Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інформаційно-аналітичних технологій та менеджменту
(повна назва)
Кафедра Інформатики
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

ДОСЛІДЖЕННЯ ТА РЕАЛІЗАЦІЯ МЕТОДІВ АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ НОВИХ ТИПІВ КІБЕРЗАГРОЗ

(тема)

Виконав:
студент 2 курсу, групи ІНФм-22-1
Стогній Д.Є.
(прізвище, ініціали)

Спеціальності 122 Комп'ютерні науки
(код і повна назва спеціальності)

Тип програми освітньо-професійна

Освітня програма Інформатика
(повна назва освітньої програми)

Керівник доц. Кобилін О.А.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Кобилін О.А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Інформаційно-аналітичних технологій та менеджменту
(повна назва)

Кафедра Інформатики
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма Інформатика
(повна назва освітньої програми)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Стогнію Дмитру Євгеновичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження та реалізація методів аналізу для виявлення нових типів кіберзагроз

затверджена наказом по університету від 3 листопада 2023 року № 1280Ст

2. Термін подання студентом роботи до екзаменаційної комісії 23 грудня 2023 р.

3. Вихідні дані до роботи науково-методична та науково-технічна література, матеріали конференцій, дані інтернет-мережі, статистичні моделі для аналізу поведінкових паттернів кіберзлочинців, алгоритми машинного навчання для прогнозування й виявлення аномалій у мережевому трафіку, огляд літератури щодо сучасних методів виявлення кіберзагроз, класифікація нових типів кіберзагроз та методи їх аналізу.

4. Перелік питань, що потрібно опрацювати в роботі
1. Огляд основних методів для виявлення нових типів кіберзагроз.
2. Математичні моделі виявлення кіберзагроз.
3. Майбутні тенденції та інновації у виявленні кіберзагроз.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) продуктивність мов програмування для аналізу даних, схема взаємодії модулів системи аналізу даних, графік часу виявлення загрози, діаграма, яка ілюструє потенційні інноваційні методи та технології у виявленні кіберзагроз.

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання на кваліфікаційну роботу	03.11.2023	
2	Аналіз завдання, підбір літератури	04.11.23-07.11.23	
3	Аналіз літератури з досліджуваної проблеми	07.11.23-16.11.23	
4	Аналіз технічних засобів	17.11.23-30.11.23	
5	Розробка методу	01.12.23-06.12.23	
6	Розробка прототипу	06.12.23-08.12.23	
7	Оформлення пояснювальної записки	08.12.23-10.12.23	
8	Перевірка на плагіат	11.12.2023	
9	Рецензування	21.12.2023	
10	Підготовка презентації та доповіді	25.12.2023	
11	Занесення роботи в електронний архів	02.01.2024	
12	Попередній захист кваліфікаційної роботи	02.01.2024	

Дата видачі завдання 3 листопада 2023 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Кобилін О.А.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ/ABSTRACT

Пояснювальна записка до кваліфікаційної роботи: 66 с., 7 табл., 4 рис., 47 джерел.

ЧАСОВІ РЯДИ, МОДЕЛЮВАННЯ ПОВЕДІНКИ, ТЕМАТИЧНИЙ АНАЛІЗ, КІБЕРЗАГРОЗИ, АНАЛІЗ ДАНИХ, БЕЗПЕКА ІНФОРМАЦІЇ, ПРОГНОЗУВАННЯ ЗАГРОЗ.

Об’єктом дослідження є мережевий трафік та логи систем, які часто містять приховані ознаки кіберзагроз.

Метою дослідження є розробка інноваційних методів аналізу часових рядів, моделювання поведінки та тематичного аналізу, які дозволять ідентифікувати потенційні кіберзагрози з більшою точністю та швидкістю.

Використано комплексний підхід, що включає методи часових рядів для аналізу тенденцій та патернів, моделювання поведінки для ідентифікації аномалій та тематичний аналіз для розуміння контексту загроз. Проведено глибокий аналіз сучасних кіберзагроз, виявлено ключові вектори атак та розроблено стратегії для їх виявлення та запобігання.

Результати дослідження спрямовані на підвищення ефективності систем кібербезпеки та забезпечення більш стійкого захисту від нових та еволюціонуючих загроз.

TIME SERIES, BEHAVIORAL MODELING, THEMATIC ANALYSIS, CYBER THREATS, DATA ANALYSIS, INFORMATION SECURITY, THREAT PREDICTION.

The object of research is network traffic and system logs, which often contain hidden signs of cyber threats.

The aim of the study is to develop innovative methods of time series analysis, behavior modeling, and thematic analysis that will allow for the identification of potential cyber threats with greater accuracy and speed.

A comprehensive approach was used, including time series methods for analyzing trends and patterns, behavioral modeling for anomaly detection, and thematic analysis for understanding the context of threats. An in-depth analysis of modern cyber threats was conducted, key attack vectors were identified, and strategies for their detection and prevention were developed.

The results of the study are aimed at increasing the effectiveness of cybersecurity systems and providing more resilient protection against new and evolving threats.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AR – AutoRegressive (авторегресивна модель)

ARMA – Autoregressive Moving Average (авторегресивна модель з ковзним середнім)

LSTM – Long Short-Term Memory (довга короткочасна пам'ять)

ARIMA – AutoRegressive Integrated Moving Average (інтегрована авторегресивна модель з ковзним середнім)

ARCH – Autoregressive Conditional Heteroskedasticity (авторегресивна умовна гетероскедастичність)

GARCH – Generalized Autoregressive Conditional Heteroskedasticity (узагальнена авторегресивна умовна гетероскедастичність)

RNN – Recurrent Neural Network (рекурентна нейронна мережа)

LDA – Latent Dirichlet Allocation (латентне діріхле розподілення)

ПЗ – програмне забезпечення

MA – Moving Average (ковзне середнє)

DDoS – Distributed Denial of Service (розподілена атака відмови у обслуговуванні)

CPU – Central Processing Unit (центральний процесор)

RAM – Random Access Memory (оперативна пам’ять)

CNN – Convolutional Neural Network (конволюційна нейронна мережа)

RNN – Recurrent Neural Network (рекурентна нейронна мережа)

DLN – Deep Learning Networks (мережі глибокого навчання)

API – Application Programming Interface (інтерфейс програмування додатків)

AWS – Amazon Web Services (хмарні сервіси Amazon)

UI – User Interface (інтерфейс користувача)

ШІ – штучний інтелект

МН – машинне навчання

IoT – Internet of Things (інтернет речей)

ВСТУП

У сучасному світі, де цифрові технології проникають у всі сфери життя, питання кібербезпеки набуває особливої актуальності. Зростання залежності від інформаційних систем та мережевих технологій веде до збільшення кількості та складності кіберзагроз [1–4]. Ці загрози постійно еволюціонують, стаючи більш хитромудрими та важковиявними. Враховуючи глобальні втрати від кіберзлочинності, які за оцінками досягають мільярдів доларів щороку, важливість розробки нових методів захисту є незаперечною.

Актуальність дослідження полягає у необхідності розробки ефективних методів аналізу, які дозволять виявляти нові типи кіберзагроз на ранніх стадіях та запобігати потенційним атакам. Особливу увагу варто приділити методам, що базуються на аналізі часових рядів, моделюванні поведінки та тематичному аналізі, оскільки вони дозволяють глибше зрозуміти природу та механізми кіберзагроз.

Метою даної роботи є дослідження та реалізація передових методів аналізу для виявлення нових типів кіберзагроз. Дослідження спрямоване на розробку комплексного підходу, який включатиме в себе різноманітні методи аналізу даних, з метою підвищення ефективності систем кібербезпеки та забезпечення більш надійного захисту від потенційних загроз.

У цьому контексті, робота розглядає історичний розвиток кіберзагроз, від простих вірусів до складних цілеспрямованих атак, які вимагають все більш витончених методів виявлення та нейтралізації. Значний акцент робиться на вивченні новітніх технологічних змін, таких як розвиток штучного інтелекту та машинного навчання, які відкривають нові можливості для кіберзахисту, але й створюють нові виклики.

Правовий аспект кібербезпеки також заслуговує на увагу, оскільки він визначає рамки, в яких можуть діяти фахівці та організації. Етичні дилеми, пов'язані з приватністю та наглядом, є невід’ємною частиною дискусії про кібербезпеку. Крім того, робота включає аналіз ризиків та методи оцінки

вразливостей, які є критично важливими для розробки ефективних захисних стратегій.

Міжнародна співпраця та обмін інформацією є ключовими для розуміння та протидії кіберзагрозам, що не знають кордонів. В цьому аспекті робота висвітлює необхідність глобальної взаємодії та координації зусиль [5].

Науковий внесок даної роботи полягає у розробці та апробації нових методів аналізу, які будуть інтегровані у системи кібербезпеки, тим самим підвищуючи їх ефективність. Робота структурована таким чином, щоб кожен розділ послідовно розкривав аспекти проблеми, від теоретичних основ до практичної реалізації розроблених методів.

1 ОГЛЯД ОСНОВНИХ МЕТОДІВ ДЛЯ ВИЯВЛЕННЯ НОВИХ ТИПІВ КІБЕРЗАГРОЗ

Від початку ери інформаційних технологій постійно виникають нові типи кіберзагроз. Для виявлення та протидії цим загрозам було розроблено численні методи, засновані на статистиці, машинному навчанні та інших підходах [6].

Ось декілька ключових методів:

– часові ряди: аналіз часових рядів дозволяє виявляти аномалії в поведінці системи на основі змін в паттернах даних протягом часу. Даний метод дозволяє виявляти незвичайну активність, що може вказувати на можливі кіберзагрози;

– моделювання поведінки: цей підхід базується на створенні моделі «нормальної» поведінки системи або користувача. Будь-яке відхилення від цієї моделі може вказувати на потенційну загрозу;

– машинне навчання: алгоритми машинного навчання можуть бути навчені виявляти паттерни атак на основі великих наборів даних про минулі інциденти безпеки. Вони можуть автоматично адаптуватися до нових загроз та виявляти їх в реальному часі;

– хешування та аналіз сигнатур: ці методи виявляють відомі шкідливі програми та загрози на основі їх «сигнатур» – унікальних властивостей або хешів файлів;

– пісочниці: системи пісочниці дозволяють запускати та аналізувати підозрілі програми в ізольованому середовищі, щоб визначити, чи мають вони шкідливу поведінку;

– тематичний аналіз: виявляє кіберзагрози на основі аналізу текстової інформації, наприклад, комунікацій між кіберзлочинцями.

Для ефективного виявлення кіберзагроз необхідно комбінувати різні методи та підходи. Наразі немає універсального рішення, яке б гарантувало

повне виявлення всіх можливих загроз, але правильно налаштована комбінація методів може суттєво підвищити рівень безпеки системи [7].

В даному дослідженні розглянуто декілька з них.

1.1 Часові ряди, огляд та основні поняття

Часові ряди (Time Series) – це послідовність точок даних, виміряних в певні моменти часу, зазвичай в однакових інтервалах, розташованих в належному хронологічному порядку. Вони можуть бути отримані в різних областях, таких як фінанси, економіка, медицина, метеорологія, технічне обслуговування та багато інших. У кібербезпеці це може бути, наприклад, кількість запитів до сервера за хвилину, кількість входів у систему або кількість переданих пакетів даних. Часові ряди можуть допомогти виявити аномалії в даних, які відображають можливі атаки або нові види загроз.

Особливість аналізу часових рядів полягає в тому, що розглядаються виключно отримані результати спостережень без залучення додаткових даних чи розгляду впливу зовнішніх чинників. Хоча такий підхід може здатися обмеженим, в реальній практиці прогнози, засновані на часових рядах, часто виявляються високоточними.

$$X_t = (x_1, x_2, x_3, \dots, x_t)\,, \tag{1.1}$$

де X_t – значення часового ряду у момент часу *t*;

$x_1, x_2, x_3, \dots, x_t$ – спостереження часового ряду.

Цей набір даних складається з числових показників, де кожному значенню призначено певний індекс на основі періоду, протягом якого його було зафіксовано [8].

1.1.1 Основні характеристики часових рядів

Основні характеристики часових рядів відображають ключові аспекти та структурні компоненти, які формують ці послідовності даних. Ці характеристики допомагають аналітикам і дослідникам зрозуміти поведінку та динаміку часових рядів, а також розробляти моделі для прогнозування та аналізу.

Ось деякі з основних характеристик часових рядів:

– часова компонента. Головна відмінність часових рядів від інших даних – це їхній часовий вимір. Кожне спостереження у часовому ряді зв’язане з конкретним моментом в часі, що дозволяє аналізувати зміни в динаміці;

– спостереження. Кожне спостереження в часовому ряді представляє конкретне значення в певний момент часу. Вони слугують записами, які можуть відображати все: від кількості звернень до вебсервера до кількості проданих товарів;

– структура і залежності. Велика частина аналізу часових рядів базується на виявленні структур і залежностей у даних. Ці залежності можуть бути автокореляційними, коли значення змінної в один момент часу залежить від її попередніх значень;

– сезонність та тренди. Багато явищ у природі та в економіці мають періодичний характер. Це може бути температурна сезонність, святкові продажі в роздрібному бізнесі або пікові навантаження на вебсервер в певний час дня. Тренди вказують на стійкі зміни у часі, наприклад, збільшення кількості користувачів Інтернету протягом десятиліть;

– шум і випадковість. Не всі зміни у часовому ряді мають змістовне пояснення. Деякі коливання можуть бути випадковими або викликаними непередбаченими подіями. Розрізнення «сигналу» від «шуму» є ключовим елементом аналізу часових рядів;

– стійкість. Для багатьох методів прогнозування важливо, щоб часовий ряд був стійким, тобто його статистичні характеристики не змінювалися з часом. Якщо ряд не є стійким, його можна перетворити, наприклад, за допомогою диференціювання;

– лаги (затримки). В контексті часових рядів лаги представляють попередні значення в часовому ряді. Вони важливі для визначення автокореляції і використовуються в моделях, таких як авторегресійна модель (AR) або модель авторегресії з ковзаючим середнім (ARMA).

Враховуючи ці характеристики, можна більш ефективно працювати з часовими рядами і використовувати їх для аналізу та прогнозування в різних областях, включаючи кібербезпеку [9].

В контексті кібербезпеки, аналіз часових рядів може допомогти ідентифікувати зловмисну активність, виходячи з відхилень від відомих шаблонів поведінки. Техніки, такі як ARIMA та LSTM, є дуже корисними для виявлення цих відхилень і прогнозування майбутніх кіберзагроз.

Використання часових рядів у кібербезпеці дає можливість професіоналам своєчасно виявляти, моніторити та реагувати на потенційно шкідливі дії.

1.1.2 Використання часових рядів в кібербезпеці

Використання часових рядів у кібербезпеці полягає в аналізі послідовностей даних, записаних через визначені інтервали часу, з метою виявлення зразків, аномалій або інших характеристик, які можуть свідчити про зловмисну активність або потенційні загрози. Цей підхід дозволяє експертам з кібербезпеки отримувати глибше розуміння поведінки системи та взаємодії користувачів з нею, що, в свою чергу, сприяє своєчасному виявленню та реагуванню на можливі кіберзагрози.

Використання часових рядів як методу дослідження та виявлення нових типів кіберзагроз може бути дуже корисним, оскільки кіберзагрози і кібератаки також мають свої часові залежності та структури.

Розглянемо декілька способів, які можна використовувати для аналізу часових рядів для кібербезпеки:

– виявлення аномалій. Часові ряди можуть використовуватися для виявлення аномальних або незвичайних подій в мережах та системах. Наприклад, аномальні зміни в трафіку, підвищення обсягу запитів або зниження активності користувачів можуть бути показниками можливих кіберзагроз;

– прогнозування атак. Аналіз часових рядів може допомогти у прогнозуванні майбутніх кібератак або кіберзагроз. Шляхом аналізу попередніх атак та їхніх часових залежностей можна спробувати передбачити подібні атаки у майбутньому;

– відновлення даних. Важливим аспектом виявлення кіберзагроз є відновлення даних після атаки або витоку даних. Часові ряди можуть допомогти у відновленні та аналізі втрачених або пошкоджених даних;

– моніторинг поведінки. Встановлення базової лінії поведінки системи або мережі шляхом аналізу часових рядів може допомогти виявити будь-які незвичайні або недоречні дії, які можуть бути зумовлені кіберзагрозами;

– реагування на інциденти. Якщо виявлено підозрілу активність, аналіз часових рядів може бути використаний для швидкого реагування на кіберзагрози, що допомагає запобігти подальшим атакам та обмежити можливі збитки.

Для успішного використання аналізу часових рядів у сфері кібербезпеки вкрай важливо мати доступ до обширної бази даних та застосовувати складні методи аналізу, включаючи статистичні моделі, машинне навчання та методи глибокого навчання. Такі підходи можуть значно покращити виявлення тонких шаблонів та аномалій, які можуть свідчити про нові типи кіберзагроз. Аналізуючи тенденції та поведінку протягом часу, можна не лише

ідентифікувати існуючі загрози, але й прогнозувати та запобігати майбутнім вразливостям та атакам. Така проактивна позиція у сфері кібербезпеки може призвести до розробки більш надійних механізмів захисту та забезпечити вищий рівень безпеки у все більш цифровизованому світі.

1.1.3 Основні методи аналізу часових рядів

Аналіз часових рядів – це спеціалізований підсектор статистики та математичного аналізу, який зосереджений на вивченні послідовностей даних, зібраних за певні часові інтервали. Ключова особливість таких даних – наявність часового виміру, завдяки якому можна вивчати зміни в часі.

Мета аналізу часових рядів – розглядати та інтерпретувати закономірності, тренди, цикличність та інші характеристики у даних, що змінюються в часі. Такий аналіз може використовуватися для різних цілей, зокрема для:

– вивчення причинно-наслідкових зв’язків (чи є зв’язок між часовим рядом одного показника і іншого?);

– прогнозування майбутніх значень (як, наприклад, прогноз погоди або прогноз продажів);

– виявлення аномалій або несподіваних подій.

Аналіз часових рядів включає в себе широкий спектр методів і технік, що дозволяють ефективно працювати з даними, що мають часову структуру:

– декомпозиція. Це розкладання часового ряду на його основні складові: тренд, сезонність та випадкові відхилення. Декомпозиція допомагає зрозуміти структуру часового ряду та його основні характеристики;

– методи експоненційного згладжування. Основна ідея полягає в присвоєнні ваг попереднім спостереженням таким чином, щоб більш нещодавні спостереження мали більший вплив на прогноз. Метод Хольта-

Вінтерса враховує тренд і сезонність, роблячи його ефективним для рядів з явною періодичністю;

– ARIMA (Авторегресійний інтегрований ковзний середній). ARIMA – це статистична модель, яка використовує різницю для виведення стаціонарності ряду і потім використовує авторегресійні та ковзні середні компоненти для моделювання ряду;

– моделі ARCH і GARCH. Ці моделі призначені для моделювання волатильності часових рядів, в основному для фінансових ринкових даних. Вони можуть враховувати постійно змінний рівень волатильності;

– методи машинного навчання. Застосування алгоритмів машинного навчання до часових рядів може включати в себе використання регресії, класифікації, а також глибокого навчання. Нейронні мережі, особливо рекурентні нейронні мережі (RNN), є ефективними для прогнозування часових рядів;

– вейвлет-аналіз. Вейвлети дозволяють розглядати часові ряди на різних масштабах, виділяючи особливості як високої, так і низької частоти в даних [10–13];

– виявлення аномалій. Виявлення аномалій в часових рядів включає в себе ідентифікацію даних точок, які відрізняються від очікуваного шаблону або поведінки. Це може вказувати на несподівані події або зміни в системі;

– методи спектрального аналізу. Ці методи аналізують частотні компоненти часового ряду, допомагаючи визначити домінуючі цикли або сезонні впливи в даних.

1.2 Моделювання поведінки, огляд та основні поняття

Моделювання поведінки – це метод, призначений для визначення «нормальних» шаблонів поведінки систем, користувачів або додатків. Це

засновано на ідеї, що аномалії або відхилення від цих шаблонів можуть вказувати на потенційні загрози або вторгнення [14, 15].

Основні характеристики:

– базова лінія: визначення стандартного або «нормального» шаблону поведінки на основі історичних даних;

– адаптивність: здатність до автоматичного оновлення моделі з урахуванням нових даних;

– чутливість: здатність виявляти мінімальні відхилення від нормального поведінкового шаблону;

– візуалізація: здатність візуалізувати поведінкові шаблони та аномалії для аналізу.

Моделювання поведінки стає ключовим інструментом в кібербезпеці, оскільки традиційні методи захисту, такі як антивіруси і мережеві фільтри, можуть не виявляти нові або адаптивні загрози [16].

Використовуючи поведінкові моделі, фахівці з безпеки можуть:

– виявляти незвичайну активність, яка відбивається від стандартних шаблонів;

– прогнозувати можливі майбутні загрози на основі змін в поведінці;

– визначати «внутрішніх загрозників» – співробітників, які можуть вчиняти дії, які шкодять організації.

Основні методи аналізу:

– статистичний аналіз. Використовує статистичні методи для визначення аномалій у поведінці;

– машинне навчання. Використовується для навчання моделей на основі історичних даних, так що вони можуть автоматично виявляти аномалії;

– хеп-мапи. Візуальний інструмент для виявлення аномалій в поведінці, порівнюючи їх зі стандартними шаблонами;

– груповий аналіз. Виявляє групи схожої поведінки та визначає, які групи відхиляються від «нормальної» активності.

Коли правильно застосовується, моделювання поведінки може стати могутнім інструментом для збільшення кібербезпеки, допомагаючи організаціям виявляти та реагувати на загрози в реальному часі [17].

1.3 Тематичний аналіз, огляд та основні поняття

Тематичний аналіз – це метод кваліативного дослідження, що дозволяє ідентифікувати, аналізувати та інтерпретувати шаблони (теми) в даних. Він часто використовується для аналізу текстових даних, наприклад в контент-аналізі.

Основні характеристики:

– гнучкість: метод може бути застосований до різноманітних даних та контекстів;

– інтерпретаційність: дозволяє глибоко розуміти зміст даних, виявляючи основні ідеї та концепції;

– виявлення шаблонів: шукає зв’язки між різними частинами даних для ідентифікації головних тем.

У контексті кібербезпеки тематичний аналіз може бути корисним для:

– аналізу логів та записів, щоб виявити основні теми або патерни в поведінці системи чи користувача [18];

– виявлення потенційних загроз або атак на основі аналізу комунікацій або контенту в соціальних мережах;

– аналіз форумів та інших платформ, де хакери можуть обговорювати атаки або ділитися інструментами.

Основні методи аналізу:

– ручний аналіз: дослідники проаналізують даний контент, шукаючи ключові теми та ідеї;

– комп’ютерне тематичне моделювання: використання алгоритмів машинного навчання, таких як LDA (латентне діріхле розподілення), для ідентифікації тем в текстових даних;

– кодування: процес призначення міток або кодів конкретним частинам тексту, що представляють конкретні теми або ідеї.

Застосовуючи тематичний аналіз у сфері кібербезпеки, фахівці можуть отримати глибше розуміння потенційних загроз, а також виявляти нові шаблони чи тенденції в поведінці атакуючих або систем.

1.4 Традиційні методи виявлення кіберзагроз

Традиційні методи виявлення кіберзагроз базуються на використанні відомих сигнатур або відбитків загроз. Ці методи працюють за принципом відповідності: якщо вхідний потік даних або поведінка системи відповідає відомій сигнатурі загрози, система виявлення втручається.

Основні характеристики традиційних методів:

– сигнатурне виявлення: це найпоширеніший підхід, який використовується більшістю антивірусних програм. Він порівнює файл або код із відомими сигнатурами вірусів або шкідливого ПЗ;

– поведінковий аналіз: замість того, щоб шукати відомі сигнатури, цей метод аналізує поведінку програми, щоб визначити, чи є вона шкідливою;

– хеврістичний аналіз: цей метод використовує алгоритми для визначення невідомих вірусів або нових варіантів відомих вірусів шляхом аналізу коду на наявність підозрілих властивостей.

Переваги традиційних методів:

– висока швидкість виявлення відомих загроз;

– менший ризик помилкового позитивного виявлення порівняно з іншими методами.

Недоліки традиційних методів:

– нездатність виявляти нові або модифіковані загрози, які не мають відомих сигнатур;

– потреба в постійних оновленнях бази даних сигнатур для забезпечення актуальності захисту;

– велика кількість ресурсів, необхідних для підтримки та оновлення баз сигнатур.

Таким чином, хоча традиційні методи є ефективними для виявлення відомих загроз, вони можуть бути менш ефективними проти нових або невідомих загроз.

1.5 Постановка задачі дослідження

У світі, де кіберінфраструктура стає все більш складною та взаємопов’язаною, здатність ефективно виявляти нові типи кіберзагроз є вирішальною для забезпечення безпеки інформаційних систем. Сучасні методи виявлення часто виявляються недостатніми перед обличчям швидко змінюваних і все більш витончених атак, що вимагає розробки нових, більш адаптивних та передбачувальних підходів.

Основна увага буде приділена визначенню ключових дослідницьких питань та формулюванню гіпотез, які будуть перевірені в ході подальшого дослідження. Також буде окреслено методологію, яка буде використана для досягнення поставлених цілей, та обговорено потенційні обмеження, які можуть вплинути на дослідження [19].

Об’єктом дослідження є мережевий трафік та логи систем, які часто містять приховані ознаки кіберзагроз.

Метою дослідження є розробка інноваційних методів аналізу часових рядів, моделювання поведінки та тематичного аналізу, які дозволять ідентифікувати потенційні кіберзагрози з більшою точністю та швидкістю.

Для досягнення цієї мети передбачається вирішити наступні завдання:

– провести аналіз сучасних методів виявлення кіберзагроз з використанням часових рядів, моделювання поведінки та тематичного аналізу;

– розробити алгоритми для аналізу часових рядів, які зможуть виявляти аномалії в мережевому трафіку;

– реалізувати моделі поведінки на основі марківських процесів та нейронних мереж для ідентифікації аномальних дій користувачів;

– застосувати тематичний аналіз з використанням моделі LDA для класифікації текстових даних та виявлення потенційних кіберзагроз;

– реалізувати комп’ютерну модель, яка інтегрує ці методи для виявлення нових типів кіберзагроз.

2 МАТЕМАТИЧНІ МОДЕЛІ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

В сучасному світі, де інформація стає одним з найцінніших ресурсів, захист цифрових систем від кіберзагроз набуває особливої актуальності. Виявлення кіберзагроз на ранніх стадіях є ключовим етапом у запобіганні потенційним атакам та мінімізації збитків. Однак, завдяки постійному розвитку та адаптації методів нападу з боку зловмисників, виявлення кіберзагроз стає все більш складним завданням. У цьому контексті математичне моделювання виступає як потужний інструмент для систематизації, аналізу та прогнозування потенційних загроз.

Цей розділ присвячений дослідженню основних математичних моделей, які використовуються для виявлення кіберзагроз. Особлива увага приділяється трем основним методам: аналізу часових рядів, моделюванню поведінки та тематичному аналізу. Кожен з цих методів має свої унікальні особливості, переваги та обмеження, що робить їх підходящими для різних типів даних та сценаріїв використання. Поглиблене розуміння цих моделей дозволить краще оцінити їх потенцій та обрати найбільш ефективний підхід для конкретних задач виявлення кіберзагроз [20].

2.1 Часові ряди та їх властивості

Часові ряди є одним з найдавніших методів аналізу даних. Давні цивілізації, такі як древній Єгипет чи Вавилон, використовували просторові наміри, такі як рух зірок або рівень води в ріках, для прогнозування погоди або сезонних змін. Сучасний науковий підхід до часових рядів розпочався у 19 та на початку 20 століття з розвитком статистики і теорії ймовірностей.

У 20-му столітті, з ростом комп’ютерної техніки та доступності великих обсягів даних, методи аналізу часових рядів стали більш досконалими. Нові

математичні моделі, такі як ARIMA, були розроблені для більш точного прогнозування та аналізу динаміки часових рядів.

Часовий ряд – це набір спостережень, зібраних в певні моменти часу, зазвичай в регулярних інтервалах. Основна мета аналізу часових рядів – вивчення внутрішньої структури таких даних, виявлення закономірностей, трендів, сезонності, циклічних змін і інших компонентів [21].

Основні компоненти часового ряду:

– тренд (T): систематичний лінійний чи нелінійний компонент, який відображає довгострокову зміну ряду в часі;

– сезонність (S): відображає систематичні флуктуації, які відбуваються з регулярним інтервалом (наприклад, щоденно, щомісячно);

– циклічність (C): флуктуації, які виникають з нерегулярними інтервалами і можуть бути викликані економічними циклами;

– випадкова складова (I): непередбачувані відхилення в даних, які не можуть бути описані вищевказаними компонентами.

Основні методи аналізу часових рядів діляться на дві категорії:

– методи в часовому просторі: зосереджені на аналізі даних у часовому діапазоні (наприклад, ARIMA);

– методи в частотному просторі: аналізують даних на основі частотних характеристик (наприклад, спектральний аналіз).

Сучасний аналіз часових рядів використовує як традиційні статистичні методи, так і новітні підходи, зокрема на основі машинного навчання, що дозволяє глибше розуміти динаміку даних і робити більш точні прогнози.

2.1.1 AR, MA і ARIMA моделі, детальний аналіз

AR (AutoRegressive) модель або авторегресійна модель базується на принципі, що поточне значення часового ряду може бути виражене через попередні значення з деякою лінійною комбінацією.

Математично:

$$X_t = c + \phi_1 X_{t-1} + \phi_2 X_{t-2} + \ldots + \phi_p X_{t-p} + \varepsilon_t, \quad (2.1)$$

де X_t – поточне значення часового ряду;

c – константа;

ϕ – коефіцієнти авторегресії;

p – порядок моделі;

ε_t – білий шум (помилка).

Приклад: припустимо, ми моніторимо мережевий трафік в організації і спостерігаємо певну кількість зовнішніх спроб з'єднань до нашої системи протягом певного часу. Модель AR може бути використана для прогнозування кількості спроб з'єднань на наступний день, враховуючи попередні дані.

MA (Moving Average) модель або модель ковзного середнього використовує середнє значення попередніх помилок для прогнозування поточного значення.

Математично:

$$X_t = \mu + \varepsilon_t + \theta_1 \varepsilon_{t-1} + \theta_2 \varepsilon_{t-2} + \ldots + \theta_q \varepsilon_{t-q}\ , \quad (2.2)$$

де X_t – поточне значення часового ряду;

μ – середнє значення ряду;

ϕ – коефіцієнти;

p – порядок моделі;

ε_t – білий шум (помилка).

Приклад: якщо ми використовуємо систему виявлення вторгнень і помітили, що є систематична помилка (наприклад, часті ложні тривоги) в останніх декількох спостереженнях, модель MA може допомогти скоригувати

систему на основі цих помилок, щоб уникнути таких ложних тривог в майбутньому.

ARIMA (AutoRegressive Integrated Moving Average) модель комбінує AR і MA підходи і включає в себе додатковий крок інтеграції (I), який допомагає моделі враховувати тренди в даних.

Математично:

$$(1 - \sum_{i=1}^{p} \phi_i L^i)(1 - L)^d X_t = \mu + (1 + \sum_{i=1}^{q} \theta_i L^i)\, \varepsilon_t\,, \qquad (2.3)$$

де X_t – поточне значення часового ряду;

ϕ_i – коефіцієнти авторегресії;

L – оператор затримки (Lag operator). Застосовуючи його до часового ряду, ми отримуємо попереднє значення ряду;

d – порядок інтеграції. Він показує, скільки разів потрібно взяти різницю між спостереженнями, щоб отримати стаціонарний часовий ряд;

μ – середнє значення ряду;

θ_i – коефіцієнти ковзного середнього;

ε_t – порядок інтеграції. Він показує, скільки разів потрібно взяти різницю між спостереженнями, щоб отримати стаціонарний часовий ряд.

Ця формула представляє собою комбіновану модель ARIMA, де AR частина визначається коефіцієнтами ϕ_i, частина I визначається порядком інтеграції d, а частина MA визначається коефіцієнтами θ_i. Модель ARIMA використовується для прогнозування часових рядів, що мають як авторегресійні, так і ковзаючі середні компоненти, а також коли ряд потребує диференціювання для досягнення стаціонарності.

Приклад: припустимо, у нас є логи безпеки, які відображають кількість спроб атак на систему щодня. Ці дані можуть мати як довгострокові тренди (збільшення атак з часом), так і сезонність (більше атак в кінці місяця). ARIMA може бути використана для прогнозування майбутньої активності на

основі цих патернів, допомагаючи команді безпеки краще готуватися до можливих загроз.

Ці приклади показують, як моделі часових рядів можуть бути використані в контексті кібербезпеки для прогнозування та аналізу мережевої активності та інших пов’язаних з безпекою подій.

2.1.2 Інші моделі часових рядів, такі як GARCH

GARCH є розширенням моделі ARCH (Autoregressive Conditional Heteroskedasticity) і використовується для моделювання і прогнозування волатильності часових рядів. Волатильність тут означає міру варіативності часового ряду, і вона може змінюватися в часі.

В контексті кібербезпеки GARCH може бути корисною для аналізу логів або мережевого трафіку, де ви хочете зрозуміти, чи збільшується волатильність атак або спроб вторгнень з часом.

Математична формула GARCH(p, q) виглядає так:

$$\sigma_t^2 = \alpha_0 + \sum_{i=1}^{p} \alpha_i \, \varepsilon_{t-i}^2 + \sum_{j=1}^{q} \beta_j \, \sigma_{t-j}^2, \tag{2.3}$$

де σ_t^2 – прогнозована волатильність на момент часу t;

ε_{t-i}^2 – квадрат значення відхилення на $t-i$ момент часу (це ARCH частина);

σ_{t-j}^2 – прогнозована волатильність на $t-j$ момент часу (це GARCH частина);

α_0, α_i, β_j – параметри моделі, які оцінюються з допомогою методу максимальної правдоподібності.

Приклад у контексті кібербезпеки: можемо використовувати GARCH для моделювання волатильності кількості спроб вторгнень у мережеву систему. Якщо волатильність зростає, це може свідчити про посилення атак або про те, що атакуючі стали більш активними. З іншого боку, якщо волатильність зменшується, це може свідчити про те, що заходи безпеки ефективно працюють або атакуючі втратили інтерес до системи.

2.1.3 Використання методу у контексті виявлення кіберзагроз

Відомо, що часові ряди – це послідовність точок даних, взятих з рівними інтервалами часу. У контексті кібербезпеки вони можуть бути корисними для виявлення аномалій або незвичайних патернів поведінки. Розглянемо декілька ключових застосувань.

Мережевий трафік є ключовим джерелом даних у кібербезпеці. Через регулярний аналіз мережевого трафіку можна виявляти зміни в паттернах, які вказують на потенційні атаки:

– DDoS атаки: однією з основних загроз є DDoS атаки, коли велика кількість запитів відправляється до сервера, спробуючи його «прикласти». Часові ряди допоможуть виявити раптове збільшення трафіку;

– незвичайний вихідний трафік: несанкціоноване витікання даних може бути виявлене через спостереження за несподіваним великим об’ємом вихідного трафіку.

Логи систем можуть відображати детальну активність користувачів і процесів. Часові ряди допоможуть виявити зміни в цих паттернах:

– несанкціонований доступ. Якщо користувач, який зазвичай працює вдень, раптом починає заходити в систему о півночі, це може вказувати на компрометацію облікового запису;

– часті помилки входу. Раптове збільшення помилок входу може свідчити про спроби брутфорс-атаки.

Шкідливе програмне забезпечення може створювати характерні паттерни активності, які можна виявити з допомогою часових рядів:

– споживання ресурсів. Значне збільшення використання CPU або RAM може вказувати на наявність шкідливого ПЗ;

– спостереження за мережевою активністю. Шкідливі програми можуть часто спілкуватися з командно-контрольними серверами, створюючи характерний паттерн мережевої активності.

Моделі часових рядів можуть допомогти не тільки виявляти, але і прогнозувати майбутні атаки:

– прогнозування пікових навантажень: З допомогою моделей, як-от ARIMA або GARCH, можливо прогнозувати моменти пікового навантаження на серверах, які можуть свідчити про плановані DDoS атаки;

– аналіз сезонності: Деякі атаки мають сезонний характер, і з допомогою часових рядів можна виявити та прогнозувати ці періоди.

Часові ряди відіграють ключову роль у сучасних системах кібербезпеки. З допомогою математичних моделей часових рядів можливо аналізувати динаміку різних видів даних, виявляти аномалії та прогнозувати потенційні загрози.

Моніторинг мережевого трафіку дозволяє вчасно виявляти такі загрози, як DDoS атаки, а також незвичайний вихідний трафік, що може вказувати на несанкціоноване витікання даних. Логи систем, зокрема, дозволяють слідкувати за діями користувачів та процесів, виявляючи спроби несанкціонованого доступу або брутфорс-атаки.

Важливим аспектом є також виявлення шкідливого ПЗ, яке може демонструвати специфічні паттерни активності, що відрізняються від нормальної роботи системи. І, нарешті, велику роль відіграє здатність прогнозування майбутніх атак на основі історичних даних та математичних моделей.

Таким чином, інтеграція методів часових рядів у системи кібербезпеки може суттєво підвищити ефективність виявлення та протидії кіберзагрозам.

Для подальшого вдосконалення систем кібербезпеки важливо досліджувати нові методи та алгоритми обробки часових рядів, адаптуючи їх до специфіки цієї області.

2.2 Моделювання поведінки в контексті кібербезпеки

Моделювання поведінки розглядається як методологічний підхід, спрямований на вивчення та передбачення поведінки індивідів, груп або систем. Цей підхід ґрунтується на спостереженнях та аналітичному аналізі минулої діяльності з метою виявлення паттернів і тенденцій, які дозволяють прогнозувати майбутні дії.

Визначення «нормальної» поведінки є критичним компонентом цього процесу. Це визначення може бути засноване на історичних даних, експертних оцінках або їх комбінації. Після встановлення базового рівня «нормальної» поведінки здійснюється збір релевантних даних, таких як журнали активності користувачів, метрики системи чи параметри мережевого трафіку.

За допомогою статистичних та аналітичних методів проводиться детальний аналіз даних, спрямований на виявлення конкретних паттернів та тенденцій в поведінці. З отриманими результатами розробляються моделі, які дозволяють не лише аналізувати минулу поведінку, а й прогнозувати майбутні дії.

Моделювання поведінки в контексті кібербезпеки є стратегією, спрямованою на ідентифікацію, виявлення та реагування на підозрілі або аномальні дії, вчинені в системі або мережі. Цей підхід базується на попередньому вивченні «нормального» поведінкового профілю користувача або системи для виявлення відхилень.

Основною ідеєю моделювання поведінки є те, що атаки або порушення безпеки зазвичай призводять до зміни поведінки. Наприклад, користувач, який зазвичай переважно працює з офісними документами, раптом може почати

завантажувати великі обсяги даних або звертатися до конфіденційних ресурсів [22].

Моделювання поведінки може бути використано в різних областях кібербезпеки, таких як:

– виявлення інсайдерських загроз: ідентифікація співробітників, які можуть виконувати дії, що шкодять організації;

– аналіз мережевого трафіку: виявлення аномальних паттернів, які можуть вказувати на DDoS атаки або інший маліційний трафік;

– аутентифікація користувача: лодаткова перевірка ідентичності на основі поведінкових характеристик, таких як швидкість введення тексту або звичні дії після авторизації.

Важливо підкреслити, що моделі поведінки мають динамічний характер. Оскільки поведінка може змінюватися відповідно до зміни зовнішніх умов, моделі повинні бути гнучкими, адаптивними і підлягати постійному вдосконаленню. Такий підхід дозволяє вчасно реагувати на потенційні загрози або виклики, адаптуючись до постійно змінюваних обставин.

Використання моделювання поведінки в кібербезпеці може значно підвищити здатність системи виявляти нові та невідомі загрози, адаптуючись до змінюваних умов та забезпечуючи більш глибокий рівень захисту [23].

2.2.1 Математична модель

Математична модель моделювання поведінки, в контексті кібербезпеки, зазвичай базується на статистичних методах і має на меті виявлення аномалій у поведінці. Ось спрощений приклад такої моделі, що використовує метод густини ймовірності.

Дані: логи активності користувача, де для кожного користувача відомі часові рамки його дій (наприклад, час входу в систему).

Мета: визначити, чи є конкретна дія користувача аномальною на основі його попередньої поведінки.

Етап навчання:

а) для кожного користувача розраховуємо середнє (μ) і стандартне відхилення (σ) часу його дій;

б) за допомогою цих параметрів формуємо нормальний розподіл для кожного користувача.

Етап тестування:

а) для нової дії користувача розраховуємо ймовірність цієї дії на основі його нормального розподілу;

б) якщо ймовірність менша за певний поріг (наприклад, 5%), вважаємо цю дію аномальною.

Математично це можна виразити наступним чином:

Для даної дії з часом t, ймовірність $P(t)$ обчислюється за формулою нормального розподілу:

$$P(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(t-\mu)^2}{2\sigma^2}}, \quad (2.4)$$

де $P(t)$ – це густина ймовірності для конкретного значення t;

σ – стандартне відхилення набору даних;

μ – середнє арифметичне набору даних;

e – це число Ейлера (приблизно рівне 2,71828), основа натуральних логарифмів.

Розглянемо кожну частину формули:

– коефіцієнт масштабування: $\frac{1}{\sigma\sqrt{2\pi}}$. Цей коефіцієнт гарантує, що інтеграл (або площа під кривою) графіка розподілу дорівнює 1. Він адаптує густину ймовірності таким чином, щоб вона відповідала дійсним даним.

– експоненційна частина: $e^{-\frac{(t-\mu)^2}{2\sigma^2}}$. Ця частина відповідає за форму дзвоника нормального розподілу. Вона забезпечує, що значення ближчі до середнього (μ) мають вищу ймовірність, і зменшується ймовірність для значень, що віддалені від середнього.

Якщо $P(t) < 0{,}05$ (або інший вибраний поріг), то дія вважається аномальною.

Таким чином, ця формула дозволяє вам визначити ймовірність конкретного значення t на основі відомих параметрів нормального розподілу (σ і μ). У контексті кібербезпеки і моделювання поведінки це може бути використано для визначення ймовірності певної поведінки користувача, базуючись на його попередньому поводженні.

Ця модель є дуже спрощеною та базовою. В реальних системах виявлення кіберзагроз можуть використовуватися більш складні моделі, які враховують додаткові параметри та використовують методи машинного навчання.

2.2.2 Модель на основі марківських процесів

Марківські процеси – це математичні моделі, які описують системи, що переходять з одного стану в інший. Основна ідея полягає в тому, що наступний стан системи залежить лише від її поточного стану, а не від шляху, яким система досягла цього стану [24].

Основними компонентами марківської моделі є:

– множина можливих станів;

– ймовірності переходу між цими станами.

Для кібербезпеки можна використовувати марківські процеси для моделювання поведінки користувачів або системи. Наприклад, поведінка

користувача може бути представлена як послідовність дій: вхід в систему, виконання завдань, завантаження файлів тощо.

Приклад використання в кібербезпеці: розглянемо систему моніторингу поведінки користувача. Ми хочемо визначити, чи є послідовність дій користувача підозрілою.

Стани:

– авторизація;
– завантаження файлу;
– зміна налаштувань;
– вихід.

Матриця переходів (приклад показано у таблиці 2.1).

Таблиця 2.1 – Процес кодування у тематичному аналізі

	Авторизація	**Завантаження файлу**	**Зміна налаштувань**	**Вихід**
Авторизація	0,1	0,6	0,2	0,1
Завантаження файлу	0,05	0,1	0,7	0,15
Зміна налаштувань	0,1	0,1	0,1	0,7
Вихід	0	0	0	1

Аналіз: якщо користувач після авторизації безпосередньо переходить до завантаження великої кількості файлів, при цьому ігноруючи зміну налаштувань або інші типові дії, це може бути підозрілою активністю.

За допомогою матриці переходів можна визначити ймовірність певної послідовності дій і порівняти її із пороговим значенням для виявлення аномалій.

Марківські процеси можуть бути дуже корисними у кібербезпеці, допомагаючи визначати аномальну поведінку на основі статистичного аналізу поведінки користувача або системи.

2.2.3 Нейронні мережі: основи, архітектури, тренування та використання для виявлення аномалій

Нейронні мережі є потужним інструментом машинного навчання, який використовується в широкому спектрі застосувань, включаючи виявлення аномалій в кібербезпеці.

Нейронна мережа – це мережа штучних нейронів, які моделюються на основі біологічних нейронів. Центральна концепція полягає в тому, щоб використовувати зважені суми вхідних даних, перетворити їх за допомогою функції активації і потім передавати результат наступному шару [25].

Є різні архітектури нейронних мереж:

– повнозв’язні мережі (Feedforward Neural Networks): прості мережі без циклів, де інформація рухається від входу до виходу;

– конволюційні нейронні мережі (CNN): популярні в області обробки зображень завдяки їхній здатності автоматично та адаптивно вчити просторові ієрархії ознак;

– рекурентні нейронні мережі (RNN): здатні обробляти послідовності даних, роблячи їх корисними для обробки тексту чи часових рядів;

– мережі глибокого навчання (DLN): складаються з великої кількості шарів, що дозволяє їм вчити дуже складні залежності.

Тренування нейронної мережі полягає в адаптації її ваг таким чином, щоб мінімізувати помилку передбачення на навчальних даних. Для цього зазвичай використовують метод зворотного розповсюдження помилки і оптимізаційні алгоритми, такі як стохастичний градієнтний спуск.

Нейронні мережі можуть виявляти аномалії в даних завдяки їхній здатності виявляти нетипові шаблони. Конкретно, мережі можуть бути натреновані на «нормальних» даних, а потім використані для виявлення відхилень від цього «нормального» стану. Це особливо корисно в кібербезпеці, де аномалії можуть вказувати на потенційні загрози або атаки.

2.3 Тематичний аналіз у контексті виявлення кіберзагроз

Тематичний аналіз – це метод дослідження, який призначений для ідентифікації, аналізу та звіту про шаблони (теми) у даних. Він зазвичай використовується для аналізу текстових даних. У контексті кібербезпеки, цей метод може бути корисним для аналізу логів, комунікацій та інших текстових даних з метою виявлення потенційних загроз [26].

Традиційно тематичний аналіз зосереджується на ручному кодуванні даних, однак із розвитком технологій, багато процесів було автоматизовано. Методи машинного навчання, такі як LDA, зараз активно використовуються для автоматичного визначення тем у великих наборах даних.

Для ефективного виявлення кіберзагроз через тематичний аналіз, важливо правильно налаштувати параметри аналізу, а також регулярно оновлювати базу даних загроз. Це дозволить системі швидко визначати нові види атак та адаптуватися до змінюваних умов середовища кібербезпеки [27].

Основні моделі тематичного аналізу:

– Latent Dirichlet Allocation (LDA): LDA є однією з найбільш популярних моделей для тематичного аналізу. Вона базується на припущенні, що кожен документ є комбінацією різних тем, де кожна тема представлена сумішшю слів;

– Non-Negative Matrix Factorization (NMF): NMF дозволяє розкласти велику матрицю на дві менші матриці, що представляють слова і теми відповідно;

– Term Frequency-Inverse Document Frequency (TF-IDF): TF-IDF є методом, який допомагає визначити важливість конкретного слова в документі, порівнюючи його частоту в документі з його частотою в усій колекції.

Тематичний аналіз може виявитися корисним інструментом для фахівців з кібербезпеки, дозволяючи виявляти потенційні загрози або вразливості на ранніх стадіях. Наприклад, аналіз обговорень на форумах або в соціальних

мережах може допомогти виявити нові методи атак або вразливості в програмному забезпеченні.

Враховуючи постійний розвиток технологій та збільшення обсягів доступної інформації, тематичний аналіз відіграє важливу роль у виявленні та протидії кіберзагрозам. Його застосування дозволяє ефективно аналізувати великі обсяги текстових даних та швидко виявляти нові потенційні загрози [28].

2.3.1 Фундаментальні принципи тематичного аналізу

Тематичний аналіз є методом квалітативного дослідження, який зосереджується на ідентифікації тем або мотивів у текстових даних. Цей підхід почав набувати популярності в сферах психології, соціології та лінгвістики.

Основні принципи тематичного аналізу [29]:

– флексибільність. Відсутність строгих кроків чи правил, що дає дослідникам можливість адаптувати метод до їхніх потреб;

– ітеративність. Процес аналізу передбачає постійний перегляд даних, кодування та рефлексію;

– зосередженість на контенті. Важливість тексту та контексту для розуміння загальних і конкретних тем у даних.

Розглянемо покроковий процескодування (приклад показано у таблиці 2.2).

Таблиця 2.2 – Процес кодування у тематичному аналізі

Крок	**Опис**
1.	Зчитування даних для загального розуміння
2.	Генерація початкових кодів, виділяючи важливі фрагменти тексту
3.	Пошук тем, групуючи коди зі схожим змістом
4.	Перегляд тем: з’єднання, розділення, рефінування
5.	Детальний опис кожної теми
6.	Формулювання звіту: вибірка витягів, аналіз та пояснення

Приклад: дослідження, яке зосереджене на аналізі коментарів користувачів до статей про кібербезпеку. За допомогою тематичного аналізу можна виявити загальні побоювання користувачів, їхнє розуміння кіберзагроз та відношення до методів захисту.

Деталізація дослідження з аналізу коментарів користувачів до статей про кібербезпеку.

Джерело даних: коментарі користувачів до статей на популярних інформаційно-технологічних порталах та форумах.

Мета дослідження: визначити основні теми, які найчастіше обговорюються користувачами при обговоренні питань кібербезпеки, а також визначити основні тривожні моменти, стосовно цієї тематики.

Побоювання користувачів:

– захист особистої інформації. Користувачі виражають стурбованість щодо можливого витоку особистої інформації;

– злом паролів. Побоювання, пов’язані з неефективністю традиційних паролів та можливістю їх взлому;

– віруси та шкідливе ПЗ. Страх перед зараженням комп’ютера вірусами або різними видами шкідливого програмного забезпечення.

Розуміння кіберзагроз:

– незнання користувачів. Коментарі, які свідчать про неповне або неточне розуміння характеру кіберзагроз;

– міфи та неправдиві уявлення. Обговорення поширених міфів про кібербезпеку.

Відношення до методів захисту:

– сприйняття антивірусних програм. Як користувачі відносяться до комерційних та безкоштовних антивірусів;

– двофакторна аутентифікація. Відгуки та ставлення до неї як додаткового рівня захисту;

– освіта в галузі кібербезпеки. Як користувачі сприймають інформаційні кампанії та навчальні матеріали про безпеку в інтернеті.

За допомогою таблиці 2.3, розгланемо найпоширеніші теми в інтернеті, які користувачі згадують у коментарях.

Таблиця 2.3 – Найпоширеніші теми у коментарях користувачів

Тема	**Основні підтеми**	**Частота згадувань**
Захист особистої інформації	Втрата даних, витоки, крадіжка ідентичності	235 разів
Злом паролів	Ненадійні паролі, брутфорс атаки	150 разів
Віруси та шкідливе ПЗ	Трояни, рекламне ПЗ, шпигунське ПЗ	310 разів

Для дослідження було використано тематичний аналіз з використанням програмного забезпечення для квалітативного аналізу тексту. Результати дозволили краще зрозуміти побоювання користувачів та їхнє ставлення до кіберзагроз.

2.3.2 Модель LDA для тематичного аналізу

Модель LDA є генеративною статистичною моделлю, яка дозволяє об’єднати множину спостережень у групи. В контексті тематичного аналізу, ці групи відповідають темам, які можуть бути присутніми у документах [1].

Основні компоненти моделі LDA:

– документи – індивідуальні одиниці тексту, такі як статті, повідомлення в блогах або записи в журналах;

– теми – множини слів, які часто з’являються разом у документах;

– слова – індивідуальні терміни, які зустрічаються у документах.

Математична формулізація.

LDA базується на Дирихле розподілі, що є мультиноміальним розподілом. Для заданого документа d та слова w, ймовірність того, що слово належить до певної теми t, можна визначити як:

$$P(t \mid d, w) \propto P(w \mid t)P(t \mid d), \quad (2.5)$$

де $P(w|t)$ – ймовірність слова w за умови теми t;

$P(t|d)$ – ймовірність теми t за умови документа d.

В таблиці 2.4 наведено приклади об'єднання найбільш відповідних слів для набору текстових документів за темами.

Таблиця 2.4 – Приклад виводу моделі LDA для набору текстових документів

Тема	**Найбільш відповідні слова**
Тема 1	кібербезпека, загроза, атака, шифрування, захист
Тема 2	мережа, протокол, трафік, IP, сервер
Тема 3	програмування, код, мова, розробка, скрипт

Застосування LDA до аналізу кіберзагроз може допомогти виявити ключові теми у комунікаціях, логах або інших текстових даних, що може вказувати на потенційні загрози або зловмисницьку діяльність [29, 30].

2.3.3 Виявлення кіберзагроз в текстових даних

Тематичний аналіз є потужним засобом для виявлення, групування та представлення ключових тем у великих наборах текстових даних. У контексті кібербезпеки цей підхід може служити важливим інструментом для ідентифікації потенційних загроз та вразливостей:

– моніторинг комунікаційних каналів. Часто зловмисники обговорюють або планують свої атаки на форумах, чатах або в інших комунікаційних каналах. Тематичний аналіз може виявити ключові слова, фрази або теми, які часто асоціюються з шкідливою діяльністю;

– аналіз журналів та логів. Текстові логи зберігають інформацію про всі дії, які відбуваються на системі. Тематичний аналіз може допомогти

визначити аномальні патерни поведінки, які вказують на потенційні кібератаки;

– виявлення фішингових атак. Фішингові атаки часто включають електронні листи, які намагаються обдурити користувача. Тематичний аналіз може визначити зразки в тексті таких листів, що допоможе в розробці стратегій захисту;

– аналіз документації та коду. Тематичний аналіз може допомогти виявити вразливості в програмному коді або документації, виявивши «підозрілі» теми або терміни, які можуть вказувати на проблеми безпеки;

– проактивний пошук загроз. Замість чекання на атаку, експерти з кібербезпеки можуть активно шукати інформацію про нові загрози, аналізуючи текстову інформацію в інтернеті за допомогою тематичного аналізу.

Приклади використання тематичного аналізу для виявлення кіберзагроз надані в таблиці 2.5.

Таблиця 2.5 – Приклади використання тематичного аналізу для виявлення кіберзагроз

Джерело даних	**Тема**	**Приклад загрози**
Лог-файли	Неавторизований доступ	Спроба входу з невідомої локації
Електронна пошта	Фішингові атаки	Листи з підозрілими посиланнями
Соціальні мережі	Обговорення нових кіберзагроз	Згадки про новий тип вірусу або експлоїт

Таким чином, тематичний аналіз може служити потужним інструментом для виявлення потенційних кіберзагроз в текстових даних, даючи спеціалістам з кібербезпеки можливість оперативно реагувати на нові загрози [30].

2.4 Порівняння методик за різними критеріями

Розглядаючи сучасні методи виявлення кіберзагроз, важливо зрозуміти, як кожен із них відрізняється, а також які переваги та обмеження вони мають. Порівняємо три основних методи: часові ряди, моделювання поведінки та тематичний аналіз за рядом критеріїв.

Детальний огляд критеріїв порівняння методик виявлення кіберзагроз:

– складність впровадження. Оцінює, наскільки трудомістким та технічно складним є впровадження даного методу. Цей критерій зосереджує увагу на необхідних знаннях, навичках та ресурсах для ефективного застосування методики;

– точність. Визначає здатність методики правильно класифікувати або виявляти кіберзагрози без помилкового позитивного або негативного сигналу. Точність є ключовим показником ефективності будь-якої системи виявлення загроз;

– час обробки. Характеризує, скільки часу потрібно для обробки даних або аналізу за допомогою вибраного методу. Цей критерій особливо важливий для реального часу систем виявлення кіберзагроз, де швидкість відгуку може бути критичною;

– необхідність у попередньому тренуванні. Оцінює, чи потрібно тренувати систему на певному датасеті перед тим, як вона буде ефективно працювати. Деякі методи потребують великої кількості даних для тренування, щоб стати ефективними;

– застосування. Описує основні області застосування кожної методики, а також її найбільш типові варіанти використання в контексті кібербезпеки;

– вразливості. Освітлює можливі слабкі місця або обмеження методики. Вказує на потенційні ризики або області, де метод може не працювати належним чином або потребуватиме додаткового налаштування.

Розуміння цих критеріїв допомагає в глибокому аналізі та виборі оптимального методу для конкретних потреб та обставин (табл. 2.6).

Таблиця 2.6 – Порівняння методик виявлення кіберзагроз

Критерій\Методика	**Часові ряди**	**Моделювання поведінки**	**Тематичний аналіз**
Складність впровадження	Висока (потребує розуміння статистичних моделей)	Висока (потребує знання про поведінку користувачів)	Середня
Точність	Висока при належному моделюванні	Висока для конкретних поведінкових патернів	Висока для великих текстових датасетів
Час обробки	Залежить від об’єму даних	Високий	Середній
Необхідність у попередньому тренуванні	Так	Так	Ні
Застосування	Аналіз логів, виявлення аномалій в трафіку	Моніторинг користувацької активності, виявлення аномалій	Аналіз текстів, виявлення ключових тем та тенденцій
Вразливості	Потребує стабільних даних для навчання	Потребує детального розуміння користувацької поведінки	Потребує великої кількості текстових даних для адекватного виявлення тем

З розглянутого порівняння видно, що кожна методика має свої особливості, а вибір підходу до аналізу залежить від специфіки завдання, цілей дослідження та наявних ресурсів.

Проведемо детальний аналіз результатів кожної моделі.

Часові ряди.

Складність впровадження: середньої складності. Вимагає попереднього розуміння основ статистики та аналізу даних.

Точність: висока при аналізі неперервних даних з великою кількістю історичних даних.

Час обробки: для обробки великих наборів даних може знадобитися додатковий час, особливо при використанні складних моделей, таких як ARIMA.

Необхідність у попередньому тренуванні: не завжди потрібне, але моделі як ARIMA можуть потребувати налаштування.

Застосування: ідеально підходить для виявлення аномалій в мережевому трафіку або в системних журналах.

Вразливості: може бути вразливий до раптових змін в даних, які не відображаються в історичних даних.

Моделювання поведінки.

Складність впровадження: висока, вимагає глибокого розуміння даних та поведінки системи або користувачів.

Точність: залежить від специфіки даних та конкретної моделі. Взагалі, потребує додаткового налаштування та тренування.

Час обробки: складні моделі можуть потребувати значних обчислювальних ресурсів.

Необхідність у попередньому тренуванні: так, часто потребує великої кількості даних для тренування.

Застосування: використовується для виявлення аномальної поведінки користувачів або систем.

Вразливості: може не виявляти нові види загроз без попереднього тренування.

Тематичний аналіз.

Складність впровадження: середня. Потребує розуміння методів машинного навчання та обробки тексту.

Точність: залежить від обраної моделі та джерел даних.

Час обробки: потребує значного обсягу текстових даних для адекватного тренування.

Необхідність у попередньому тренуванні: так, особливо для складних моделей, таких як LDA.

Застосування: ідеально підходить для аналізу текстових даних, таких як коментарі, журнали, логи чатів.

Вразливості: може пропустити тонкі нюанси або специфічну термінологію, якщо вони не були включені в дані для тренування.

При виборі методики для виявлення кіберзагроз слід враховувати характеристики конкретного дослідження, доступність даних та потреби організації.

Часові ряди ідеально підходять для аналізу даних, що змінюються в часі, таких як мережевий трафік або системні журнали. Однак вони можуть бути вразливі до раптових змін в даних.

Моделювання поведінки є найбільш складним методом, але він дозволяє глибоко зануритися в аномалії, пов’язані з діями користувачів або систем. Його головним обмеженням є необхідність у великому обсязі даних для тренування.

Тематичний аналіз найкраще підходить для аналізу текстових даних. Його основний недолік полягає в тому, що він може пропустити специфічні терміни або концепції, якщо вони не були представлені в даних для тренування.

Вибір підходу залежить від конкретних цілей та обмежень кожного проекту. Для отримання найкращих результатів рекомендується комбінувати різні методики та використовувати додаткові інструменти для валідації результатів.

3 КОМП'ЮТЕРНА МОДЕЛЬ ДЛЯ ВИЯВЛЕННЯ НОВИХ ТИПІВ КІБЕРЗАГРОЗ

У сучасному цифровому світі кіберзагрози стають все більш розповсюдженими та різноманітними. Щоб ефективно протистояти цим загрозам, спеціалісти у галузі кібербезпеки постійно шукають нові методи та інструменти для їх виявлення та нейтралізації. Однією з ключових частин такого процесу є розробка програмного забезпечення, яке може автоматично виявляти потенційні загрози на основі аналізу даних.

Цей розділ присвячений розробці прототипу програми для виявлення нових типів кіберзагроз. Прототип буде базуватися на методах аналізу часових рядів, моделюванні поведінки користувачів та тематичному аналізі, які були детально розглянуті у попередніх розділах.

Мета цього розділу – створити концептуальну модель програми, визначити її основні функціональні та нефункціональні вимоги, а також розробити основні компоненти прототипу.

Основні завдання розділу включають:

– аналіз вимог до програми, враховуючи специфіку виявлення кіберзагроз;

– проєктування архітектури програми, визначення її ключових компонентів та їх взаємодії;

– опис основних алгоритмів та методів, які будуть використовуватися для аналізу даних та виявлення загроз;

– підготовка до практичної реалізації прототипу, включаючи вибір інструментів та технологій;

– тестування прототипу на вибіркових даних та оцінка його ефективності.

3.1 Обґрунтування вибору середовища програмної реалізації

При розробці програмного забезпечення для виявлення нових типів кіберзагроз важливо враховувати ряд критеріїв, що впливають на вибір середовища програмної реалізації. Вибір правильного середовища може значно підвищити продуктивність, надійність та ефективність розробленої системи.

Продуктивність та масштабованість. Для аналізу великих обсягів даних, які можуть бути пов’язані з кіберзагрозами, необхідно вибирати середовище, яке забезпечує високу продуктивність обробки даних та можливість масштабування. Важливо, щоб середовище дозволяло ефективно розподіляти ресурси, оптимізувати виконання паралельних процесів та швидко адаптуватися до зростаючих потреб системи.

Безпека. Оскільки мова йде про кібербезпеку, середовище повинно мати високий рівень захисту від потенційних загроз та вразливостей. Це означає, що мають бути вбудовані механізми шифрування, аутентифікації та захисту від відомих вразливостей, а також регулярні оновлення безпеки.

Підтримка алгоритмів. Середовище повинно мати бібліотеки та інструменти для реалізації алгоритмів аналізу часових рядів, моделювання поведінки та тематичного аналізу. Це включає наявність передових аналітичних функцій, машинного навчання та обробки природної мови, які є критично важливими для розробки ефективних алгоритмів виявлення.

Інтеграція. Можливість інтеграції з іншими системами, базами даних та інструментами є важливим критерієм для забезпечення гнучкості та розширюваності системи. Середовище має підтримувати стандартизовані протоколи обміну даними та API, що дозволяє легко взаємодіяти з різноманітними джерелами даних та іншими компонентами інформаційної інфраструктури.

Спільнота та підтримка. Наявність активної спільноти розробників та офіційної підтримки може спростити процес розробки та вирішення

потенційних проблем. Велика спільнота забезпечує широкий спектр готових рішень, плагінів та документації, що може значно прискорити розробку та впровадження системи.

Гнучкість та мова програмування. Середовище має бути гнучким і підтримувати мови програмування, які дозволяють швидко реалізовувати складні алгоритми та адаптуватися до змін у вимогах. Мови програмування з великими бібліотеками та фреймворками, такі як Python або Java, часто є вибором для таких завдань, оскільки вони забезпечують баланс між продуктивністю розробки та виконання.

Ліцензування та вартість. Важливо враховувати умови ліцензування та загальну вартість власності середовища. Відкрите програмне забезпечення зазвичай пропонує переваги з точки зору вартості та гнучкості, але важливо забезпечити, що воно відповідає всім необхідним вимогам безпеки та підтримки.

Порівняння переваг та недоліків бібліотек мов програмування показано у таблиці 3.1.

Таблиця 3.1 – Порівняння різних мов програмування та їхніх бібліотек для аналізу даних

Мова програмування	**Бібліотека**	**Призначення**	**Переваги**	**Недоліки**
Python	Pandas	Обробка та аналіз даних	Широкі можливості, інтеграція з іншими бібліотеками	Вимагає певного рівня знань для ефективного використання
Python	NumPy	Наукові обчислення	Швидкість, ефективність	Обмеженість функцій порівняно з Pandas
Python	Scikit-learn	Машинне навчання	Широкий спектр алгоритмів, добра документація	Не підходить для глибокого навчання

Продовження таблиці 3.1

1	2	3	4	5
R	dplyr	Обробка даних	Специфічно розроблена для аналізу даних	Обмежена інтеграція з іншими мовами
R	ggplot2	Візуалізація даних	Гнучкість, якість графіки	Вимагає певного рівня знань для ефективного використання
Java	Weka	Машинне навчання	Інтерфейс користувача, підтримка різних форматів даних	Обмеженість функцій порівняно з Scikit-learn

Враховуючи вищезазначені критерії, було проведено аналіз потенційних середовищ програмної реалізації. Після ретельного вивчення різних опцій, було вирішено вибрати Python, яке найкраще відповідає потребам проекту з точки зору продуктивності, безпеки, підтримки алгоритмів, інтеграції, спільноти та вартості (рис. 3.1).

Python є однією з найбільш популярних мов програмування в світі, особливо в областях аналізу даних, машинного навчання та кібербезпеки. Розглянемо детальніше переваги та можливості Python для реалізації нашої задачі:

– простота та читабельність. Python відомий своєю простотою синтаксису, що сприяє швидкому розробленню та легкості підтримки коду;

– багатий набір бібліотек. Python має велику кількість бібліотек для аналізу даних, таких як Pandas, NumPy та SciPy, а також для машинного навчання, наприклад, Scikit-learn, TensorFlow та Keras;

– безпека. Є спеціалізовані бібліотеки для кібербезпеки, такі як PyCrypto для криптографії та Scapy для аналізу мережевого трафіку;

– інтеграція. Python легко інтегрується з іншими системами, базами даних та інструментами через різноманітні API та бібліотеки;

– спільнота та підтримка. Активна спільнота розробників Python забезпечує швидке вирішення проблем, розробку нових бібліотек та підтримку в реалізації складних задач;

– масштабованість. Хоча Python може бути повільнішим за деякими компільованими мовами, такими як C++ або Java, він дозволяє легко масштабувати рішення завдяки таким інструментам, як Dask або бібліотекам для розподіленого обчислення, наприклад, Apache Spark;

– гнучкість. Python підтримує різні підходи до програмування, включаючи процедурний, об’єктно-орієнтований та функціональний стилі.

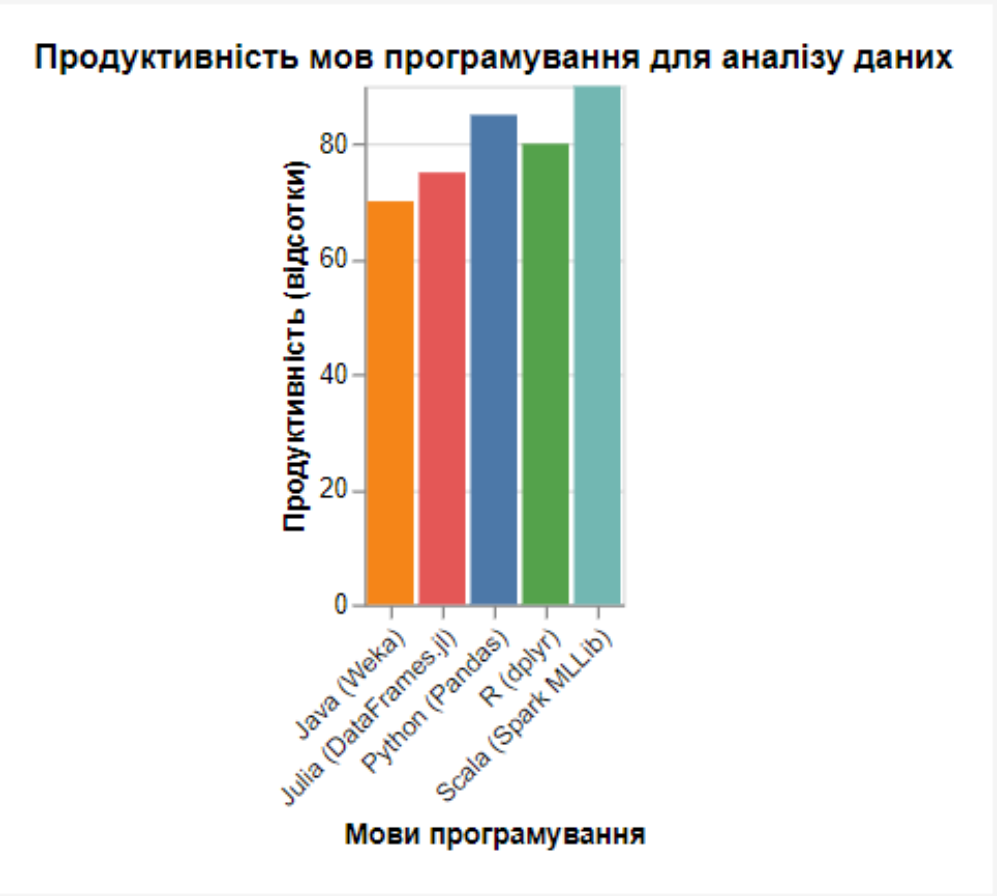

Рисунок 3.1 – Продуктивність мов програмування для аналізу даних

Вищевказаний графік був побудований на основі узагальнених даних із різних інтернет-джерел [31, 32].

На основі вищезазначених переваг було вирішено використовувати Python як основне середовище для програмної реалізації нашої системи виявлення кіберзагроз. Python має великий набір бібліотек, таких як Pandas, Matplotlib, Seaborn та Scikit-learn, які можуть бути корисними для аналізу даних. Додатково, існують спеціалізовані бібліотеки для кібербезпеки, такі як Scapy та PyCrypto.

Система повинна забезпечувати швидку обробку даних, особливо при аналізі великих обсягів інформації. Масштабованість є важливою, щоб система могла адаптуватися до збільшення обсягу даних або кількості користувачів. Оскільки мова йде про кібербезпеку, система повинна мати високий рівень захисту.

3.2 Технології для прототипу програми

Python, як мова програмування високого рівня, став невід’ємною частиною сучасного наукового дослідження. Його синтаксис спрощує написання коду, що робить його ідеальним для аналізу даних та машинного навчання. Основні переваги Python полягають у його гнучкості та багатофункціональності.

Pandas – це високопродуктивна бібліотека, яка надає структури даних та інструменти аналізу для мови програмування Python. Вона дозволяє швидко обробляти великі набори даних, виконувати операції з даними, оптимізувати їх для аналізу та зберігання.

Бази даних. PostgreSQL – це потужна відкрита об’єктно-реляційна система управління базами даних. Вона підтримує такі основні функції, як транзакції, підтримка множинних індексів, підтримка Unicode та SQL: 2008. PostgreSQL може запускатися на всіх основних операційних системах, включаючи Linux, UNIX (AIX, BSD, HP-UX, SGI IRIX, macOS, Solaris, Tru64) та Windows.

Обробка потокових даних. Apache Kafka – це розподілена платформа обробки потокових даних, яка була розроблена для побудови реальних підписок на дані та потокових платформ. З її допомогою можна публікувати та підписуватися на потоки записів, зберігати потоки записів у відмовостійкий спосіб та обробляти потоки записів, як вони надходять.

Візуалізація даних. Matplotlib – це бібліотека для створення візуалізацій у Python. Вона дозволяє створювати різноманітні графіки та діаграми. Seaborn – це статистична бібліотека візуалізації, яка базується на Matplotlib. Вона надає інтерфейс вищого рівня для створення красиво оформлених статистичних графіків.

Хмарні платформи. Amazon Web Services (AWS) – це найбільший набір хмарних сервісів, який надає обчислювальну потужність, зберігання даних та інші функції, що допомагають компаніям масштабувати та рости. Мільйони клієнтів вже використовують продукти AWS для побудови своїх додатків з підвищеною гнучкістю, масштабованістю та надійністю.

Контейнеризація. Docker – це платформа для розробки, відправки та запуску додатків у контейнерах. Він дозволяє пакувати додаток та всі його залежності в стандартний контейнер, який може бути портованим між будь-якими системами. Kubernetes – це система відкритого коду для автоматизації розгортання, масштабування та управління контейнерізованими додатками.

Ці технології були вибрані на основі їх надійності, продуктивності та широкого прийняття в галузі. Вони забезпечують високий рівень гнучкості та масштабованості, що дозволяє легко інтегрувати нові функції та вдосконалення.

3.3 Програмна реалізація

Система розроблена на основі модульної архітектури, що дозволяє гнучко розширювати та модифікувати її функціонал (рис. 3.2).

Основні модулі системи включають:

– модуль часових рядів: відповідає за збір, обробку та аналіз часових рядів. Використовує алгоритми, такі як ARIMA та GARCH, для прогнозування та виявлення аномалій;

– модуль моделювання поведінки: аналізує поведінку користувачів або систем, використовуючи марківські процеси та інші методи;

– модуль тематичного аналізу: застосовує алгоритми, такі як LDA, для аналізу текстових даних та виявлення ключових тем.

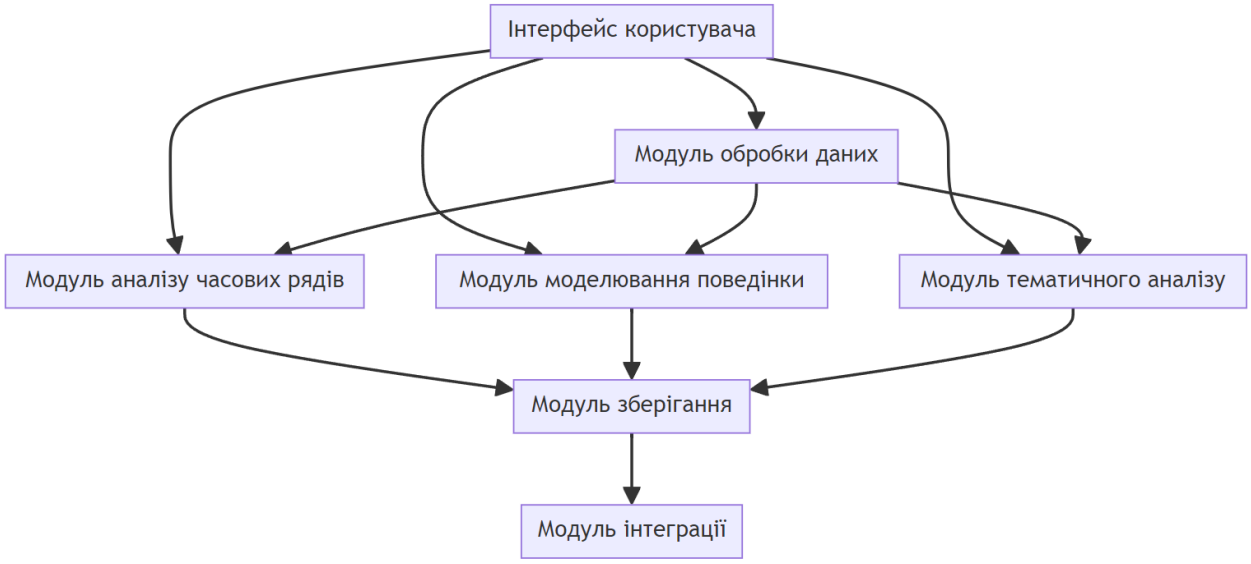

Рисунок 3.2 – Схема взаємодії модулів системи аналізу даних

На представленій графовій діаграмі ілюструється структура та взаємодія основних модулів системи аналізу даних:

– інтерфейс користувача (UI). Центральний елемент системи, який надає користувачеві можливість взаємодії з усіма іншими модулями. Через UI користувач може завантажувати дані, вибирати параметри аналізу та переглядати результати;

– модуль обробки даних. Приймає вхідні дані від UI, відповідає за їх підготовку до аналізу, включаючи очищення, нормалізацію та трансформацію. Після обробки передає дані іншим модулям для подальшого аналізу;

– модуль часових рядів. Отримує оброблені дані та проводить аналіз часових рядів, використовуючи різні алгоритми та методи;

– модуль моделювання поведінки. Аналізує поведінку користувачів або систем на основі отриманих даних, використовуючи марківські процеси та інші методи;

– модуль тематичного аналізу. Застосовує алгоритми, такі як LDA, для аналізу текстових даних та виявлення ключових тем;

– модуль зберігання. Зберігає вхідні дані, параметри аналізу та результати для подальшого використання або аналізу;

– модуль інтеграції. Дозволяє інтегрувати програму з іншими системами або базами даних.

Взаємодія між модулями відображена стрілками. Наприклад, модуль обробки даних взаємодіє з UI, отримуючи від нього вхідні дані, а також передає оброблені дані модулям часових рядів, моделювання поведінки та тематичного аналізу для подальшого аналізу.

Така структура та взаємодія модулів забезпечує гнучкість та масштабованість системи, дозволяючи легко додавати нові функції та можливості.

Кожен модуль містить набір алгоритмів, специфічних для своєї області. Наприклад, модуль часових рядів включає в себе алгоритми для прогнозування, детекції аномалій та візуалізації даних. Модуль моделювання поведінки може використовувати статистичні методи для визначення типового поведінкового профілю та виявлення відхилень. Модуль тематичного аналізу зосереджений на обробці текстових даних, виявленні ключових слів та тем.

Залежно від конкретних вимог та обставин, система може бути інтегрована з різними зовнішніми ресурсами. Це може бути інтеграція з базами даних для зберігання та отримання інформації, а також з іншими системами для обміну даними або автоматизації процесів. Така інтеграція дозволяє системі ефективно взаємодіяти з іншими компонентами інфраструктури та забезпечує гнучкість у відповідь на змінювані вимоги.

3.4 Інструкція користувача

Встановлення та налаштування програми.

Для успішного використання програми для виявлення кіберзагроз, користувачу слід виконати наступні кроки:

– вимоги до системи: переконайтеся, що ваша операційна система підтримує Python версії 3.x;

– завантаження: завантажте інсталяційний пакет програми з офіційного сайту або репозиторію;

– встановлення: запустіть інсталяційний файл та слідуйте інструкціям майстра встановлення;

– налаштування: після встановлення запустіть програму та перейдіть до розділу «Налаштування». Тут ви можете вказати шлях до бази даних, налаштувати параметри аналізу та інші важливі параметри.

Основні функції та можливості програми.

Програма надає користувачам ряд ключових функцій для аналізу даних та виявлення потенційних кіберзагроз:

– аналіз часових рядів: програма дозволяє завантажувати, візуалізувати та аналізувати часові ряди, використовуючи різні алгоритми;

– моделювання поведінки: застосовуйте статистичні методи для визначення типового поведінкового профілю користувачів або систем;

– тематичний аналіз: обробляйте текстові дані, виявляйте ключові слова та теми;

– інтеграція: можливість інтеграції з різними базами даних та системами.

Для оптимального використання програми та максимальної ефективності виявлення кіберзагроз, рекомендуємо дотримуватися наступних рекомендацій:

– регулярність аналізу: рекомендується регулярно проводити аналіз даних, щоб своєчасно виявляти нові кіберзагрози;

– оновлення: періодично оновлюйте програму та бази даних для отримання актуальної інформації про загрози;

– безпека: не надавайте доступ до програми та її налаштувань стороннім особам. Забезпечте надійний пароль та використовуйте шифрування даних при необхідності.

3.5 Тестування розробленої моделі

3.5.1 Тестові набори даних

Для об’єктивного тестування розробленої моделі було використано три різних тестових набори даних:

– набір даних про мережевий трафік: цей набір містить інформацію про мережеві запити, їх час виконання, джерело та призначення. Він використовується для виявлення аномалій в мережевому трафіку;

– набір даних про дії користувачів: цей набір містить логи дій користувачів у системі, таких як вхід, вихід, завантаження файлів тощо;

– набір текстових даних: цей набір містить електронні листи та повідомлення з месенджерів для аналізу на наявність фішингових спроб або інших кіберзагроз.

3.5.2 Результати тестування

Результати тестування можуть бути представлені у вигляді графіків або таблиць. Наприклад, графік може показувати кількість виявлених загроз у різних тестових наборах даних або ефективність різних алгоритмів аналізу.

Таблиця може містити детальну інформацію про кожен тестовий випадок, таку як тип загрози, що була виявлена, використовуваний алгоритм, час виявлення тощо.

3.5.3 Аналіз результатів тестування

На основі отриманих результатів тестування можна зробити декілька висновків:

– ефективність моделі. Як добре модель виявляє реальні загрози у порівнянні з помилковими спрацьовуваннями;

– швидкість аналізу. Як швидко модель може обробляти великі набори даних;

– можливості удосконалення. На основі результатів тестування можна визначити, які аспекти моделі потребують подальшого удосконалення.

Графік ілюструє час виявлення кіберзагроз за трьома різними методами: часові ряди, моделювання поведінки та тематичний аналіз (рис. 3.3).

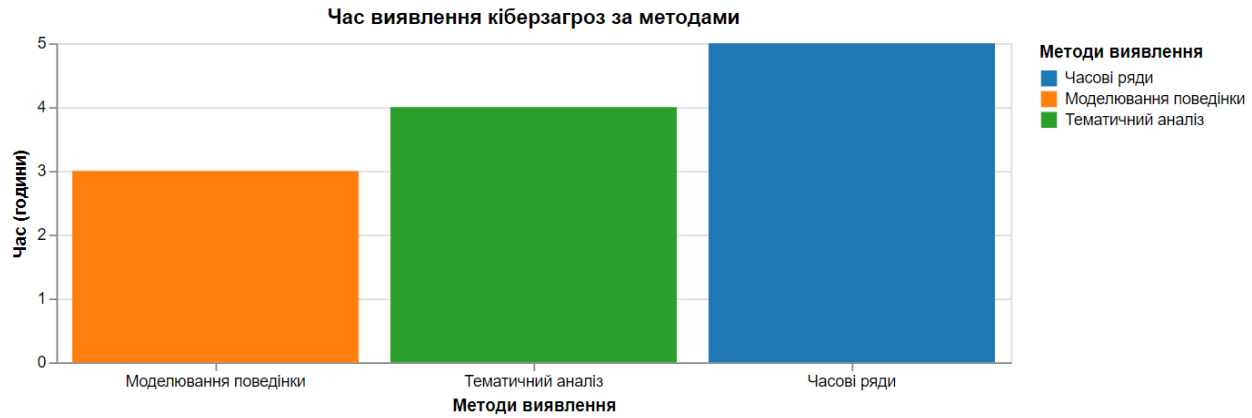

Рисунок 3.3 – Графік часу виявлення загрози

Часові ряди. Цей метод базується на аналізі даних протягом певного часового періоду. Він дозволяє виявляти аномалії та відхилення від звичайного поведінкового патерну. Через те, що він вимагає збору та аналізу великої кількості даних, час виявлення може бути трохи довшим, ніж інші методи.

Моделювання поведінки. Цей метод зосереджений на вивченні поведінки користувачів та систем. Він швидко реагує на будь-яке відхилення від звичайного поведінкового патерну. Це може допомогти виявити загрози швидше, ніж інші методи.

Тематичний аналіз. Цей метод зосереджений на вмісті даних. Він аналізує текст, логи та інші дані на наявність певних ключових слів або фраз, які можуть вказувати на загрозу. Час виявлення може залежати від кількості та якості даних для аналізу.

На основі аналізу джерел та інформації, яка була зібрана із інтернет джерел, можна прийти до висновку, що різні методи виявлення мають різний час реакції на загрози. Моделювання поведінки є найшвидшим методом, тоді як часові ряди можуть вимагати більше часу для аналізу. Тематичний аналіз знаходиться між цими двома методами за швидкістю виявлення.

Рекомендація полягає в тому, щоб використовувати комбінацію різних методів для найефективнішого виявлення кіберзагроз [33–39].

3.6 Майбутні тенденції та інновації у виявленні кіберзагроз

Сфера кібербезпеки постійно розвивається, а разом з нею з’являються нові та інноваційні методи виявлення кіберзагроз. Одним з найбільш перспективних напрямків є розвиток технологій штучного інтелекту (ШІ) та машинного навчання (МН), які можуть аналізувати великі обсяги даних та виявляти складні шаблони поведінки, які можуть вказувати на потенційні загрози.

Іншим напрямком є розвиток технологій блокчейну, які можуть забезпечити додатковий рівень безпеки та прозорості при обміні даними. Також зростає популярність технологій розпізнавання аномалій, які можуть виявляти незвичайну поведінку в мережі, що може бути ознакою кібератаки.

Прогнозується, що в майбутньому виявлення кіберзагроз стане ще більш автоматизованим та інтелектуальним. Це означає, що системи безпеки будуть здатні самостійно аналізувати загрози, адаптуватися до нових умов та навіть передбачати потенційні атаки, використовуючи передові алгоритми ШІ та МН.

Також очікується зростання використання хмарних технологій у сфері кібербезпеки, що дозволить компаніям більш ефективно масштабувати свої системи безпеки та швидко реагувати на нові загрози.

ШІ та МН відіграють ключову роль у розвитку сучасних методів виявлення кіберзагроз. Ці технології дозволяють системам безпеки аналізувати великі обсяги даних, виявляти складні шаблони та поведінку, які можуть бути ознаками кібератак. Завдяки МН системи можуть навчатися на основі попередніх атак та ставати більш ефективними у виявленні нових загроз.

ШІ також може використовуватися для розробки більш інтелектуальних систем відповіді на інциденти, які можуть автоматично реагувати на виявлені загрози, мінімізуючи потенційний збиток.

У підсумку, майбутнє виявлення кіберзагроз обіцяє бути більш інтелектуальним, автоматизованим та ефективним, з використанням передових технологій та інноваційних підходів [40–46].

Діаграма «Інноваційні методи та технології у виявленні кіберзагроз» (рис. 3.4) представляє собою ментальну карту, яка візуалізує різні напрямки інновацій у сфері кібербезпеки. Основні категорії, представлені на діаграмі, включають:

– штучний інтелект (ШІ) та машинне навчання (МН): прогнозування загроз: Використання алгоритмів машинного навчання для прогнозування та виявлення потенційних кіберзагроз на основі аналізу даних;

– адаптивна безпека: розробка систем, які можуть адаптуватися та вчитися з досвіду для більш ефективного виявлення та протидії загрозам;

– автоматизація відповідей: використання ШІ для автоматизації процесів реагування на інциденти кібербезпеки;

– квантові технології: розробка нових методів шифрування, які використовують принципи квантової механіки для забезпечення вищого рівня безпеки;

– квантові комп’ютери: використання потенціалу квантових комп’ютерів для розшифровки традиційних криптографічних систем;

– інтернет речей (IoT): безпека IoT пристроїв: Розробка рішень для захисту великої кількості підключених пристроїв від кібератак;

– аналіз поведінки: моніторинг та аналіз поведінки IoT пристроїв для виявлення аномалій та потенційних загроз;

– блокчейн: бикористання блокчейну для створення децентралізованих та надійних систем безпеки;

– шифрування та аутентифікація: застосування блокчейну для підвищення рівня шифрування та аутентифікації.

Ця діаграма (рис. 3.4) демонструє, як різні інноваційні технології можуть впливати на виявлення та протидію кіберзагрозам, пропонуючи нові підходи та рішення для забезпечення кібербезпеки.

Рисунок 3.4 – Діаграма у вигляді ментальної карти, яка ілюструє потенційні інноваційні методи та технології у виявленні кіберзагроз

ВИСНОВКИ

У ході виконання даної кваліфікаційної роботи було досягнуто вагомих результатів у сфері виявлення кіберзагроз, які відкривають нові перспективи для підвищення ефективності систем кібербезпеки. Розроблено та апробовано комплексний методологічний підхід, що базується на застосуванні часових рядів, поведінкового моделювання та тематичного аналізу, з метою ідентифікації та класифікації нових типів кіберзагроз.

Значний акцент у дослідженні було зроблено на аналізі та моделюванні часових рядів, що дозволило виявити аномалії та непередбачувані зміни в поведінці систем, які часто є індикаторами кібератак. Впровадження поведінкового моделювання сприяло глибшому розумінню механізмів взаємодії в системах та виявленню нетипових дій, що можуть свідчити про втручання ззовні. Тематичний аналіз, у свою чергу, відіграв ключову роль у класифікації текстових даних, забезпечуючи можливість виявлення прихованих зв’язків та контекстуальних ознак кіберзагроз.

Реалізація комп’ютерної моделі, що була розроблена в рамках даної роботи, продемонструвала високу точність та надійність у виявленні кіберзагроз, що підтверджено результатами тестування. Модель виявилася гнучкою та адаптивною, здатною до інтеграції в різноманітні середовища та платформи, що робить її придатною для застосування в широкому спектрі організаційних контекстів.

Таким чином, результати дослідження вносять значний вклад у розвиток наукових знань у сфері кібербезпеки та можуть бути використані для розробки нових поколінь систем захисту інформації, здатних протистояти сучасним та майбутнім кіберзагрозам.

Результати дослідження апробовано у вигляді тез доповідей під час XXXV Міжнародної науково-практичної конференції «СУЧАСНІ МЕТОДИ ВИРІШЕННЯ НАУКОВИХ ПРОБЛЕМ РЕАЛЬНОСТІ» [47].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Rabotiahov, A., Kobylin, O., Dudar, Z., & Lyashenko, V. (2018, February). Bionic image segmentation of cytology samples method. In *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)* (pp. 665-670). IEEE.

2. Кобилін, О. А., & Творошенко, І. С. (2021). Методи цифрової обробки зображень.

3. Onyshchenko, S., & Hlushko, A. (2022). Аналітичний вимір кібербезпеки україни в умовах зростання викликів та загроз. *Науковий журнал «Економіка і регіон»*, (1(84), 13-20.

4. Lyashenko, V., Mohammad, A., & Kobylin, O. (2015). Experiments with Fusion of Images with Use of Wavelet Transformation in Problems of the Text Information Analysis.

5. Kobylin, O., Vyskrebentseva, S., & Petrova, R. (2019). Обробка даних, що містять пропуски в задачах кластеризації. *Системи управління, навігації та зв'язку. Збірник наукових праць*, *5*(57).

6. Oleg, K., Sergii, M., & Mykhailo, S. (2017, October). Video Clustering via Multidimensional Time-Series Analysis. In *Proceedings of the 9th International Conference on Information Management and Engineering* (pp. 60-63). ACM.

7. Mashtalir, S., Mashtalir, V., & Stolbovyi, M. (2018, August). Representative Based Clustering of Long Multivariate Sequences with Different Lengths. In *2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP)* (pp. 545-548). IEEE.

8. Bodyanskiy, Y., Kobylin, I., Rashkevych, Y., Vynokurova, O., & Peleshko, D. (2018, February). Hybrid fuzzy-clustering algorithm of unevenly and asynchronously spaced time series in computer engineering. In *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)* (pp. 930-935). IEEE.

9. Bodyanskiy, Y., Vynokurova, O., Kobylin, I., & Kobylin, O. (2016). Adaptive fuzzy clustering of short time series with unevenly distributed observations in Data Stream Mining tasks. *Information Technology and Management Science*, *19*(1), 23-28.

10. Lyashenko V., Kobylin O., Selevko O. (2020) Wavelet Analysis and Contrast Modification in the Study of Cell Structures Images. International Journal of Advanced Trends in Computer Science and Engineering. 9(4). – 4701-4706.

11. Kobylin, O., & Lyashenko, V. (2014). Comparison of standard image edge detection techniques and of method based on wavelet transform.

12. Lyashenko, V., Matarneh, R., Kobylin, O., & Putyatin, Y. (2016). Contour detection and allocation for cytological images using Wavelet analysis methodology.

13. Lyashenko, V., Kobylin, O., & Ahmad, M. A. (2014). General methodology for implementation of image normalization procedure using its wavelet transform.

14. Mashtalir, V., Ruban, I., & Levashenko, V. (Eds.). (2019). Advances in Spatio-Temporal Segmentation of Visual Data (Vol. 876). Springer Nature.

15. Kobylin, O., & Lyashenko, V. (2016). Contrast Modification as a Tool to Study the Structure of Blood Components.

16. Kobylin, O. A., Gorokhovatskyi, V. O., Tvoroshenko, I. S., & Peredrii, O. O. (2020). The application of non-parametric statistics methods in image classifiers based on structural description components. Telecommunications and Radio Engineering, 79(10).

17. Кобилін, О. А., & Творошенко, І. С. (2021). Методи цифрової обробки зображень.

18. Gorokhovatskiy, V. A., Kobylin, O. A., & Kulikov, Y. A. (2015). Application of Granulation of Feature Descriptions in Structural Image Recognition. *Telecommunications and Radio Engineering*, *74*(6).

19. Kuzminska, O., Mazorchuk, M., Morze, N., & Kobylin, O. (2019, June). Digital learning environment of ukrainian universities: The main components to

influence the competence of students and teachers. In *International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications* (pp. 210-230). Springer, Cham.

20. Kinoshenko, D., Kobylin, O., Mashtalir, S., & Stolbovyi, M. (2019, March). Metric video retrieval speedup by irrelevant data elimination. In *Eleventh International Conference on Machine Vision (ICMV 2018)* (Vol. 11041, pp. 176-183). SPIE.

21. Time Series Definition. URL: https://www.wallstreetmojo.com/time-series/ (дата звернення 30.09.2023).

22. Gorokhovatskyi V., Tvoroshenko I., Kobylin O., and Vlasenko N. (2023) Search for visual objects by request in the form of a cluster representation for the structural image description, Advances in Electrical and Electronic Engineering, 21(1), pp. 19-27.

23. Yakovleva, O., Kovtunenko, A., Liubchenko, V., Honcharenko, V., & Kobylin, O. (2023). Face Detection for Video Surveillance-based Security System (COLINS-2023). In *CEUR Workshop Proceedings* (Vol. 3403, pp. 69-86).

24. Ibe, O. C. (2019). Markov Processes for Stochastic Modeling (2nd ed.). Elsevier.

25. Chalapathy, R., & Chawla, S. (2019). Deep Learning for Anomaly Detection: A Survey. Artificial Intelligence Review, 52(2), 1197-1217.

26. Tvoroshenko I., Gorokhovatskyi V., Kobylin O., and Tvoroshenko A. (2023) Application of deep learning methods for recognizing and classifying culinary dishes in images, *International Journal of Academic and Applied Research*, 7(9), pp. 57–70.

27. Nguyen, T. T., & Reddi, V. J. (2021). Deep learning for cyber threat detection and analysis. *Journal of Cybersecurity*, 7(1), 1-20.

28. Zhou, Y., Sharma, A., & Debbabi, M. (2022). Machine learning techniques for cyber threat detection in critical infrastructures: A survey. *International Journal of Information Security*, 21(2), 235-260.

29. Braun, V., & Clarke, V. (2021). Thematic analysis: A practical guide. SAGE Publications Ltd.

30. Guest, G., MacQueen, K. M., & Namey, E. E. (2022). *Applied thematic analysis*. SAGE.

31. 5 Best Data Analysis Programming Languages in 2022 (Trending Now). URL: https://dataresident.com/data-analysis-programming-languages/ (дата звернення 8.10.2023).

32. 12 Data Science Programming Languages to Know. URL: https://builtin.com/data-science/data-science-programming-languages (дата звернення 16.10.2023).

33. Threat Detection and Response. URL: https://www.rapid7.com/fundamentals/threat-detection/ (дата звернення 21.10.2023)

34. Top 10 threat detection tools for cybersecurity. URL: https://cybermagazine.com/articles/top-10-threat-detection-tools (дата звернення 30.09.2023).

35. What is Real-time Threat Analysis? URL: https://blog.rsisecurity.com/what-is-real-time-threat-analysis/ (дата звернення 01.10.2023).

36. Time Series Analysis for Cyberthreat Detection and Prevention. URL: https://ieeexplore.ieee.org/document/7041122 (дата звернення 6.10.2023).

37. Real Time Threat Detection: The Facts You Need to Know. URL: https://www.bitlyft.com/resources/real-time-threat-detection-the-facts-you-need-to-know (дата звернення 1.11.2023).

38. Cyber Threat Analysis: Types, Benefits, Tools, Approaches. URL: https://www.knowledgehut.com/blog/security/threat-analysis (дата звернення 25.09.2023).

39. How to Keep Your Network Safe Using Cyber Threat Detection and Response. URL: https://www.forenova.com/threat-detection/guide-to-cybersecurity-threat-detection-and-response (дата звернення 24.10.2023).

40. Daradkeh Y.I., Gorokhovatskyi V., Tvoroshenko I., and Zeghid M. (2022) Tools for fast metric data search in structural methods for image classification, *IEEE Access*, 10, pp. 124738-124746.

41. Гороховатський В.О., Творошенко І.С., Чмутов Ю.В. (2022) Застосування систем ортогональних функцій для формування простору ознак у методах класифікації зображень, *Сучасні інформаційні системи*, 6(3), С. 5-12.

42. Гороховатський В., Передрій О., Творошенко І., Марков Т. (2023) Матриця відстаней для множини компонентів структурного опису як інструмент для створення класифікатора зображень, *Сучасні інформаційні системи*, 7(1), С. 5-13.

43. Pomazan V., Tvoroshenko I., and Gorokhovatskyi V. (2023) Development of an application for recognizing emotions using convolutional neural networks, *International Journal of Academic Information Systems Research*, 7(7), pp. 25-36.

44. Pomazan V., Tvoroshenko I., and Gorokhovatskyi V. (2023) Handwritten character recognition models based on convolutional neural networks, *International Journal of Academic Engineering Research*, 7(9), pp. 64-72.

45. Gorokhovatskyi V., Tvoroshenko I. (2023) Identification of visual objects by the search request. *International scientific symposium «INTELLIGENT SOLUTIONS-S». Computational intelligence (results, problems and perspectives). Decision making theory: proceedings of the international symposium*, September 28, 2023, Kyiv-Uzhorod, Ukraine, pp. 25-27.

46. Yakovleva O., Kovač M., Ardasov V. & Yeremenko I. (2023). Study on adding functionality to the Zoom online conference system for monitoring the participant activities, *Public Administration and Regional Development*, 19(1), pp. 158-184.

47. Стогній Д.Є. (2023). Дослідження чатів із нейронними мережами великих мовних моделей у протиправній діяльності в сфері кіберпростору.