Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 004
DOI: 10.32447/20784643.32.2025.08

А. О. Нікітенко, Є. А. Соболь
Донецький національний технічний університет, м. Дрогобич, Україна
ORCID: https://orcid.org/0009-0006-1363-2324 – А. О. Нікітенко
https://orcid.org/0009-0001-1607-8289 – Є. А. Соболь
andrii.nikitenko@donntu.edu.ua

ІНТЕРАКТИВНА СИСТЕМА ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ У РЕАЛЬНОМУ ЧАСІ НА ОСНОВІ ГЛИБОКОГО НАВЧАННЯ

У статті розглядається актуальна проблема виявлення мережевих вторгнень у режимі реального часу, що є критично важливою в сучасних умовах зростання кількості кіберзагроз та складності атак. Класичні методи детектування, як сигнатурні чи статистичні, мають низку обмежень — зокрема, неспроможність виявляти нові або модифіковані атаки, високу чутливість до налаштувань та обмежену адаптивність. З метою підвищення ефективності виявлення загроз запропоновано програмну систему TraceRanger, яка реалізує сучасну архітектуру мережевої системи виявлення вторгнень на основі глибокого навчання. Система має повнофункціональний графічний інтерфейс, підтримує обробку мережевого трафіка в реальному часі та аналіз за PCAP-файлами. Ключовим компонентом є модифікована гібридна модель CNN–BiGRU–Attention, що поєднує згорткові мережі, двонаправлені рекурентні шари GRU та гібридний механізм уваги для глибшого аналізу потокових характеристик трафіка.

Застосовано методи попередньої обробки та зменшення розмірності (PCA, метаевристичні алгоритми), а також оптимізацію гіперпараметрів для покращення узагальнюючої здатності моделі. Проведено експериментальні дослідження у віртуалізованому середовищі та на основі відкритого набору даних CSE-CIC-IDS-2018, включаючи атаки різного типу (DoS, DDoS, Bruteforce, Bot, SQLi, тощо). За результатами тестування зафіксовано високу точність виявлення загроз, а також підтверджено відповідність типів атак, джерел і IP-адрес, визначених системою, із ground-truth розміткою датасету. Додатково здійснено порівняльний аналіз із системами BGPGuard та Dique, який показав перевагу TraceRanger за точністю, гнучкістю налаштувань і рівнем інтеграції користувача.

Наукова новизна полягає у запропонованій програмній системі TraceRanger, яка забезпечує практичну інтеграцію моделей глибокого навчання у повноцінне середовище виявлення мережевих загроз. На відміну від більшості існуючих досліджень, зосереджених лише на теоретичних аспектах побудови NIDS-моделей, запропонована система реалізує механізм динамічного керування та валідації моделей через стандарт ONNX, а також надає графічний інтерфейс для моніторингу трафіка в реальному часі. Практична значущість полягає у можливості використання системи для навчання фахівців з кібербезпеки, тестування NIDS-моделей, а також для розгортання у лабораторних або корпоративних середовищах моніторингу мережевого трафіка.

Ключові слова: система виявлення мережевих вторгнень, TraceRanger, CNN–BiGRU–Attention, механізм уваги, глибоке навчання

A. O. Nikitenko, Y. A. Sobol
Donetsk National Technical University, Drohobych, Ukraine

INRERACTIVE SYSTEM FOR DETECTING NETWORK INTRUSIONS IN REAL TIME BASED ON DEEP LEARNING

The article examines the urgent problem of detecting network intrusions in real time, which is critically important in today's environment of growing cyber threats and increasingly sophisticated attacks. Classical detection methods, such as signature-based or statistical approaches, have several limitations, including the inability to detect new or modified attacks, high sensitivity to configuration settings, and limited adaptability. To enhance threat detection efficiency, the TraceRanger software system has been proposed. It implements a modern architecture for a network intrusion detection system based on deep learning. The system includes a full-featured graphical interface, supports real-time network traffic processing, and allows PCAP file analysis. The key component is a modified hybrid CNN–BiGRU–Attention model that

combines convolutional neural networks, bidirectional GRU recurrent layers, and a hybrid attention mechanism for more in-depth analysis of traffic stream characteristics.

Preprocessing and dimensionality-reduction methods (PCA, metaheuristic algorithms) were applied, along with hyperparameter optimization to improve the model's generalization ability. Experimental studies were conducted in a virtualized environment and based on the open CSE-CIC-IDS-2018 dataset, which includes various types of attacks (DoS, DDoS, Bruteforce, Bot, SQLi, etc.). The test results demonstrated high accuracy in detecting threats and confirmed that the types of attacks, sources, and IP addresses identified by the system corresponded to the ground-truth labeling of the dataset. In addition, a comparative analysis with the BGPGuard and Dique systems was performed, showing TraceRanger's superiority in terms of detection accuracy, configuration flexibility, and user integration. The proposed solution has practical value as both a monitoring and research tool in network security, with significant potential for further improvement.

The scientific novelty lies in the proposed TraceRanger software system, which enables practical integration of deep learning models into a full-fledged network threat detection environment. Unlike most existing studies that focus solely on the theoretical aspects of building NIDS models, the proposed system implements a mechanism for dynamic control and validation of models through the ONNX standard and provides a graphical interface for real-time traffic monitoring. The practical significance lies in the system's ability to support the training of cybersecurity specialists, the testing of NIDS models, and deployment in laboratory or corporate network traffic monitoring environments.

Keywords: network intrusion detection system, TraceRanger, CNN–BiGRU–Attention, attention mechanism, deep learning.

Вступ. У сучасному цифровому середовищі захист комп'ютерних мереж є одним із ключових завдань кібербезпеки. Зростання кількості користувачів, пристроїв та мережевих сервісів сприяє збільшенню ризиків, пов'язаних із несанкціонованим доступом, витоком даних, атакою з використанням вразливостей тощо. У зв'язку з цим зростає актуальність розробки ефективних систем виявлення мережевих вторгнень (Network Intrusion Detection System – NIDS), здатних функціонувати в реальному часі з високою точністю та мінімальною кількістю хибнопозитивних спрацювань.

Одним із найбільш перспективних напрямів розвитку сучасних засобів захисту є створення програмних систем IDS, що аналізують мережевий трафік з метою виявлення як відомих, так і нових типів атак. Це зумовлює зростаючий інтерес дослідників до тематики NIDS [1]. Загалом IDS є спеціалізованим програмним забезпеченням або апаратно-програмним механізмом, що відстежує трафік для виявлення підозрілої чи аномальної активності та ініціює відповідні дії у відповідь на виявлені загрози [2].

Існуючі підходи до реалізації NIDS можна умовно класифікувати на декілька груп. Класичні системи (наприклад, Snort, Zeek/Bro) ґрунтуються переважно на сигнатурному аналізі та правилах, які дозволяють ефективно виявляти вже відомі типи атак. Водночас вони часто виявляються неефективними у виявленні нових або модифікованих загроз. З цією метою були розроблені системи, що використовують алгоритми машинного навчання (Machine Learning – ML), які навчаються розрізняти нормальну та аномальну поведінку мережевого трафіка. Подальшим етапом розвитку стали моделі глибокого навчання (Deep Learning – DL), зокрема згорткові (Convolutional Neural Networks – CNN), рекурентні (Long Short Term Memory – LSTM, Gated Recurrent Unit – GRU) та гібридні архітектури, які демонструють високі показники точності на відкритих датасетах.

Найбільш перспективними на сьогодні вважаються гібридні моделі, що поєднують переваги різних підходів. Однією з таких архітектур є модифікована модель CNN–BiGRU–Attention, яка дозволяє ефективно виділяти ознаки з мережевого трафіка, враховувати послідовність подій та фокусуватися на найбільш інформативних ознаках завдяки механізму уваги (attention mechanism). Однак, незважаючи на активні дослідження DL-моделей для задач виявлення вторгнень, повноцінні програмні реалізації з інтеграцією таких моделей у графічний інтерфейс для роботи в реальному часі досі майже не представлено в науковій літературі.

Аналіз літературних джерел. Проведено аналіз сучасних підходів до виявлення мережевих вторгнень із використанням методів глибокого навчання. Розглянуто актуальні моделі, зокрема CNN, LSTM, GRU та їхні гібридні комбінації з механізмами уваги, а також існуючі програмні реалізації NIDS. Метою огляду є обґрунтування вибору архітектури CNN–BiGRU–Attention для інтеграції у розроблену систему TraceRanger.

У дослідженні [3] представлено систему Dique, яка реалізує функції виявлення та запобігання DoS-атакам за допомогою глибокої нейронної мережі типу Deep Feedforward Neural Network (DFNN). Для навчання моделі використано датасет CICDDoS2019, де спочатку відібрали 22 найважливіші ознаки, а згодом – для покращення точності – застосовано повний набір із 73 ознак. Найкраща модель досягла accuracy 99,94%, precision – 99,95%, recall – 99,9%, F1-score – 99,93% у бінарній класифікації (benign vs malicious). На відміну від багатьох досліджень,

автори зосередились не лише на теоретичних результатах, а й на практичній реалізації та валідації в польових умовах. Недоліком є використання обмеженої архітектури та тестування моделі лише на DoS-атаках.

У роботі [4] запропоновано систему виявлення мережевих вторгнень у реальному часі, що базується на глибокій нейронній мережі (DNN), навченої на 28 ознаках з набору даних NSL-KDD. Архітектура включає конвеєр машинного навчання з поетапним категоріальним кодуванням і масштабуванням ознак, який застосовується до мережевих даних перед їх передачею в DNN для класифікації. Для обробки трафіка в реальному часі використовується модуль вилучення ознак, розгорнутий між шлюзом і локальною мережею, що дає змогу формувати вхідні дані згідно зі структурою NSL-KDD. Навчена модель разом з конвеєром розміщена на сервері, доступ до якого здійснюється через REST API. За результатами тестування, DNN досягла accuracy – 81%, precision – 96%, recall – 70% та F1-score – 81%. Робота містить детальний технічний опис усіх компонентів реалізованої системи, що може слугувати основою для побудови вдосконалених IDS, здатних до виявлення сучасних типів атак у режимі реального часу. Недоліками роботи є обмеженість набору ознак та використання лише одного набору даних.

У дисертації [5] розглянуто класифікацію мережевих аномалій з використанням традиційних, глибоких та швидких алгоритмів машинного навчання, а також запропоновано два нові варіанти Broad Learning System – VFBLS та VCFBLS. Для підвищення ефективності застосовано різні алгоритми відбору ознак (Fisher, mRMR, autoencoder тощо). Моделі оцінювались за метриками accuracy, precision, recall, F1-score, час навчання та матрицею помилок. У якості наборів даних використано як BGP-трафік під час відомих інцидентів (Slammer, Code Red, WannaCry), так і стандартні датасети NSL-KDD, CICIDS2017, CIC-IDS-2018. Для невеликих вибірок (BGP) найкращі результати показали SVM та HMM, тоді як для великих – BiGRU, BiLSTM та LightGBM. Розроблено власну систему BGPGuard для виявлення аномалій у BGP-трафіка в реальному часі (термінальна та веб-версія). Основними недоліками є неповне охоплення ознак для BGP, обмежене тестування на додаткових наборах даних, відсутність реалізації запропонованих покращень (ESN, Transformers, Self-Attention), високе споживання ресурсів деяких моделей та незавершеність впровадження BGPGuard як повноцінного сервісу.

У роботі [6] запропоновано ReTiNA-IDS – фреймворк для виявлення мережевих вторгнень у реальному часі, що інтегрує інструмент CICFlowMeter із методами машинного навчання (Random Forest та Multi-Layer Perceptron), використовуючи обрані 13 ознак з датасету CSE-CIC-IDS2018. Попередньо проведено очистку даних, балансування та генерацію додаткових даних для FTP-атак шляхом реалістичної емуляції у GNS3. Навчена модель експортується у форматі PMML і вбудовується у CICFlowMeter, який також має GUI для моніторингу трафіка. Систему протестовано в умовах реальної мережі (Windows/Kali), де вона успішно виявляла атаки (DoS, Brute Force, Port Scan) без хибнопозитивних спрацювань, досягнувши точності 100% для всіх класів. Недоліками є відсутність розгляду складних атак, таких як APT або zero-day, модель обмежена лише 13 ознаками, що може зменшити її узагальненість; відсутній порівняльний аналіз з більш сучасними DL-архітектурами.

У роботі [7] представлено RTIDS (Robust Transformer-based Intrusion Detection System) – модель виявлення мережевих вторгнень на основі трансформера, оптимізовану для роботи в реальному часі. Для підвищення ефективності запропоновано попередню класифікацію трафіка за допомогою MLP, після чого застосовано модифікований трансформер для детального аналізу, з урахуванням взаємодій між мережевими ознаками. Модель навчено на наборах даних CIC-IDS2017 та CIC-DDoS2019, де для першого набору даних отримано accuracy 99,35%, precision 98,98%, recall 98,83%, 99,17%, для другого набору даних accuracy 98,58%, precision 98,82%, recall 98.66%, f1-score 98,48% відповідно і продемонструвала стабільність в умовах мультикласової класифікації. Архітектура підтримує паралельну обробку пакетів, що забезпечує високу швидкодію. Недоліком можна назвати те, що модель протестовано лише в офлайн-режимі без розгортання у реальному мережевому середовищі.

У роботі [8] запропоновано метод виявлення мережевих вторгнень TGA, що поєднує Temporal Convolutional Network (TCN), BiGRU та механізм уваги для моделювання часових та просторових залежностей у трафіку. Вектори ознак, отримані в TCN і BiGRU, об’єднуються, а потім вводяться в механізм самонавчання, щоб зафіксувати кореляцію між різними позиціями в послідовності і перепризначити ваги часових ознак для подальшого покращення можливостей моделі. Нарешті, дані надходять до класифікатора для класифікації різних класів мережевого трафіка. Модель навчено на CSE-CIC-IDS-2018, де вона досягла accuracy 97,83%, 97,85%, 97,83%, 97,57%, а також показала переваги

в порівнянні з LSTM, DNN та іншими базовими архітектурами. Завдяки поєднанню TCN і BiGRU забезпечується ефективне вилучення послідовних характеристик, а механізм уваги надає вагу ключовим частинам трафіка. Недоліками є відсутність тестування в реальному середовищі або в умовах реального часу; не оцінено затримку, навантаження на ресурси та можливість розгортання у прикладному середовищі.

У роботі [9] запропоновано модель виявлення вторгнень на основі вдосконаленого трансформатора зору (ViT). Модель використовує механізм уваги для обробки даних, що дозволяє подолати недолік короткочасної пам'яті в рекурентній нейронній мережі (RNN) і складність навчання віддаленої залежності в згортковій нейронній мережі. Для експериментальних досліджень використано публічний набір даних NSL-KDD. За результатами експериментів, accuracy становить 99.68%, рівень помилкових спрацьовувань 0.22%, а recall 99.57%. Недоліком роботи автори зазначають довший час роботи запропонованої моделі порівняно з базовою моделлю ViT та традиційними алгоритмами машинного навчання.

Проведений аналіз літературних джерел показав, що більшість досліджень у сфері NIDS зосереджені на розробці та експериментальній перевірці моделей машинного навчання на відкритих наборах даних в офлайн-режимі. Водночас лише поодинокі роботи приділяють увагу інтеграції таких моделей у повноцінні програмні системи з графічним інтерфейсом і їх тестуванню в умовах, наближених до реального середовища. Відтак, особливої актуальності набуває наукова задача, що передбачає створення, експериментальне дослідження й практичну реалізацію системи виявлення із перевіркою ефективності моделей безпосередньо у програмному комплексі

Методи досліджень. У ході дослідження використано методи аналізу літературних джерел для вивчення сучасних підходів до виявлення мережевих атак, а також системний підхід для проектування архітектури програмної системи TraceRanger. Проведено експериментальне тестування у віртуалізованому середовищі з використанням PCAP-файлів, що містять різні типи атак, із подальшим аналізом результатів. Для побудови моделі застосовано методи глибокого навчання, оптимізації та зниження розмірності ознак, а також порівняльну оцінку з існуючими системами.

Мета і завдання досліджень. Метою статті є створення та оцінювання ефективності програмної реалізації системи виявлення мережевих вторгнень TraceRanger, інтегрованої з модифікованою моделлю CNN–BiGRU–Attention для обробки трафіка в режимі реального часу. У межах дослідження проведено оцінку ефективності запропонованого рішення на експериментальному трафіку з використанням сучасних метрик, а також здійснено порівняння з іншими підходами. Для досягнення мети необхідно вирішити такі завдання:

- створити повнофункціональну програмну реалізацію сучасної системи виявлення мережевих вторгнень;
- інтегрувати та протестувати натреновану модифіковану модель CNN-BiGRU-Attention у практичному середовищі;
- провести порівняльний аналіз із існуючими підходами та оцінити переваги і обмеження запропонованого рішення.

Результати дослідження. Розроблена програмна система TraceRanger реалізує функціонал NIDS із можливістю роботи в режимі реального часу та аналізу попередньо записаного трафіка. Архітектура системи побудована на основі принципів *Clean Architecture*, що забезпечує чітке розділення інфраструктурних компонентів і користувацького інтерфейсу, а також використовує шаблон *Model-View-ViewModel (MVVM)* для підвищення модульності й підтримуваності коду. На рисунку 1 представлено концептуальну схему архітектури TraceRanger, яка відображає ключові підсистеми, їхню взаємодію між модулями.

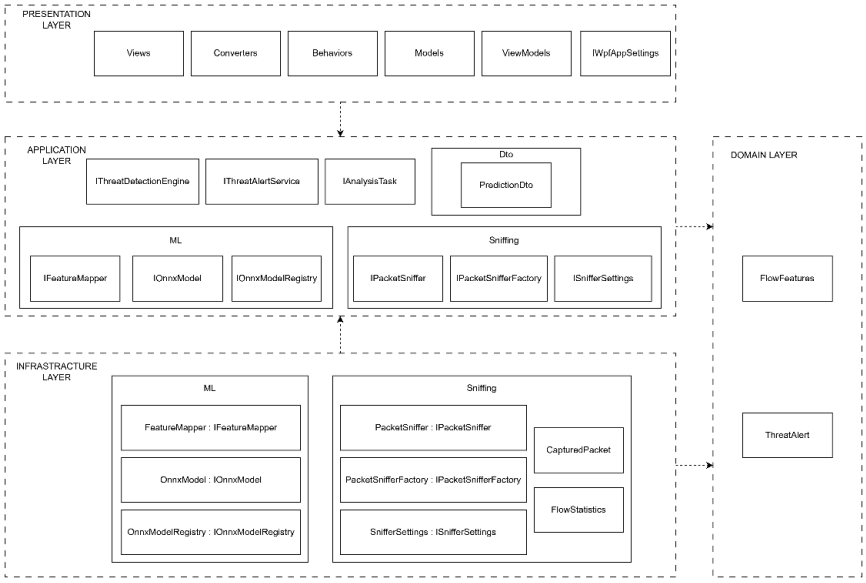

Рисунок 1 – Концептуальна схема архітектури TraceRanger

Нижній рівень реалізує захоплення трафіка через бібліотеку SharpPcap, після чого пакети агрегуються у потоки за п’ятиелементним ключем та передаються в модуль екстракції ознак. Вектор ознак далі надходить до диспетчера, який розподіляє його між аналітичними завданнями та передає на вхід моделі машинного навчання у форматі ONNX. Результати класифікації аналізуються, і в разі виявлення загрози активується механізм реагування, що забезпечує логування, блокування, сповіщення користувача та інші дії, відповідно до налаштувань.

Архітектура підтримує інтеграцію моделей машинного навчання через ONNX Runtime, що дозволяє використовувати попередньо натреновані моделі без їхнього повторного тренування у середовищі користувача. Завдяки цьому досягається гнучкість системи та її здатність до подальшого розширення шляхом інтеграції додаткових моделей. Щоб проілюструвати взаємодію користувача із системою, на **рисунку 2** наведено діаграму варіантів використання TraceRanger.

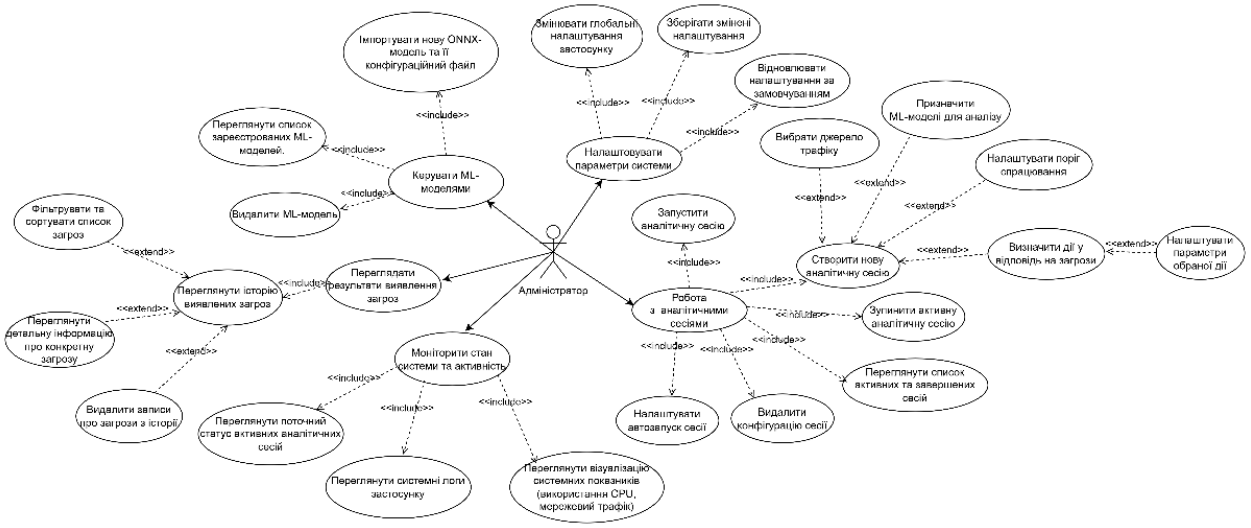

Рисунок 2 – Діаграма варіантів використання

Основним актором виступає адміністратор, який має змогу конфігурувати аналітичні сесії, імпортувати й керувати моделями машинного навчання, переглядати історію виявлених загроз і системних журналів, а також змінювати налаштування системи та ініціювати відповідні дії.

Графічний інтерфейс системи реалізовано на основі технології WPF із використанням бібліотеки WPF UI, що забезпечує сучасний вигляд, зручність у користуванні та чітку інтеграцію з бізнес-логікою. Після встановлення користувач отримує доступ до головного вікна-дешборду, яке представлено на рисунку 3.

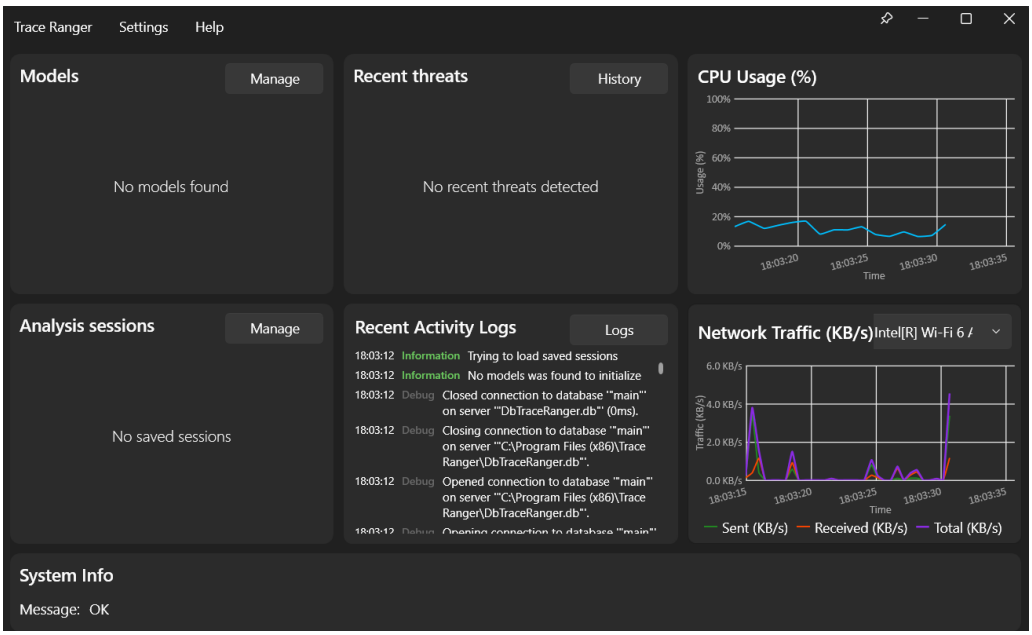

Рисунок 3 – Головне вікно застосунку TraceRanger

У верхній частині вікна розташовано меню для переходу до різних функцій, тоді як основну область займають віджети зі списком активних сесій, нещодавно виявленими загрозами, журналами подій та графіками завантаження процесора й мережевої активності що дозволяє адміністратору швидко оцінити поточний стан системи та оперативно реагувати на інциденти.

Система також передбачає можливість імпорту моделей машинного навчання, конфігурації аналітичних сесій у різних режимах (захоплення живого трафіка, аналіз PCAP-файлів, захоплення з одночасним створенням датасету), керування журналами та перегляду детальної історії інцидентів.

Сукупність зазначених архітектурних рішень і функціональних можливостей надає системі TraceRanger необхідну адаптивність для ефективного виявлення загроз у широкому спектрі мережевих сценаріїв.

Використання моделі CNN-BiGRU-Attention. У попередніх роботах розроблено та досліджено гібридну архітектуру глибокої нейронної мережі CNN-BiGRU-Attention [10], яка поєднує згорткові шари, двоспрямовані GRU та механізм уваги з метою підвищення точності та інтерпретованості NIDS. Така архітектура враховує, що мережевий трафік має одночасно локальні просторові та глобальні послідовні залежності, а також високу частку нерелевантних ознак, що ускладнює процес навчання.

Архітектура моделі передбачає, що CNN-шари виконують роль детекторів локальних ознак, виділяючи ключові статистичні та протокольні шаблони з матриці ознак потоку. Далі BiGRU-шари опрацьовують послідовності ознак у прямому та зворотному напрямках, моделюючи причинно-наслідкові зв’язки та контекст. Нарешті, механізм уваги**,** інтегрований поверх BiGRU, акцентує вагу моделі на найбільш інформативних фрагментах потоку, що підвищує її узагальнювальну здатність та інтерпретованість. Важливою інновацією є використання гібридного механізму уваги**,** що поєднує *self-attention* та *dynamic local attention*, реалізованих через динамічне налаштування вікна уваги (*MorphingLocalAttention*). На рисунку 4 наведено схему архітектури CNN-BiGRU-Attention.

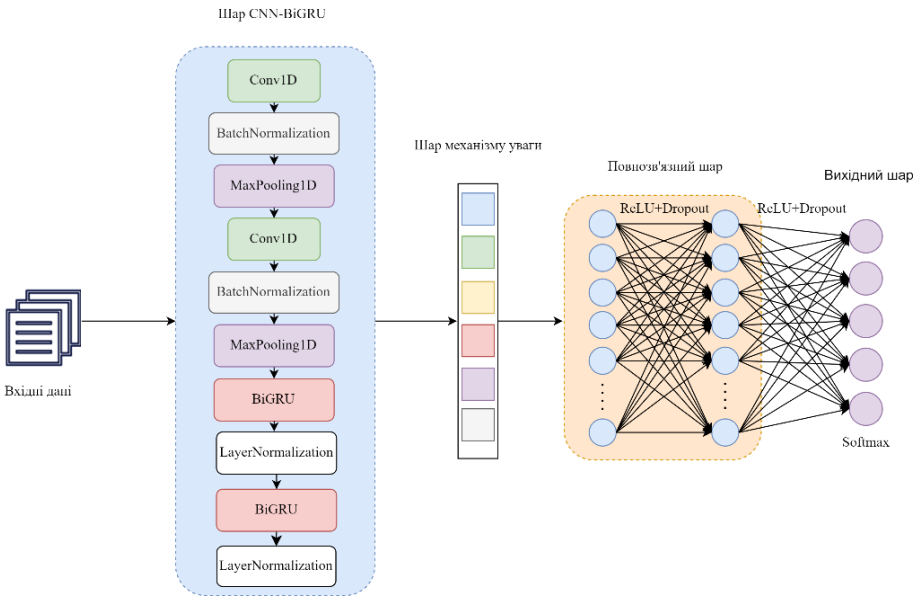

Рисунок 4 – Архітектура CNN-BiGRU-Attention [9]

Такий підхід дозволяє під час навчання оптимально регулювати ширину вікна локальної уваги, підлаштовуючи модель під властивості конкретного завдання та забезпечуючи кращу здатність до узагальнення порівняно з традиційними локальними чи глобальними варіантами [10].

Для налаштування моделі використано гіперпараметричну оптимізацію за допомогою *Optuna*, що дозволило підібрати оптимальні значення ключових параметрів (кількість фільтрів CNN, розміри GRU, коефіцієнти dropout тощо). Навчання та тестування проведено на еталонних наборах даних NSL-KDD, UNSW-NB15 та CSE-CIC-IDS2018 із використанням стандартних метрик – точність, precision, recall, F1-score, а також *false positive rate* для комплексної оцінки.

Отримані експериментальні результати показали, що модель з гібридним механізмом уваги досягає найвищих значень точності як на навчальних, так і на тестових вибірках, перевершуючи сучасні підходи за всіма ключовими метриками. Додатково застосування методів зменшення розмірності та оптимізації ознак забезпечило скорочення часу тренування та підвищення ефективності при мінімальних обчислювальних витратах. Крім того, модель додатково дотреновано на завчасно підготовленому наборі даних [11], що дозволило адаптувати її до нових умов та розширеного простору ознак. Для цього реалізовано методику точного налаштування (fine-tuning), яка передбачала завантаження попередньо навченої моделі та заморожування всіх її шарів, окрім останніх, з подальшим перенавчанням вихідного шару на нових даних. Попередньо дані очищено від пропущених та некоректних значень, нормалізовано та закодовано, після чого проведено донавчання на 21 клас із використанням оптимізатора Adam та функції втрат categorical_crossentropy. Результати донавчання продемонстрували помірне, але стабільне покращення показників точності, precision, recall та F1-score порівняно з базовою моделлю: наприклад, точність зросла з 99,41 % до 99,44 %, а FPR знизився з 0,0035 до 0,0033. Це свідчить про наявність у зібраному наборі даних релевантної інформації для підвищення ефективності класифікації та підтверджує перспективність підходу до формування локальних навчальних вибірок.

Експериментальна оцінка. Для оцінки працездатності та ефективності запропонованої системи TraceRanger проведено серію експериментів у контрольованих умовах, які моделювали реальні сценарії атак на корпоративну мережу. Метою є перевірка здатності системи виявляти широкий спектр атак як у режимі реального часу, так і при аналізі попередньо записаних файлів трафіка, а також порівняти її продуктивність із альтернативними підходами.

Використано тестове середовище, яке реалізовано на базі локальної бездротової мережі, до якої підключено два ноутбуки. Один із них, під керуванням Ubuntu 24,04, виконував роль атакуючого хоста та використовував три Docker-контейнери з Kali Linux для запуску атак різних типів. Інший ноутбук, із встановленою Windows 10, виступав цільовим вузлом, на якому розгорнуто систему TraceRanger та HTTP-сервер на порту 80. На рисунку 5 подано схему експериментального середовища.

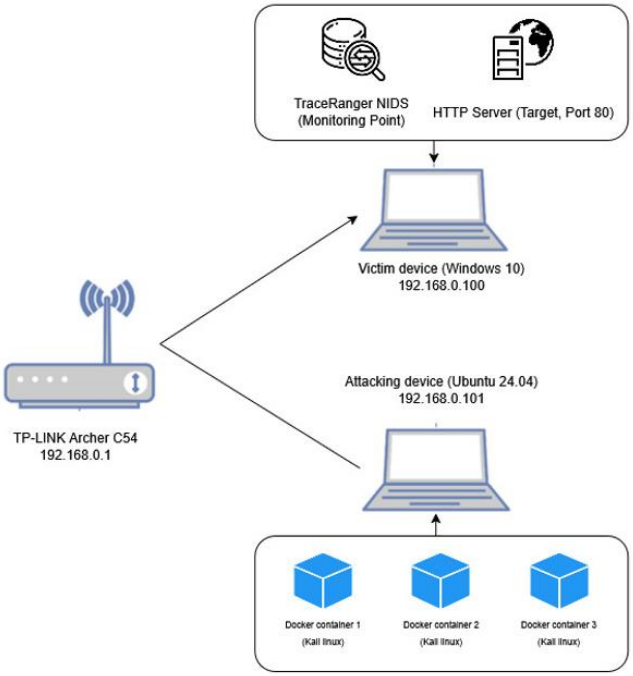

Рисунок 5 – Схема експериментального середовища

Обидва пристрої підключено до однієї локальної мережі через Wi-Fi роутер, що забезпечило прямий обмін трафіком між учасниками експерименту. Параметр Confidence у Trace Ranger встановлено на рівні 0,5, що відповідає середньому рівню впевненості системи у виявленні потенційної загрози. Час виконання кожної атаки дорівнює 15 хвилинам. За результатами експерименту система Trace Ranger успішно ідентифікувала кожен тип атаки, що підтверджується відповідними повідомленнями, які надсилались користувачеві через центр сповіщень Windows. Як видно з рисунка 6, при проведенні атак TraceRanger почав повідомляти користувача про атаки на систему, в цей момент користувач може побачити у вікні “Recent threats” всю інформацію про атаку: тип, з якого порту, час атаки та значення параметра Confidence, також автоматично користувач отримує повідомлення в центрі сповіщення Windows.

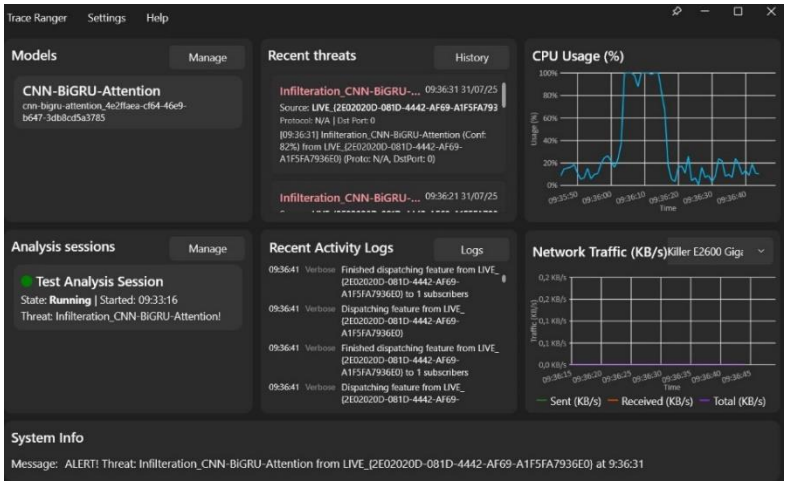

Рисунок 6 – Результат виявлення атак в режимі реального часу

Для комплексної оцінки здатності системи Trace Ranger ідентифікувати аномальну активність та відомі типи атак на основі попередньо записаного мережевого трафіка проведено серію тестових запусків з використанням PCAP-файлів з набору даних CSE-CIC-IDS-2018 [12]. Зокрема, для аналізу обрано найрепрезентативніші типи атак, серед яких *Infiltration, Botnet, Slowloris, Brute Force (SSH/FTP)*, *SQL Injection* та *SlowHTTPTest*. Відповідні .pcap-файли містять мережевий трафік, що імітує реальні сценарії зловмисної активності.

Методика тестування передбачала послідовне завантаження кожного файлу у застосунок TraceRanger для повного офлайн-аналізу. Система функціонувала у пасивному режимі, генеруючи відповідні повідомлення про виявлені загрози у

графічному інтерфейсі користувача та реєструючи події у внутрішньому журналі без впливу на середовище виконання.

У процесі тестування спостерігалася стабільна робота нейромережевої моделі з **рівнем впевненості у класифікації загроз на рівні 81–86 %**, що є прийнятним показником для задач виявлення аномалій у реальному трафіку. Узагальнені результати виявлення подано в таблиці 1.

Таблиця 1

Результати виявлення атак у TraceRanger на основі аналізу .pcap файлів CIC-IDS-2018

Тип атаки	Відсоток виявлення, %	Середній рівень впевненості,%
Infiltration	100	83
Bot	100	84
Slowloris	100	86
BruteForce	100	84
SQL Injection	100	85
SlowHTTPTest	100	86

Аналіз вихідних даних системи підтвердив, що розроблений конвеєр обробки даних, включаючи екстракцію ознак, їх попередню обробку та класифікацію за допомогою інтегрованої моделі, функціонує коректно. Система успішно ідентифікувала потоки, що відповідали сигнатурам атак, присутніх у тестових файлах, та класифікувала їх з достатнім рівнем впевненості, що перевищував встановлений поріг. Водночас, при аналізі сегментів трафіка, відомих як нормальні Benign згідно з описом датасету, система не генерувала сповіщень про загрози, що свідчить про адекватну розрізнювальну здатність моделі та низький рівень хибних спрацювань на відомому нормальному трафіку. Отже інтегрована модель CNN-BiGRU-Attention та вся система обробки даних в Trace Ranger ефективно функціонують для виявлення заздалегідь відомих типів вторгнень при аналізі записаного трафіка. У таблиці 2 представлено результати порівняльного аналізу запропонованого підходу з існуючими рішеннями, що дозволяє оцінити його ефективність відносно відомих методів

Таблиця 2

Порівняльний аналіз з існуючими рішеннями

Критерій	TraceRanger	Dique [3]	BGPGuard [5]
Призначення	Виявлення мережевих вторгнень в реальному часі	Виявлення та запобігання DoS-атакам	Виявлення аномалій BGP у режимах реального часу та офлайн
Модель	Можливість використання ML-моделей на базі ONNX	Multi-layer Deep Feedforward NN	Broad Learning System (BLS), VFBLS/VCFBLS з інкрементним навчанням
Архітектура	Clean Architecture, MVVM, GUI на WPF, підтримка ONNX моделей	GUI з режимами IDS/IPS, простий, з відображенням потоків	CLI та веб-додаток з інтеграцією різних ML-моделей та модулів
Графічний інтерфейс	Сучасний GUI: дашборд з віджетами, журналами, конфігуруванням	Базовий GUI для моніторингу та перемикання між IDS та IPS	Базовий GUI для перегляду BGP подій, також консольна версія
Підтримувані дані	Мережевий трафік	Мережевий трафік із DoS атаками	BGP оновлення та маршрутизаційні аномалії
Обмеження	Працює лише на Windows, немає підтримки складних zero-day/APT, потребує тестування під навантаженням	Тільки DoS, немає розгортання в реальному середовищі, немає комплексної перевірки	Орієнтована лише на BGP, відсутня інтеграція з «загальним» трафіком

На основі порівняльного аналізу представлених систем зроблено висновок, що **TraceRanger** має низку переваг, які виділяють його серед аналогів. Насамперед система підтримує інтеграцію різних моделей машинного навчання завдяки використанню формату ONNX, що забезпечує гнучкість та можливість адаптації до різних сценаріїв виявлення атак. Крім того, TraceRanger оснащено сучасним графічним інтерфейсом користувача, реалізованим на базі WPF із дашбордом, інтерактивними віджетами, журналами подій і зручними механізмами керування, що значно підвищує зручність і швидкість взаємодії адміністратора із системою порівняно з більш примітивними інтерфейсами BGPGuard та Dique. Завдяки підтримці як реального часу, так і аналізу записаних файлів, TraceRanger демонструє високу універсальність і придатність для застосування в різноманітних мережевих середовищах, що, разом із низьким рівнем хибнопозитивних спрацювань і підтвердженою ефективністю на еталонних наборах даних, робить його більш практичним і перспективним рішенням.

Висновки. У результаті виконання поставлених завдань:

1. Розроблено повнофункціональну програмну систему TraceRanger, яка реалізує сучасний підхід до виявлення мережевих вторгнень із можливістю обробки трафіка в реальному часі та аналізу попередньо записаних файлів.

2. У систему інтегровано модифіковану гібридну модель CNN–BiGRU–Attention, що поєднує згорткові шари, двоспрямовані GRU та гібридний механізм уваги. Модель продемонструвала високу точність класифікації та низький рівень хибнопозитивних спрацювань.

3. Експериментальне тестування у віртуалізованому середовищі та на основі датасету CSE-CIC-IDS-2018 підтвердило коректність функціонування конвеєра обробки даних і здатність системи ідентифікувати різні типи атак із середнім рівнем впевненості 81–86 %.

4. Порівняльний аналіз із відомими системами (BGPGuard, Dique) показав перевагу TraceRanger щодо точності виявлення атак, гнучкості інтеграції, сучасного графічного інтерфейсу та підтримки різних моделей ML.

5. Визначено напрями подальшого розвитку системи, зокрема:

- оптимізація затримок обробки та зменшення споживання ресурсів;
- розширення набору підтримуваних типів атак, включно з багатостадійними та zero-day сценаріями;
- реалізація кросплатформенності для підтримки інших операційних систем;
- впровадження онлайн-навчання та адаптивного оновлення моделей;
- масштабне тестування продуктивності під високими навантаженнями.

6. Обґрунтовано наукову новизну, що запропонована програмна система TraceRanger, яка забезпечує інтеграцію моделей глибокого навчання через стандарт ONNX у повнофункціональне середовище виявлення мережевих загроз. Запропоноване рішення усуває розрив між теоретичними дослідженнями та їх практичним застосуванням, забезпечуючи моніторинг трафіка й аналіз загроз у реальному часі.

7. Отримані результати підтверджують ефективність та практичну цінність TraceRanger як інструменту для моніторингу, аналізу та дослідження мережевих загроз у реальному часі з потенціалом подальшого вдосконалення.

Список літератури:

1. Ozkan-Okay M., Samet R., Aslan O., Gupta D. A Comprehensive Systematic Literature Review on Intrusion Detection Systems. *IEEE Access*. 2021. Vol. 9. P.157727-157760. DOI: 10.1109/ACCESS. 2021.3129336.

2. Hnamte V., Hussain J. DCNNBiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System. *Telematics and Informatics Reports*. 2023. Vol. 10.
DOI: 10.1016/j.teler.2023.100053.

3. Garcia J. F. C., Blandon G. E. T. A Deep Learning-Based Intrusion Detection and Preventation System for Detecting and Preventing Denial-of-Service Attacks. *IEEE Access*. 2022. P. 1.
DOI: 10.1109/access.2022.3196642.

4. Thirimanne S.P., et al. Deep Neural Network Based Real-Time Intrusion Detection System. *SN Computer Science*. 2022. Vol. 3, no. 2. DOI: 10.1007/s42979-022-01031-1.

5. Zhida Li. Machine Learning for Classifying Anomalies and Intrusions in Communication Networks. Ph.D, 2022, British Columbia, Canada, p. 196.

6. Murtaj E., Marcantoni F., Loreti M., Quadrini M., Witchel H. Real-Time Intrusion Detection via Machine Learning Approaches. Proceedings of the Ital-IA Intelligenza Artificiale, Naples, Italy, ay 29-30, 2024, CEUR-WS.org. URL: https://ceur-ws.org/Vol-3762/582.pdf

7. Wu Z. et al. RTIDS: a robust transformer-based approach for intrusion detection system. *IEEE Access*. 2022. P. 1. DOI: 10.1109/access.2022.3182333.

8. Song Y. et al. TGA: A Novel Network Intrusion Detection Method Based on TCN, BiGRU and Attention Mechanism. *Electronics*. 2023. Vol. 12, no. 13. P. 2849. DOI: 10.3390/electronics 12132849.

9. Yang Y. et al. Intrusion detection: A model based on the improved vision transformer. *Trans Emerging Tel Tech*. 2022. Vol. 33. DOI:10.1002/ett.4522.

10. Nikitenko A., Bashkov Y. Construction of a network intrusion detection system based on a convolutional neural network and a bidirectional gated recurrent unit with attention mechanism. Eastern-European Journal of Enterprise Technologies. 2024. Vol. 3, No. 9(129). P. 6-15. DOI: 10.15587/1729-4061.2024.305685.

11. Нікітенко А. Процес створення авторського датасету для донавчання моделей систем виявлення мережевих вторгнень на основі глибокого навчання. Вісник Херсонського національного технічного університету. 2025. Т. 2, № 2(93). С. 256-265. DOI: 10.35546/kntu2078-4481.2025.2.2.30.

12. CSE-CIC-IDS2018. Canadian Institute for Cybersecurity. Режим доступу: https://www.unb.ca/cic/datasets/ids-2018.html

References:

1. Ozkan-Okay, M. *et al.* (2021). 'A comprehensive systematic literature review on Intrusion Detection Systems', *IEEE Access*, 9, pp. 157727-157760. doi:10.1109/access.2021.3129336.

2. Hnamte, V. and Hussain, J. (2023). 'DCNNBILSTM: An efficient hybrid deep learning-based Intrusion Detection System', *Telematics and Informatics Reports*, 10, p. 100053. doi:10.1016/j.teler.2023.100053.

3. Canola Garcia, J.F. and Blandon, G.E. (2022). 'A deep learning-based intrusion detection and preventation system for detecting and preventing denial-of-service attacks', *IEEE Access*, 10, pp. 83043-83060. doi:10.1109/access.2022.3196642.

4. Thirimanne, S.P. *et al.* (2022). 'Deep neural network based real-time intrusion detection system', *SN Computer Science*, 3(2). doi:10.1007/s42979-022-01031-1.

5. Zhida Li (2022). Machine Learning for Classifying Anomalies and Intrusions in Communication Networks. Ph.D, 2022, British Columbia, Canada.

6. Murtaj E., Marcantoni F., Loreti M., Quadrini M., Witchel H. (2024). *Real-time intrusion detection via machine learning*. Available at: https://ceur-ws.org/Vol-3762/582.pdf.

7. Wu, Z. *et al.* (2022). 'RTIDS: A robust transformer-based approach for Intrusion Detection System', *IEEE Access*, 10, pp. 64375-64387. doi:10.1109/access.2022.3182333.

8. Song, Y. *et al.* (2023). 'TGA: A novel network intrusion detection method based on TCN, BiGRU and attention mechanism', *Electronics*, 12(13), p. 2849. doi:10.3390/electronics12132849.

9. Yang Y. *et al.* (2022). 'Intrusion detection: A model based on the improved vision transformer', *Trans Emerging Tel Tech*. 33(9). doi:10.1002/ett.4522.

10. Nikitenko, A. and Bashkov, Y. (2024) 'Construction of a network intrusion detection system based on a convolutional neural network and a bidirectional gated rЬIecurrent unit with attention mechanism', *Eastern-European Journal of Enterprise Technologies*, 3(9 (129)), pp. 6-15. doi:10.15587/1729-4061.2024.305685.

11. Nikitenko A. (2025). 'The process of creating an autor's dataset for retraining models of network intrusion detection systems based on deep learning', *Visnyk Of Kherson National Technical University*, Vol. 2, No. 2(93), pp. 256-265. doi:10.35546/kntu2078-4481.2025.2.2.30.

12. CSE-CIC-IDS2018. Canadian Institute for Cybersecurity. Available at: https://www.unb.ca/cic/datasets/ids-2018.html

Науково-методична стаття.
Надійшла до редакції 01.09.2025.
Прийнято до публікації 26.11.2025.