необхідно досліджувати витрати на розкриття вкладених адресних груп.

Під час експериментів вимірюються час імпорту, тривалість нормалізації, час формального аналізу та витрати на машинне навчання.

Для порівняння доцільно використовувати конфігурації з поступовим збільшенням кількості правил. Результатом є оцінка масштабованості програмного комплексу.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Програмне забезпечення системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання призначене для автоматизованої перевірки правил фільтрації мережевого трафіку, визначення потенційних конфліктів і формування оцінок конфігураційних ризиків.

Система поєднує статичний аналіз мережевих політик із виявленням нетипових правил за допомогою машинного навчання.

Результати перевірки використовуються для підготовки рекомендацій щодо вдосконалення налаштувань міжмережевих екранів. Головне вікно програми показане на рисунку 5.1.

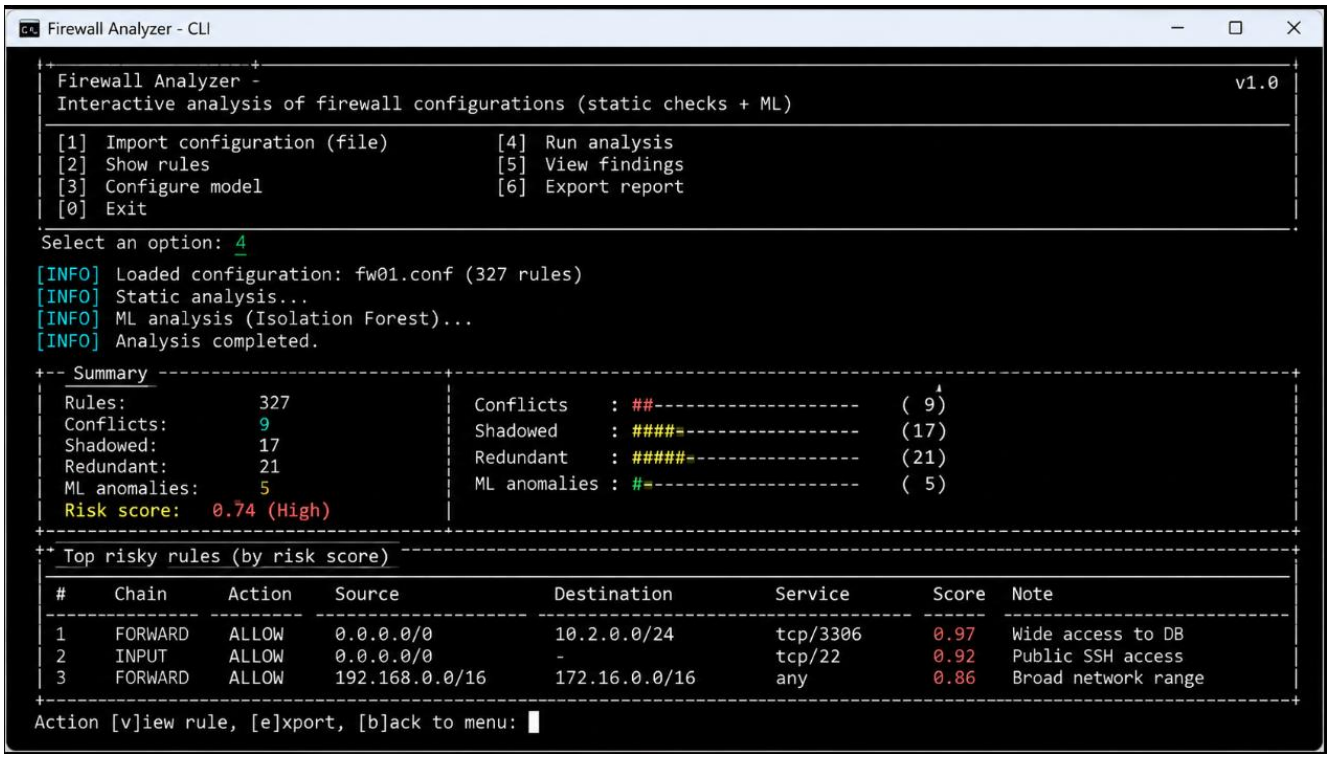

Рисунок 5.1 – Головне вікно розробленого ПЗ

Впровадження програмного комплексу передбачає підготовку обчислювального середовища, налаштування джерел конфігураційних даних, встановлення аналітичних компонентів і перевірку роботи моделі машинного навчання. Функціональна структура охоплює модулі імпорту конфігурацій, нормалізації правил, статичного аналізу, оцінювання ризиків та інтелектуального виявлення аномалій. Окремий компонент відповідає за збереження результатів перевірок і формування аналітичних звітів.

Для серверної частини як можливий технологічний варіант доцільно використовувати Python. Оброблення структурованих конфігураційних записів може здійснюватися засобами стандартних бібліотек Python і pandas. Для роботи з IPv4 та IPv6 використовується модуль ipaddress. Реалізація інтелектуального компонента можлива за допомогою scikit-learn. Зокрема, алгоритм Isolation Forest може застосовуватися для визначення статистично нетипових характеристик правил. Конкретний склад бібліотек повинен відповідати фактичній програмній реалізації.

Програмний комплекс може розгортатися на серверній операційній системі Linux або іншій платформі, яка підтримує вибране середовище виконання. Вимоги до апаратного забезпечення визначаються кількістю правил, складністю адресних груп і розміром навчального набору.

Для статичного аналізу та використання Isolation Forest не є обов'язковим застосування графічного прискорювача. Основними ресурсами залишаються продуктивність центрального процесора, обсяг оперативної пам'яті та дисковий простір для зберігання конфігурацій.

Підготовка середовища починається зі встановлення інтерпретатора Python і необхідних програмних залежностей. Для ізоляції компонентів доцільно створити окреме віртуальне середовище. Після встановлення перевіряється доступність бібліотек, правильність оброблення мережевих адрес та можливість запуску аналітичного модуля. Якщо програмне забезпечення використовує серверний інтерфейс, додатково налаштовуються його мережеві параметри та механізми автентифікації користувачів.

У програмному забезпеченні також передбачається представлення інформації про розробника. Вона використовується для ідентифікації програмного продукту та організації подальшого технічного супроводження. Відомості про автора системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання представлені на рисунку 5.2.

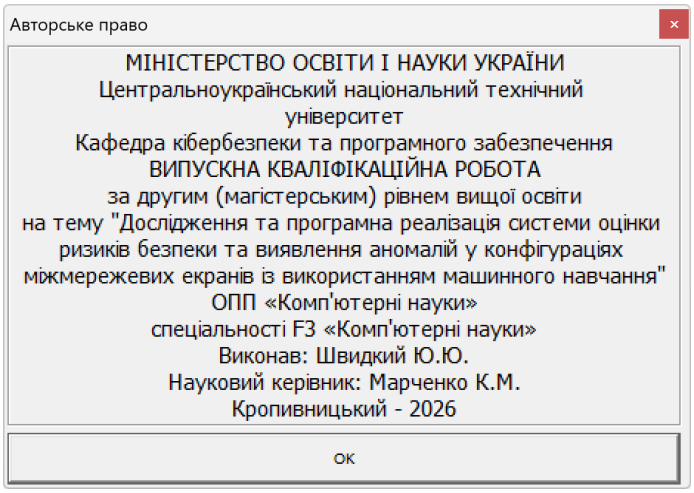

Рисунок 5.2 – Авторське право

Для зберігання конфігураційних знімків і результатів перевірок може використовуватися PostgreSQL. У відповідному сховищі передбачається облік міжмережевих екранів, імпортованих конфігурацій, нормалізованих правил, виявлених відхилень та оцінок ризику. Окремо можуть зберігатися версії моделей машинного навчання. Після налаштування необхідно перевірити можливість записування нової конфігурації та подальшого отримання її аналітичних результатів.

Наступним етапом є налаштування джерел конфігураційних даних. Програмний комплекс може використовувати експортовані файли правил або підтримувані інтерфейси керування міжмережевими екранами. Для кожного типу джерела визначається відповідний адаптер імпорту. Якщо передбачено отримання конфігурацій безпосередньо з обладнання, доцільно використовувати облікові

записи лише з правами читання. Це дозволяє виконувати аналіз без можливості випадкової зміни робочих правил фільтрації.

Після підключення джерел необхідно перевірити правильність нормалізації. Для цього використовується контрольована конфігурація з відомими адресними діапазонами, протоколами, портами та діями. Отримані записи порівнюються з початковими параметрами. Особливу увагу потрібно приділити відповідності правил фактичній семантиці міжмережевого екрана. Для послідовних політик із принципом першого збігу та для nftables можуть використовуватися різні способи інтерпретації порядку виконання.

Налаштування статичного аналізатора передбачає визначення підтримуваних перевірок. До них належать виявлення повністю затінених правил, часткових перетинів, конфліктних дій і потенційної надлишковості. Для оцінювання ризиків додатково задаються характеристики критичності мережевих ресурсів та допустимих напрямів доступу. Відомості про призначення серверів і мережевих сегментів повинні отримуватися з підтвердженої інвентаризаційної документації.

Підготовка інтелектуального компонента включає завантаження навченої моделі та відповідної схеми ознак. Для кожного правила можуть визначатися довжини мережевих префіксів, характеристики портів, тип дії та результати статичних перевірок. Якщо використовується Isolation Forest, необхідно забезпечити відповідність структури ознак під час навчання й експлуатації. Порогові значення аномальності повинні уточнюватися на контрольованому наборі конфігурацій. Статистичне відхилення не повинно автоматично трактуватися як підтверджена вразливість.

Окремо налаштовуються параметри моделі оцінювання ризику. Для цього визначаються вагові коефіцієнти, які характеризують значущість широти доступу, критичності ресурсу, порушення політики та результатів машинного навчання. Після встановлення параметрів доцільно перевірити декілька контрольованих сценаріїв. Правила, які створюють широкий доступ до критичних

адміністративних сервісів, повинні отримувати відповідну пріоритетність згідно із заданою політикою оцінювання.

Рекомендована послідовність запуску починається з перевірки доступності сховища даних. Далі активуються компоненти імпорту та нормалізації конфігурацій. Після цього запускається статичний аналізатор правил. Наступним етапом завантажується модель машинного навчання та ініціалізується модуль оцінювання ризиків. Завершується запуск активацією користувацького інтерфейсу й перевіркою взаємодії між аналітичними компонентами.

Первинну функціональну перевірку доцільно проводити на тестовій конфігурації, яка містить заздалегідь визначені конфлікти. Наприклад, широке дозволяюче правило може передувати конкретній забороні доступу до адміністративного порту. Для відповідної послідовної політики система повинна визначити затінення наступного правила. Окремо перевіряються правила з однаковими діями, частковими перетинами та незалежними адресними діапазонами. Отримані результати порівнюються з очікуваними висновками.

Для перевірки машинного навчання використовується набір конфігурацій із відомими характеристиками. Після формування ознак виконується обчислення оцінок аномальності. Необхідно перевірити правильність завантаження моделі, оброблення вхідних даних і відображення результатів. Окремо контролюється поведінка програмного комплексу за відсутності сумісної моделі. У такому випадку результати статичного аналізу повинні залишатися доступними без необґрунтованих інтелектуальних висновків.

Під час експлуатації можливі помилки синтаксичного розбору, відсутність адресних об'єктів, недоступність міжмережевого екрана та порушення роботи аналітичних компонентів.

Для діагностики використовуються службові журнали й повідомлення про стан перевірок. Якщо окреме правило містить непідтримувану конструкцію, система повинна позначити неповноту аналізу. Неперевірені записи не повинні автоматично вважатися безпечними або небезпечними.

Перед введенням програмного комплексу в регулярну експлуатацію необхідно перевірити розмежування користувацьких повноважень, захист конфігураційних даних і резервне копіювання сховища. Окремо контролюється правильність відновлення після перезапуску та збереження історії перевірок. Запропоновані зміни правил доцільно аналізувати в окремій проєктній конфігурації. Їхнє застосування до робочого міжмережевого екрана повинно виконуватися лише після перевірки впливу та підтвердження відповідальним адміністратором.

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Метою розробки є дослідження та програмна реалізація системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Об'єктом дослідження є процес оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Предметом дослідження є методи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Методи дослідження базуються на методах машинного навчання, методи захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

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

– Удосконалено метод оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

– Розроблено вітчизняний продукт оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання, який має більш широкі можливості, на відміну від існуючих аналогів.

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

7.1 Вступ

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

– Інструкцій з охорони праці по кожній професії і загальні.

– Положення про охорону праці.

– Накази з охорони праці.

– Журнали реєстрації та інструктажу.

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

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

Законом України “Про охорону праці” [3] регламентуються загальні положення державної політики в галузі охорони праці, а конкретизуються ці положення нормативно-правовими актами про охорону праці, зокрема Наказом Міністерства соціальної політики України 14.02.2018 № 207, який зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за №508/31960 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» [5], яким затверджено нормативно-правовий акт з охорони праці НПАОП 0.00-7.15-18, «Правила охорони праці під час експлуатації електронно-обчислювальних машин», та «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-97.

Програмісти у процесі роботи мають негативний вплив на органи зору, а також мають значну розумову напругою і нервово-емоційне навантаження. Руки (суглоби пальців та м'язи рук) при роботі з клавіатурою мають теж істотне навантаженням. До шкідливих факторів, які впливають на робітників галузі інформаційних технологій (ІТ), фахівці відносять високочастотні електромагнітні коливання (випромінювання) роботи апаратної частини ЕОМ та виділення шкідливих газів.

Ці шкідливі фактори можуть привести до професійних захворювань.

Розглянемо шкідливі чинники роботи програмістів керуючись наступними нормативно-правовими актами: «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-98 [5], та «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» НПАОП 0.00-7.15-17.

Умови праці програміста включають наступні фактори:

– параметри повітряного середовища в приміщенні;

– вентиляція приміщення;

– освітлення приміщення;

– параметри повітряного середовища в приміщенні, тощо.

Щоб запропонувати заходи щодо зменшення негативного впливу комп’ютера на організм людини визначимо фактори, які можуть викликати професійне захворювання і впливають на працездатність програміста.

7.2 Аналіз умов праці на робочому місці ІТ-фахівця

На робочому місці ІТ-фахівця (або програміста) виникають небезпечні та шкідливі для безпечної життєдіяльності фактори:

– підвищений рівень шуму;

– несприятливі мікрокліматичні умови;

– недостатній рівень освітленості;

– шкідливі речовини;

– підвищений рівень електромагнітних випромінювань радіочастот;

– висока напруга електричної мережі;

– статична електрика та інші.

Робота програміста супроводжується також підвищеним ступенем напруженості трудового процесу. При систематичному впливі виробничих факторів, які не відповідають нормативним показникам, зростає рівень професійно зумовленої захворюваності працюючих та можуть виникнути професійні захворювання органів зору, руху, нервової системи. Таким чином, вивчення умов праці на робочому місці програміста є необхідною умовою запобігання негативних наслідків впливу небезпечних та шкідливих факторів. Робоче місце, добре пристосоване до трудової діяльності інженера, правильно і доцільно організоване, щодо простору, форми, розміру забезпечує йому зручне положення при роботі і високу продуктивність праці при найменшому фізичному і психічному напруженні.

Нормування параметрів проводиться в залежності від періоду року та категорії важкості виконуваних робіт. Для постійних робочих місць, якими є робочі місця ІТ-фахівців, встановлені оптимальні параметри мікроклімату, а за неможливості їх дотримання використовують допустимі параметри. Робота ІТ-фахівця за важкістю відноситься до Іа (роботи, що виконуються сидячи і не потребують фізичного напруження) та Іб (роботи, що виконуються сидячи, стоячи або пов'язані з ходінням та супроводжуються деяким фізичним напруженням) категорій. В таблиці 7.1. наведені оптимальні параметри мікроклімату в приміщеннях.

Виміряні за допомогою приладів температура та вологість у приміщеннях праці ІТ-фахівців повинні відповідати зазначеним у таблиці для теплого періоду року. Слід зазначити, що для нормалізації параметрів мікроклімату слід використовувати у приміщеннях кондиціювання повітря, або забезпечити подачу свіжого повітря системами вентиляції. Норми подачі свіжого повітря наведені у таблиці 7.2.

Таблиця 7.1 – Параметри мікроклімату для приміщень з ПК

Період року	Параметр мікроклімату	Величина
Холодний	Температура повітря в приміщенні; відносна вологість; швидкість руху повітря	22...24°С; 40... 60%; до 0,1 м/с
Теплий	Температура повітря в приміщенні; відносна вологість; швидкість руху повітря	23...25 °С; 40...60%; 0,1...0,2 м/с

Таблиця 7.2 – Норми подачі свіжого повітря в приміщення

Характеристика приміщення	Об'ємна витрата свіжого повітря, що подається в приміщення, $м^3$ на одну людину в годину
Об'єм до 20 $м^3$ на людину	Не менше 30
20... 40 $м^3$ на людину	Не менше 20
Більше 40 $м^3$на людину	Може біти використана природна вентиляція

Створення сприятливих умов праці і правильне естетичне оформлення робочих місць на виробництві має велике значення як для полегшення праці, так і для підвищення його привабливості, позитивно впливає на продуктивність праці. Забарвлення приміщень і меблів повинні сприяти створенню сприятливих умов для зорового сприйняття, гарного настрою. У службових приміщеннях, у яких виконується одноманітна розумова робота, що вимагає значної нервової напруги і великого зосередження, забарвлення повинно бути спокійних тонів – малонасичені відтінки холодного зеленого або блакитного кольорів.

При розробці оптимальних умов праці програміста необхідно враховувати освітленість. Раціональне освітлення робочого місця є одним з найважливіших факторів, що впливають на ефективність трудової діяльності людини, що попереджають травматизм і професійні захворювання. Правильно організоване освітлення створює сприятливі умови праці, підвищує працездатність і продуктивність праці. Освітлення на робочому місці

програміста повинно бути таким, щоб працівник міг без напруги зору виконувати свою роботу. Стомлюваність органів зору залежить від ряду причин: недостатність освітленості; надмірна освітленість; неправильний напрям світла. Недостатність освітлення приводить до напруги зору, ослабляє увагу, приводить до настання передчасної стомленості. Надмірно яскраве освітлення викликає засліплення, роздратування і різь в очах. Неправильний напрямок світла на робочому місці може створювати різкі тіні, відблиски, дезорієнтувати працюючого. Всі ці причини можуть призвести до нещасного випадку або профзахворювань. [4]

7.3 Пропозиції щодо підвищення працездатності ІТ – фахівців

Поява та впровадження нових інформаційно-комунікаційних технологій зумовлює необхідність подальшого вдосконалення охорони праці фахівців ІТ-індустрії. Все це потребує розробки нових нормативно-правових актів з регламентації праці та відпочинку фахівців ІТ-індустрії і стандартів підприємств, центрів комп'ютерної техніки, центрів інформаційних технологій, сучасних комп'ютерних класів.

Для підвищення розумової працездатності то зорової роботи повинна здійснюватися ергономічна оптимізація в рамках системи «оператор-термінал», яка сприятиме результативній фізичній та інтелектуальний працездатності і відновленню психосоматичного здоров'я фахівців ІТ-індустрії. Всі наведені заходи щодо вдосконалення охорони праці фахівців ІТ-індустрії повинні контролюватися службою охорони праці та комісією з охорони праці підприємства.

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

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

1. Середовище і розпорядок праці.

Для мінімізації негативних ефектів, що пов’язані з перевтомленням ІТ-фахівців, потрібно чітко прописати і реалізувати графік періодів праці-відпочинку, щоб фахівець міг можливість переключити увагу, дати можливість відпочити очам, мозку, елементарно, встати розім’яти ноги.

Також потрібно зробити максимально комфортними умови мікроклімату у офісному приміщенні, де працюють ІТ-фахівці. Мається на увазі встановлення і експлуатація, коли виникає необхідність, кондиціонерів, опалення, та системи вентиляції, задля попередження перегрівання, переохолодження ІТ-фахівців, і подальшої неможливості ними виконувати свої функції.

Також, за можливості, нами пропонується введення практики віддаленої праці ІТ-фахівцями, якщо роботодавець не може забезпечити оптимальні і безпечні умови в офісному приміщенні, або якщо фахівця вони не влаштовують із певних причин.

2. Фізичні і психоемоційні чинники.

Першим і найважливішим чинником, що впливає на працездатність ІТ-фахівців є робоче місце, і саме тому, роботодавець має забезпечити максимальний його комфорт і безпеку.

Гарантією цих факторів може слугувати сертифікація меблів, що використовуються на підприємстві ІТ-галузі. Тому нами пропонується закупівля тільки меблів, які пройшли сертифікацію на відповідність. Під психоемоційними чинниками ми розуміємо гарне самопочуття фахівців, позитивний настій, гарний психологічний клімат у колективі, тощо. Задля того, щоб психоемоційні чинники мали максимально позитивний ефект, керівництву слід поводити заходи, які сприятимуть укріпленню і покращенню міжособистісних стосунків у колективі, таких як психологічні тренінги, таймбілдінг, спортивні змагання і естафети.

Також, сюди можна віднести розробку і впровадження системи мотивації працівників, як фінансової, так моральної і адміністративної.

7.4 Розрахункова частина

Для захисного штучного заземлення застосовуються вертикальні електроди: металевий куток 50х50х5 мм, довжиною L=3 м, та горизонтальний електрод – металева полоса з перетином 50х5 мм. Напруга – 220/380 В. Розрахункова схема розташування заземлюючих електродів – по контуру (прямокутником).

Розрахунок проведемо за допустимим опором розтіканню струму заземлювача.

Початкові дані для розрахунку захисного заземлення: тип верхнього шару ґрунту – чорнозем, нижнього шару ґрунту – глина (питомий опір ρ_2 = 40 Ом·м). Умовна товщина верхнього шару ґрунту: H=0,6 м. Відстань між вертикальними заземлювачами (електродами) A=3 м. Глибина закладення горизонтального контура заземлення t=0,75 м. Опір заземлювача, який нормується: $R_{ЗН}$ = 4 Ом. Необхідно визначити необхідну кількість вертикальних заземлювачів та довжину полоси (горизонтального заземлювача) (рис. 7.1).

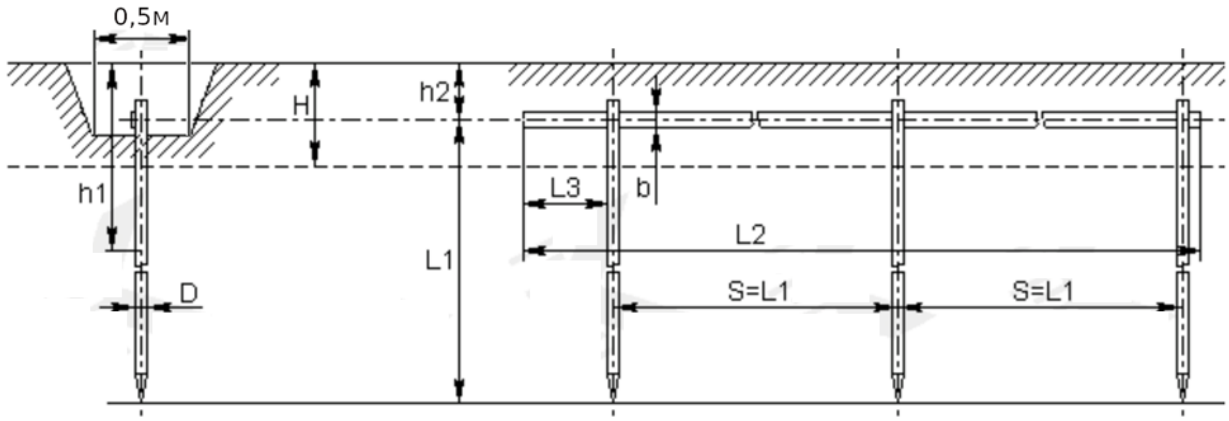

Рисунок 7.1 – Схема штучного заземлення

Виконуємо розрахунок.

Відстань від центра вертикального заземлювача до поверхні землі:

$$T = t + L/2 = 0,75 + 3/2 = 2,25 \text{ м.}$$

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

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

де

$\psi = 1{,}36$ – табличне значення коефіцієнта сезонності для відповідної кліматичної зони у багатошаровому ґрунті [11];

$\rho_2 = 40$ Ом·м – табличне значення питомого опору нижнього шару ґрунту (глина) [11].

Еквівалентний діаметр вертикального електрода (кутка) [11]:

$$D_в = 0{,}95 \cdot К = 0{,}95 \cdot 50 = 47{,}5 \text{ мм.} = 0{,}0475 \text{ м.}$$

де К= 50 мм – розмір металевого кутка (задано).

Відношення A/L=3/3=1.

Опір розтіканню електричного струму одного електрода вертикального заземлювача з урахуванням заглиблення заземлювача [11]:

$$R_О = 0{,}366 \cdot (\rho/L) \cdot [\lg(2L/D_в) + (1/2) \cdot \lg((4T+L)/(4T-L))] =$$

$$= 0{,}366 \cdot (54{,}5/3) \cdot [(\lg(2 \cdot 3/0{,}0475) + (1/2) \cdot \lg((4 \cdot 2{,}25+3)/(4 \cdot 2{,}25-3))] = 14{,}9 \text{ Ом.}$$

Визначаємо коефіцієнт екранування вертикальних електродів Кев=0,53 при орієнтовній кількості вертикальних електродів, яке дорівнює 5 [11].

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

$$N = R_О / (К_{ев} R_{ЗН}) = 14{,}9 / (0{,}53 \cdot 4) = 7{,}05 \approx 7 \text{ шт.}$$

Визначаємо довжину з'єднуючої полоси:

$$L_П = 1{,}05 \cdot A \cdot N = 1{,}05 \cdot 3 \cdot 7 = 18{,}5 \approx 18 \text{ м.}$$

Опір розтіканню електричного струму з'єднуючої полоси з урахуванням кліматичного коефіцієнта питомого опору ґрунту $К_П$ [11]:

$$R_П = 0{,}366(\rho \cdot К_П / L_П) \lg(2 \cdot L_П^2 / (B \cdot t)) =$$

$$= 0{,}366(40 \cdot 5/18) \cdot \lg((2 \cdot 18^2)/(0{,}05 \cdot 0{,}75)) = 20{,}1 \text{ Ом.}$$

де

$К_П = 5$ – табличне значення кліматичного коефіцієнта питомого опору ґрунту для відповідної кліматичної зони для з'єднуючої полоси [11]:

B = 50 мм = 0,05 м.- ширина з’єднуючої полоси (задана).

Загальний опір розтіканню електричного струму заземлювача [11]:

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

$$= (14{,}9 \cdot 20{,}1)/(14{,}9 \cdot 0{,}55 + 7 \cdot 20{,}1 \cdot 0{,}53) = 3{,}56 \text{ Ом}.$$

де $\eta_П = 0{,}55$ – табличне значення коефіцієнта екранування з’єднуючої полоси [11].

Умова $R \leq R_{ЗН}$ виконується ($3{,}56 \leq 4$).

Остаточно кількість вертикальних електродів дорівнює 7.

За потреби можна зменшити кількість електродів заземлювача, зменшивши загальний опір розтіканню електричного струму заземлювача методом зменшення питомого опору ґрунту, домішуючи у ґрунт безпосередньо навколо електродів заземлювача розчини солей NaCl, CaCl, сажу, соду, шлак або спеціальні суміші.

7.5 Висновки до розділу

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

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

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

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

8 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

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 оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

– Досліджена система оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

– На основі отриманих результатів досліджень створена програмна реалізація системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання.

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. Швидкий Ю.Ю. Дослідження та програмна реалізація системи оцінки ризиків безпеки та виявлення аномалій у конфігураціях міжмережевих екранів із використанням машинного навчання // Збірник праць молодих науковців ЦНТУ. – Вип. 17. – Кропивницький: ЦНТУ, 2027.
2. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 p.
3. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.
4. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.
5. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.
6. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p
7. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.
8. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.
9. 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.
10. 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.
11. Смірнова Т.В., Усік П.С., Лисенко І.А., Буравченко К.О., Смірнов

О.А. «Методологія підтримки технологічних процесів у критичній інфраструктурі з забезпеченням безпеки інформації на основі хмарних технологій». *Безпека інформації.* 2025. Том 31 № 1. С. 49-60.

12. Смірнова Т.В., Буравченко К.О., Добринчук О.А., Смірнов С.А., Якименко Н.М., Смірнов О.А. «Хмарна технологія моніторингу ключових індикаторів ефективності технологічних процесів у критичній інфраструктурі». *Центральноукраїнський науковий вісник. Технічні науки.* 2025. № 12(43), ч. II. С. 36-54.

13. 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.

14. 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/

15. 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.

16. 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.

17. Chulinda L., Smirnov O., Shapenko L., Ustynova I., Bohatiuk I., Kelyp S. «The role of innovation in ensuring the safety of international civil aviation». *Ceur Workshop Proceedings,* 2025, 4024, pp. 530–542.

18. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А, Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.:

Видавничий центр “Кафедра”, 2025.– 320 с.

19. 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

20. 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.

21. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.

22. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.

23. 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.

24. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241.

25. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless*

Communication Systems, 2024, pp. 379–402.

26. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447.

27. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 2024. № 2(26), С. 170–188.

28. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка.* 2024. №4(24), С. 6-27.

29. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка.* 2024. №3(23), С. 111-131.

30. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології,* 2024, № 13, с. 28-35.

31. 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.

32. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings*, 2023, 3550, pp. 313-320.

33. 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

34. 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.

35. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings*, Volume 3504, 2023, pp. 1-11.

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. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». *Кібербезпека: освіта, наука, техніка*, №3(19), 2023, С. 176-196.

38. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». *II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи hозвитку інформаційних технологій (ІПШРІТ-2023)»* м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.

39. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». *VII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення,* м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.

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

листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.

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

42. 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,

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

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

45. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку,* 2022, № 3(69). С. 93-98.

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

47. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного

захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.

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

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

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

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

52. 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.

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

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

55. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A.,

Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 122-131.

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

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

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

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

60. 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.

61. 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.

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