ДОДАТОК А

Звіт результатів перевірки на унікальність тексту в базі ХНУРЕ

StrikePlagiarism.com

Дата звіту 6/16/2025
Дата редагування ---

Звіт не був оцінений

Звіт подібності

метадані

Назва організації
Kharkiv National University of Radio Electronics

Заголовок
2025_М_ПІ_ІПЗм-23-4_Трипілка_А_В_скорочений

Автор / Науковий керівник / Експерт
Трипілка Андрій ВолодимировичКравец Н.С./Нечволод В.Ю.

підрозділ
каф. ПІ

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

0.45% 0.45% КП 1

1.84% 1.84% КЦ

25	10168	80882
Довжина фрази для коефіцієнта подібності 2	Кількість слів	Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	0
Інтервали	A→	0
Мікропробіли		0
Білі знаки	ß	0
Парафрази (SmartMarks)	a	1

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://link.springer.com/content/pdf/10.1007/s10922-020-09512-5.pdf	13 0.13 %
2	1-3 (2).pdf [redacted] 12/19/2024 East Ukrainian National University named after Volodymyr Dahl (East Ukrainian National University named after Volodymyr Dahl)	11 0.11 %
3	https://link.springer.com/content/pdf/10.1007/s10462-021-10037-9.pdf	11 0.11 %

Рисунок А.1 – Перша сторінка звіту на унікальність

4	https://link.springer.com/content/pdf/10.1007/s10462-021-10037-9.pdf	11 0.11 %

з бази даних RefBooks (0.00 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

з домашньої бази даних (0.00 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

з програми обміну базами даних (0.11 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	1-3 (2).pdf [redacted] 12/19/2024 East Ukrainian National University named after Volodymyr Dahl (East Ukrainian National University named after Volodymyr Dahl)	11 (1) 0.11 %

з Інтернету (0.34 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://link.springer.com/content/pdf/10.1007/s10462-021-10037-9.pdf	22 (2) 0.22 %
2	https://link.springer.com/content/pdf/10.1007/s10922-020-09512-5.pdf	13 (1) 0.13 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

1

ВСТУП

Сучасний розвиток інформаційних технологій призвів до значного зростання обсягів зашифрованого мережевого трафіку, що ускладнило завдання виявлення кіберзагроз. Зокрема, особливу небезпеку для хмарних систем становлять DDoS-атаки, які можуть здійснюватися через шифровані з'єднання, маскуючись під легітимну активність.

Метою цієї роботи є дослідження методів виявлення зашифрованого зловмисного трафіку з акцентом на DDoS-атаки у хмарному середовищі та розробка прототипу системи виявлення на основі рекурентних нейронних мереж (RNN) у поєднанні з AutoEncoder. Основними завданнями дослідження є аналіз сучасних підходів до обробки зашифрованого трафіку, вивчення методів збору та аналізу мережевих потоків, дослідження ефективності RNN та AutoEncoder у задачах виявлення аномалій, а також формування теоретичних рекомендацій щодо побудови архітектури системи.

Об'єктом дослідження є процеси аналізу зашифрованого трафіку в хмарних середовищах з метою виявлення DDoS-атак. Предметом дослідження є методи машинного навчання, зокрема RNN та AutoEncoder, які дозволяють виявляти аномальні шаблони поведінки у мережевих потоках.

У ході роботи використовуються такі методи: аналіз літературних джерел з кібербезпеки та глибокого навчання, обробка даних мережевого трафіку, побудова та навчання моделей RNN та AutoEncoder, експериментальна перевірка ефективності моделей на тестових датасетах. Такий підхід дозволяє глибше дослідити особливості виявлення шкідливої активності у зашифрованому трафіку та сформувати практичні рекомендації щодо впровадження систем захисту в хмарних середовищах.

Очікувані результати дослідження включають створення теоретичної основи для побудови інтелектуальних систем виявлення DDoS-атак у зашифрованому трафіку, а також розробку прототипу рішення, що забезпечує ефективний моніторинг мережевого трафіку та підвищує рівень безпеки хмарних сервісів.

Рисунок А.2 – Друга сторінка звіту на унікальність

ДОДАТОК Б

Слайди презентації

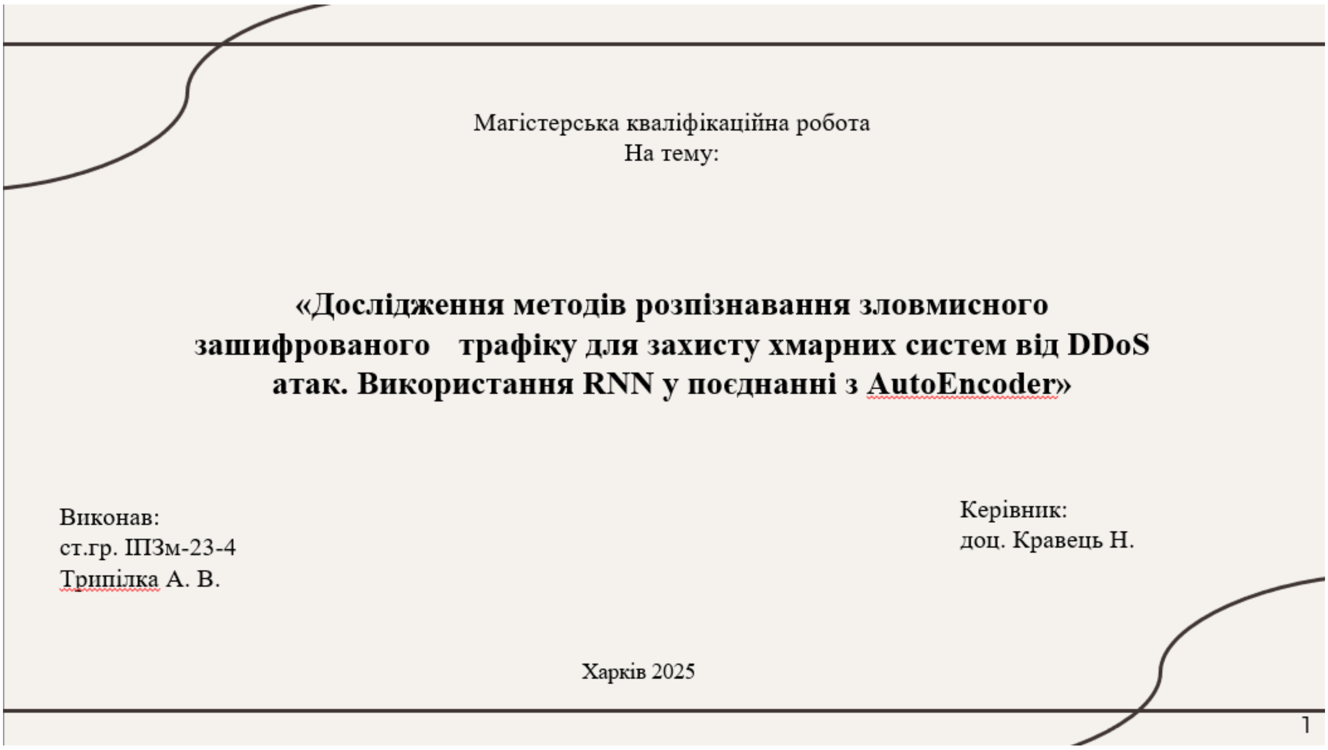
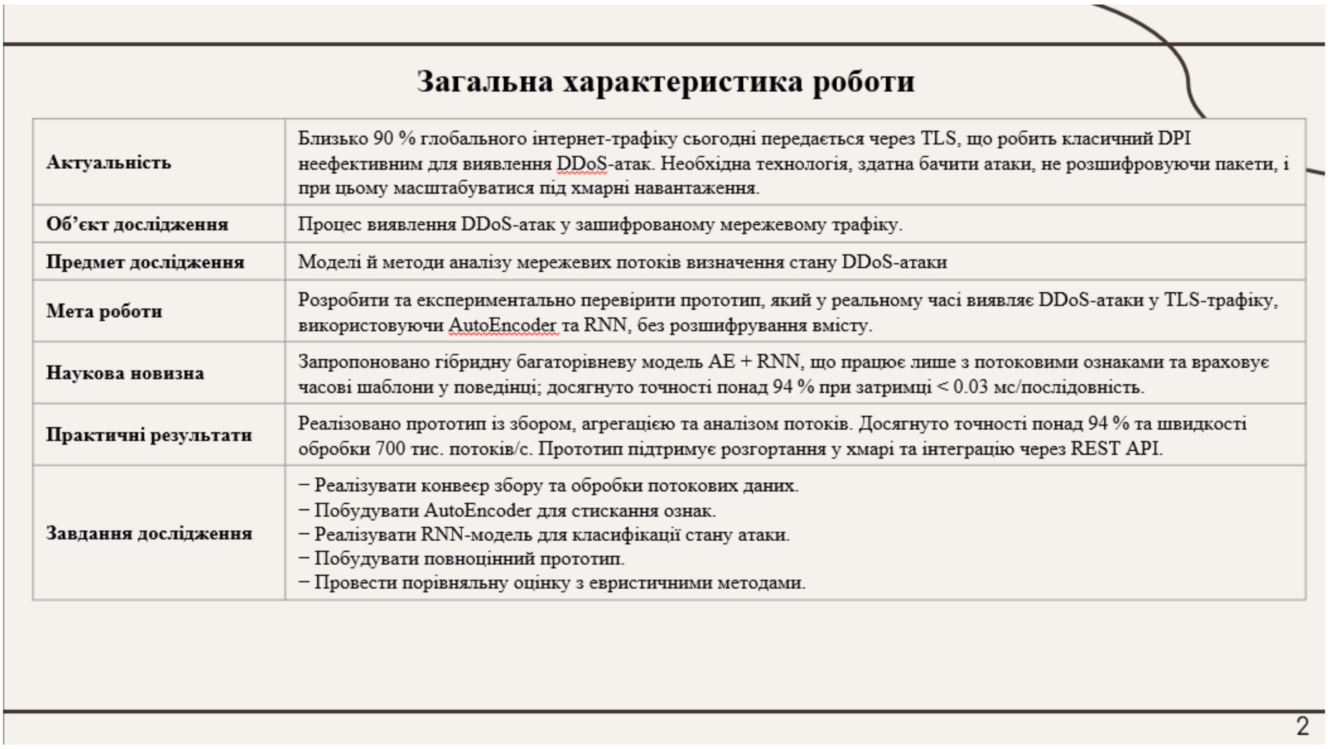


Рисунок Б.1 – слайд 1 (рисунок виконано самостійно)

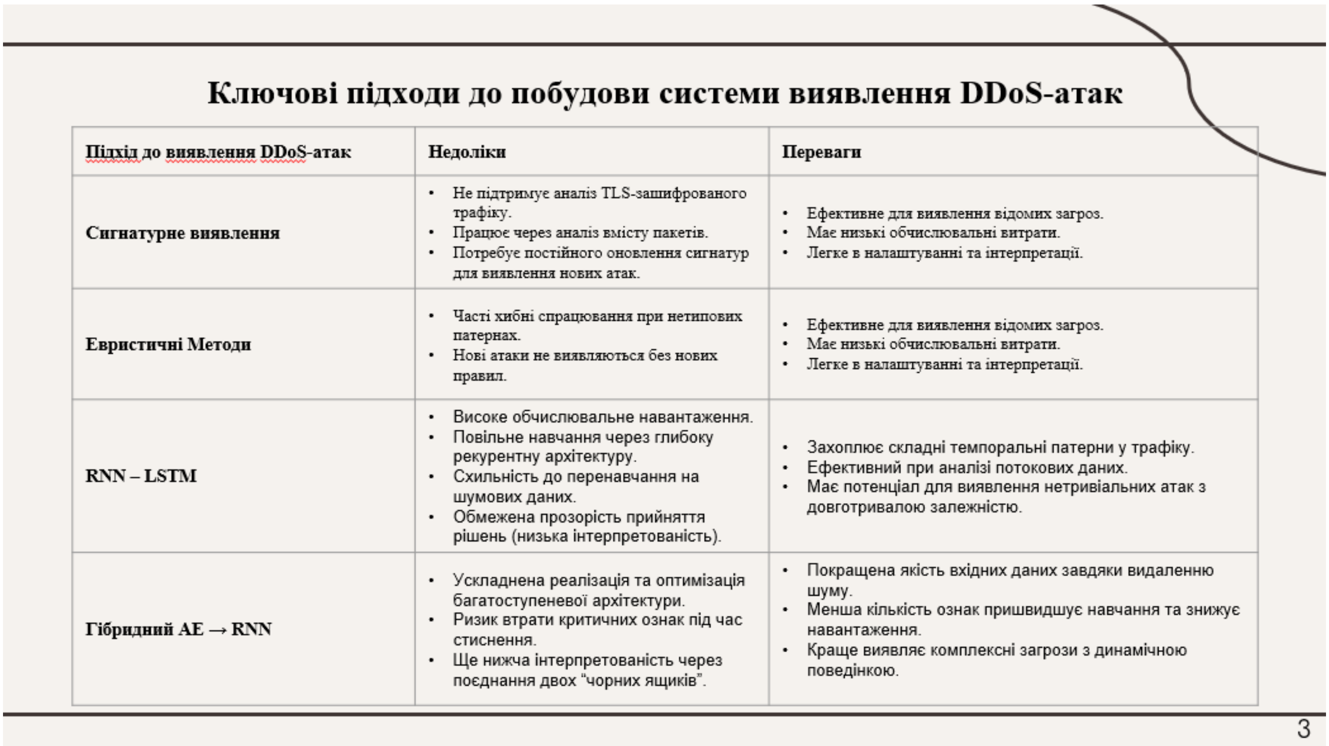


Загальна характеристика роботи

Актуальність	Близько 90 % глобального інтернет-трафіку сьогодні передається через TLS, що робить класичний DPI неефективним для виявлення DDoS-атак. Необхідна технологія, здатна бачити атаки, не розшифровуючи пакети, і при цьому масштабуватися під хмарні навантаження.
Об'єкт дослідження	Процес виявлення DDoS-атак у зашифрованому мережевому трафіку.
Предмет дослідження	Моделі й методи аналізу мережевих потоків визначення стану DDoS-атаки
Мета роботи	Розробити та експериментально перевірити прототип, який у реальному часі виявляє DDoS-атаки у TLS-трафіку, використовуючи AutoEncoder та RNN, без розшифрування вмісту.
Наукова новизна	Запропоновано гібридну багаторівневу модель AE + RNN, що працює лише з потоковими ознаками та враховує часові шаблони у поведінці; досягнуто точності понад 94 % при затримці < 0.03 мс/послідовність.
Практичні результати	Реалізовано прототип із збором, агрегацією та аналізом потоків. Досягнуто точності понад 94 % та швидкості обробки 700 тис. потоків/с. Прототип підтримує розгортання у хмарі та інтеграцію через REST API.
Завдання дослідження	– Реалізувати конвеєр збору та обробки потокових даних. – Побудувати AutoEncoder для стискання ознак. – Реалізувати RNN-модель для класифікації стану атаки. – Побудувати повноцінний прототип. – Провести порівняльну оцінку з евристичними методами.

2

Рисунок Б.2 – слайд 2 (рисунок виконано самостійно)

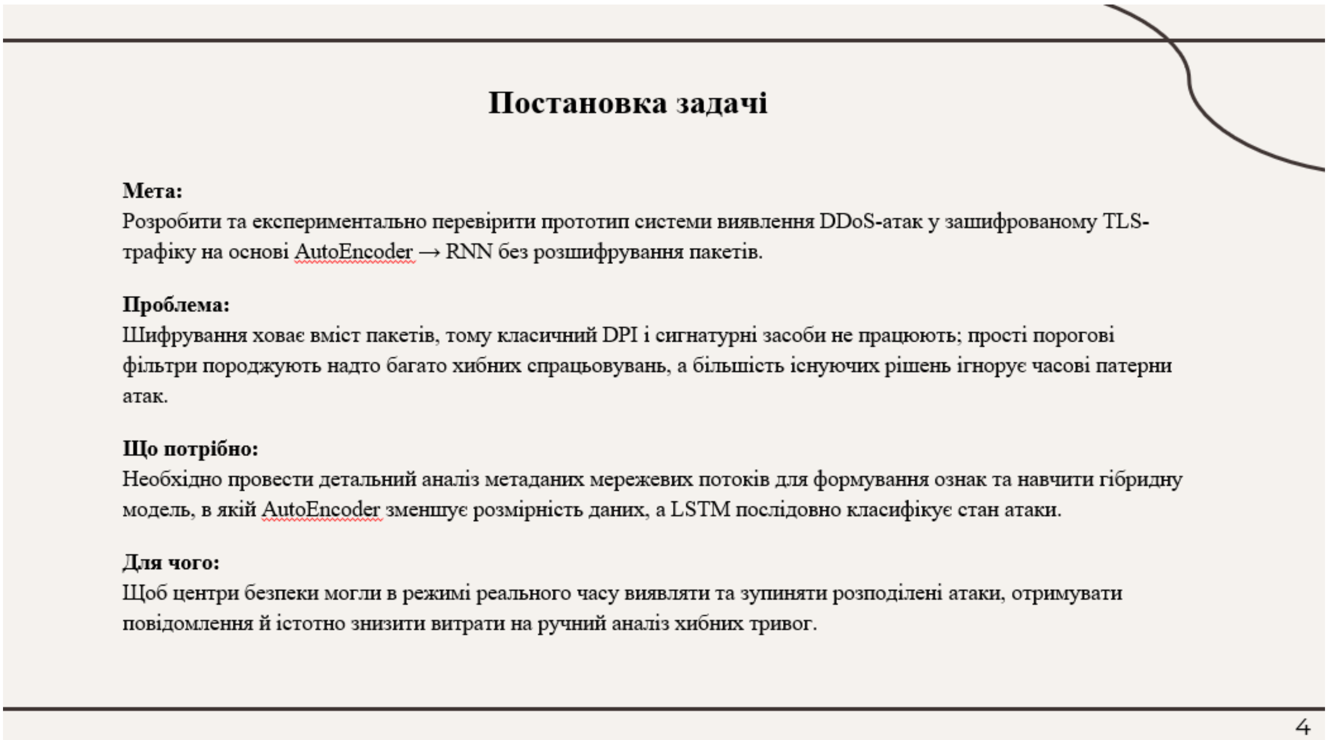


Ключові підходи до побудови системи виявлення DDoS-атак

Підхід до виявлення DDoS-атак	Недоліки	Переваги
Сигнатурне виявлення	• Не підтримує аналіз TLS-зашифрованого трафіку. • Працює через аналіз вмісту пакетів. • Потребує постійного оновлення сигнатур для виявлення нових атак.	• Ефективне для виявлення відомих загроз. • Має низькі обчислювальні витрати. • Легке в налаштуванні та інтерпретації.
Евристичні Методи	• Часті хибні спрацювання при нетипових патернах. • Нові атаки не виявляються без нових правил.	• Ефективне для виявлення відомих загроз. • Має низькі обчислювальні витрати. • Легке в налаштуванні та інтерпретації.
RNN – LSTM	• Високе обчислювальне навантаження. • Повільне навчання через глибоку рекурентну архітектуру. • Схильність до перенавчання на шумових даних. • Обмежена прозорість прийняття рішень (низька інтерпретованість).	• Захоплює складні темпоральні патерни у трафіку. • Ефективний при аналізі потокових даних. • Має потенціал для виявлення нетривіальних атак з довготривалою залежністю.
Гібридний AE → RNN	• Ускладнена реалізація та оптимізація багатоступеневої архітектури. • Ризик втрати критичних ознак під час стиснення. • Ще нижча інтерпретованість через поєднання двох "чорних ящиків".	• Покращена якість вхідних даних завдяки видаленню шуму. • Менша кількість ознак пришвидшує навчання та знижує навантаження. • Краще виявляє комплексні загрози з динамічною поведінкою.

3

Рисунок Б.3 – слайд 3 (рисунок виконано самостійно)



Постановка задачі

Мета:
Розробити та експериментально перевірити прототип системи виявлення DDoS-атак у зашифрованому TLS-трафіку на основі AutoEncoder → RNN без розшифрування пакетів.

Проблема:
Шифрування ховає вміст пакетів, тому класичний DPI і сигнатурні засоби не працюють; прості порогові фільтри породжують надто багато хибних спрацьовувань, а більшість існуючих рішень ігнорує часові патерни атак.

Що потрібно:
Необхідно провести детальний аналіз метаданих мережевих потоків для формування ознак та навчити гібридну модель, в якій AutoEncoder зменшує розмірність даних, а LSTM послідовно класифікує стан атаки.

Для чого:
Щоб центри безпеки могли в режимі реального часу виявляти та зупиняти розподілені атаки, отримувати повідомлення й істотно знизити витрати на ручний аналіз хибних тривог.

4

Рисунок Б.4 – слайд 4 (рисунок виконано самостійно)

Рисунок Б.5 – слайд 5 (рисунок виконано самостійно)

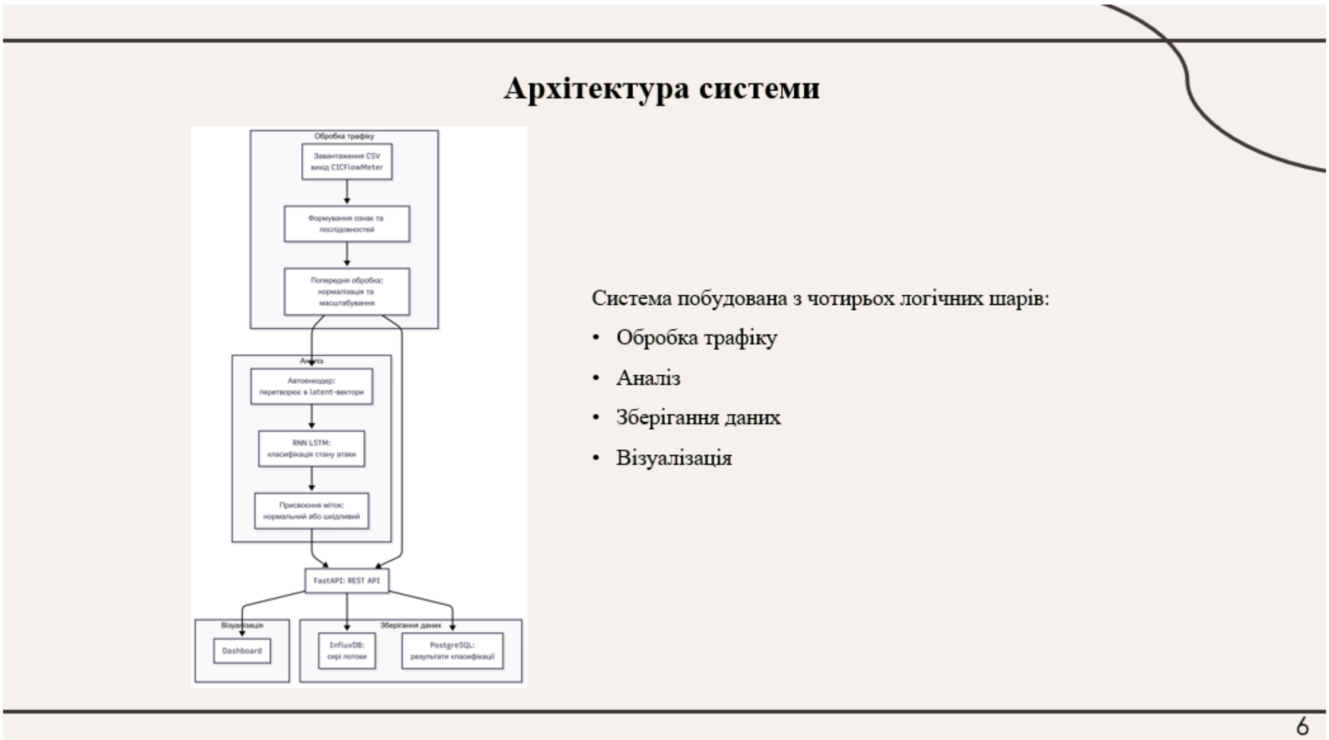


Рисунок Б.6 – слайд 6 (рисунок виконано самостійно)

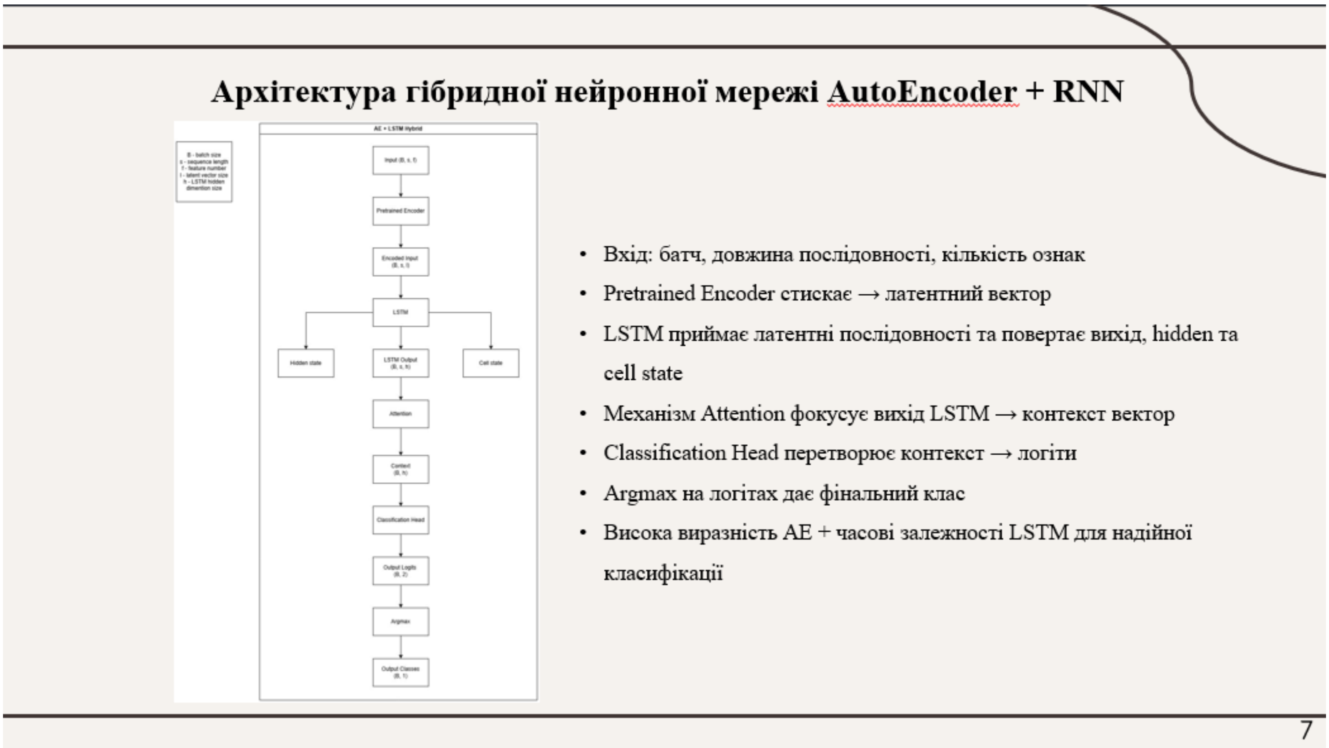


Рисунок Б.7 – слайд 7 (рисунок виконано самостійно)

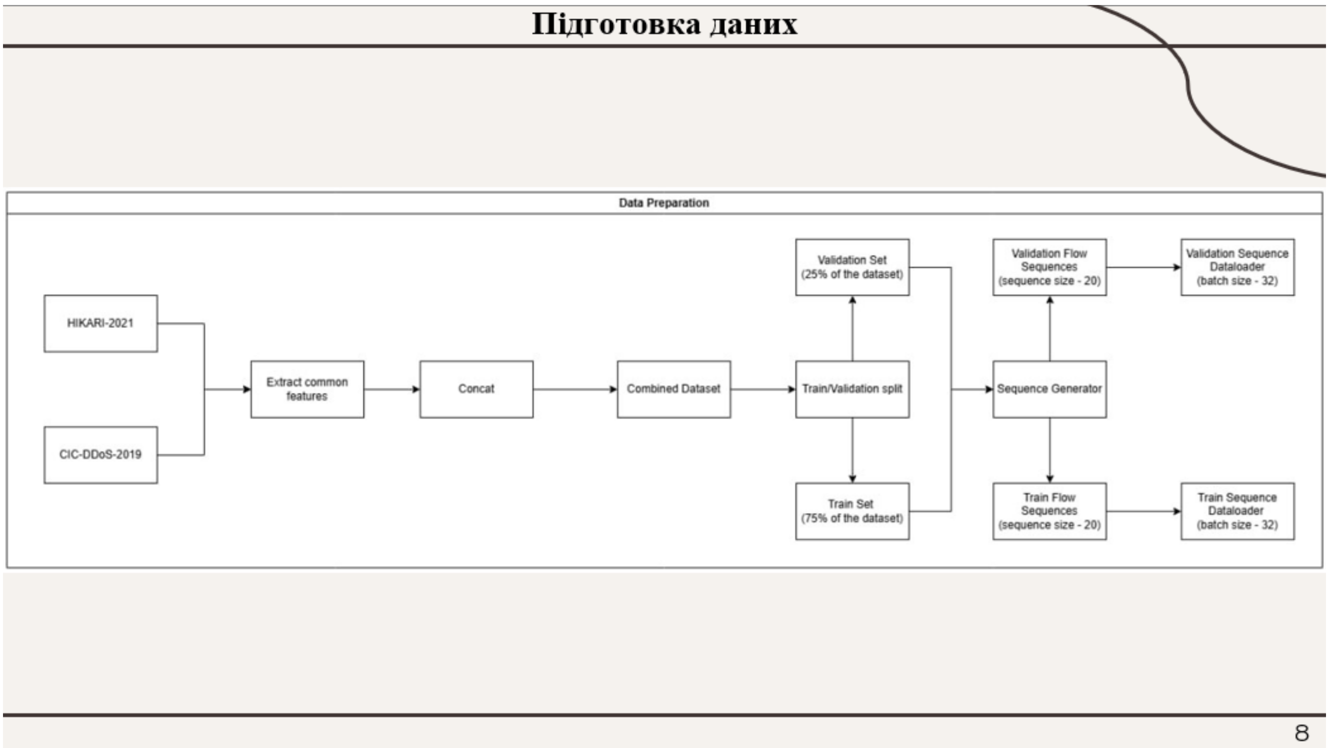


Рисунок Б.8 – слайд 8 (рисунок виконано самостійно)

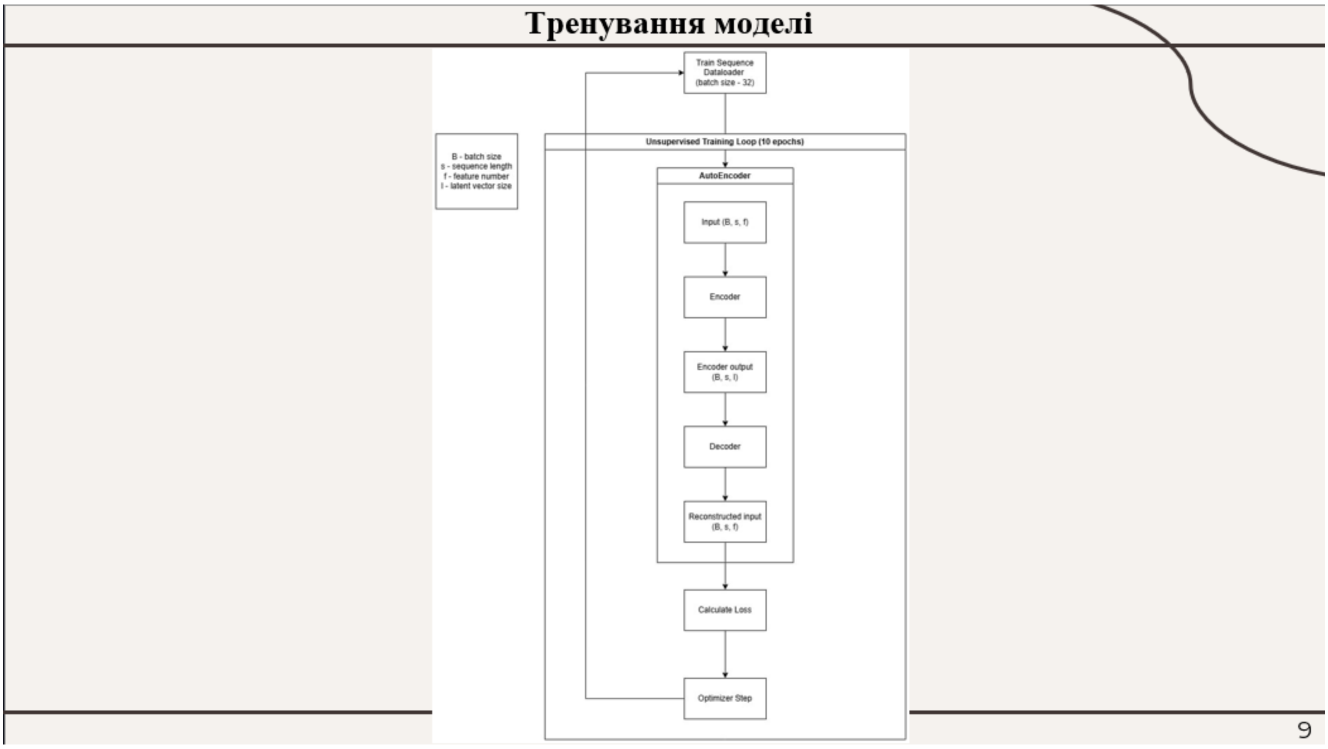


Рисунок Б.9 – слайд 9 (рисунок виконано самостійно)

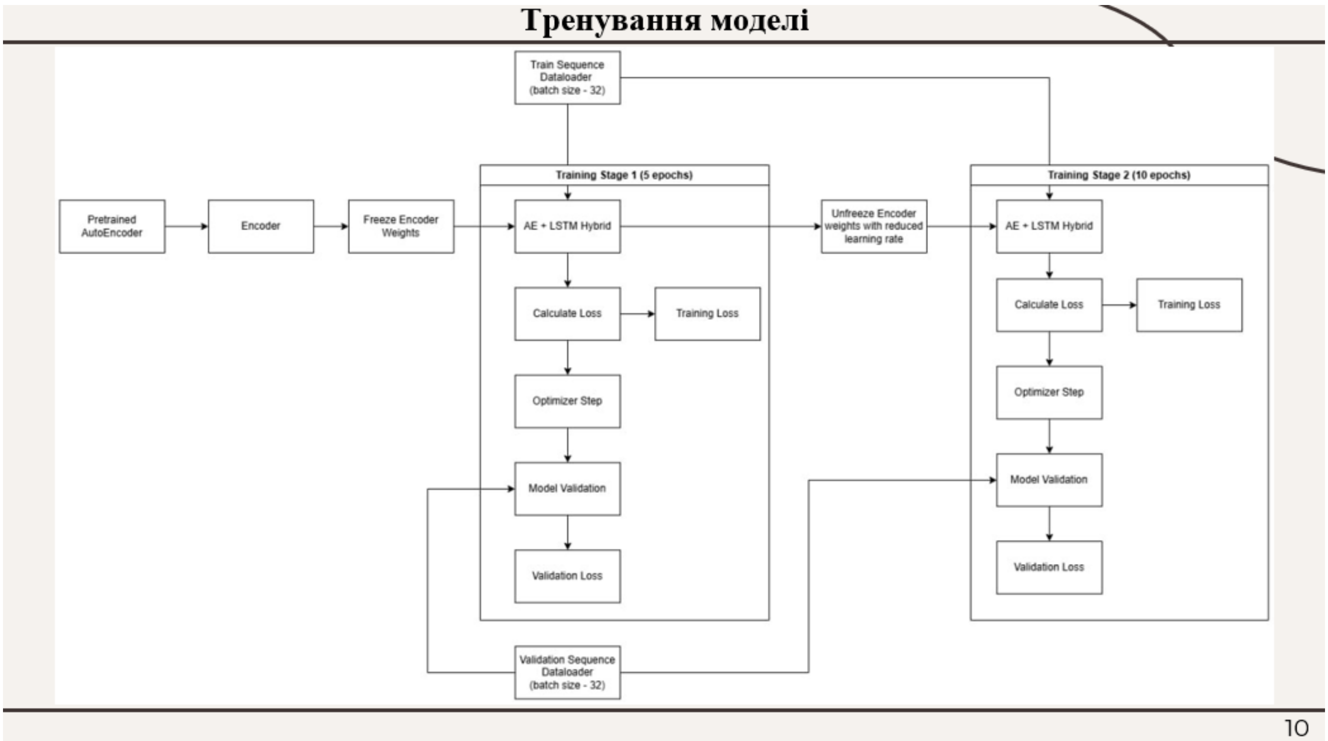


Рисунок Б.10 – слайд 10 (рисунок виконано самостійно)

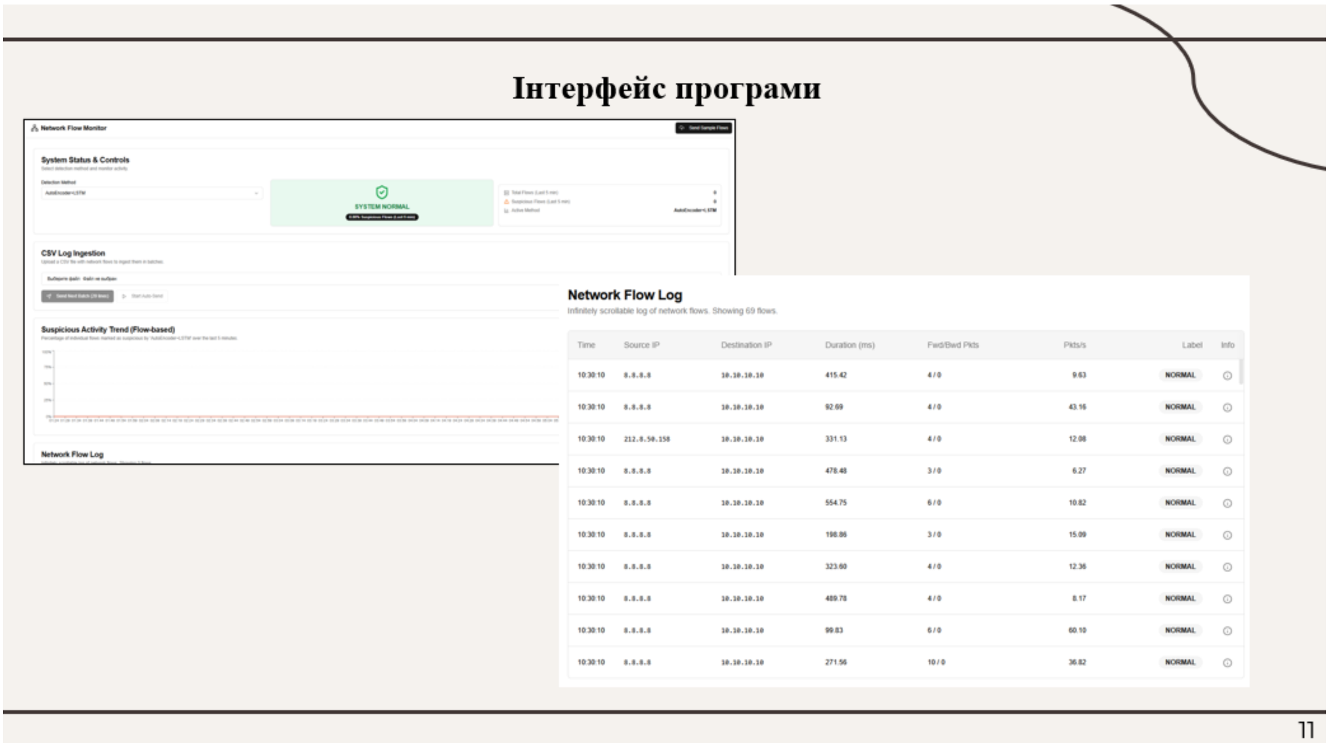


Рисунок Б.11 – слайд 11 (рисунок виконано самостійно)

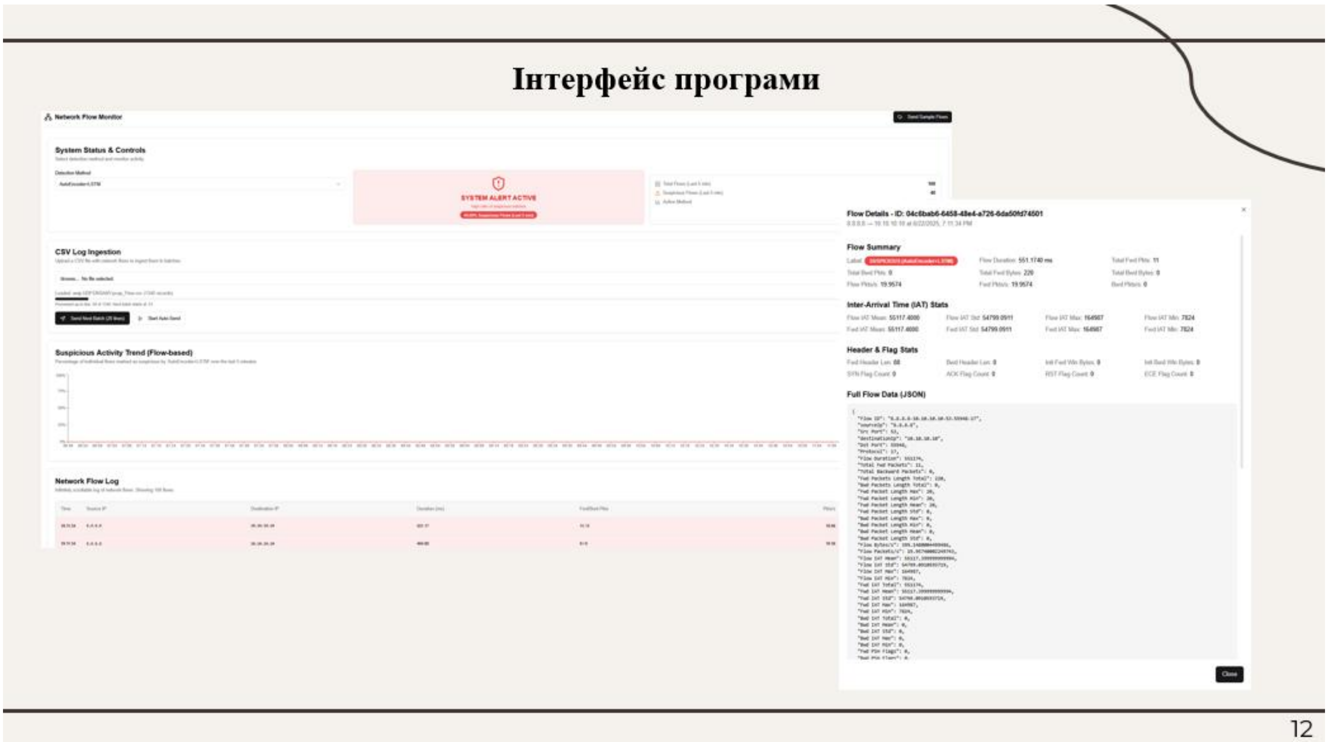


Рисунок Б.12 – слайд 12 (рисунок виконано самостійно)

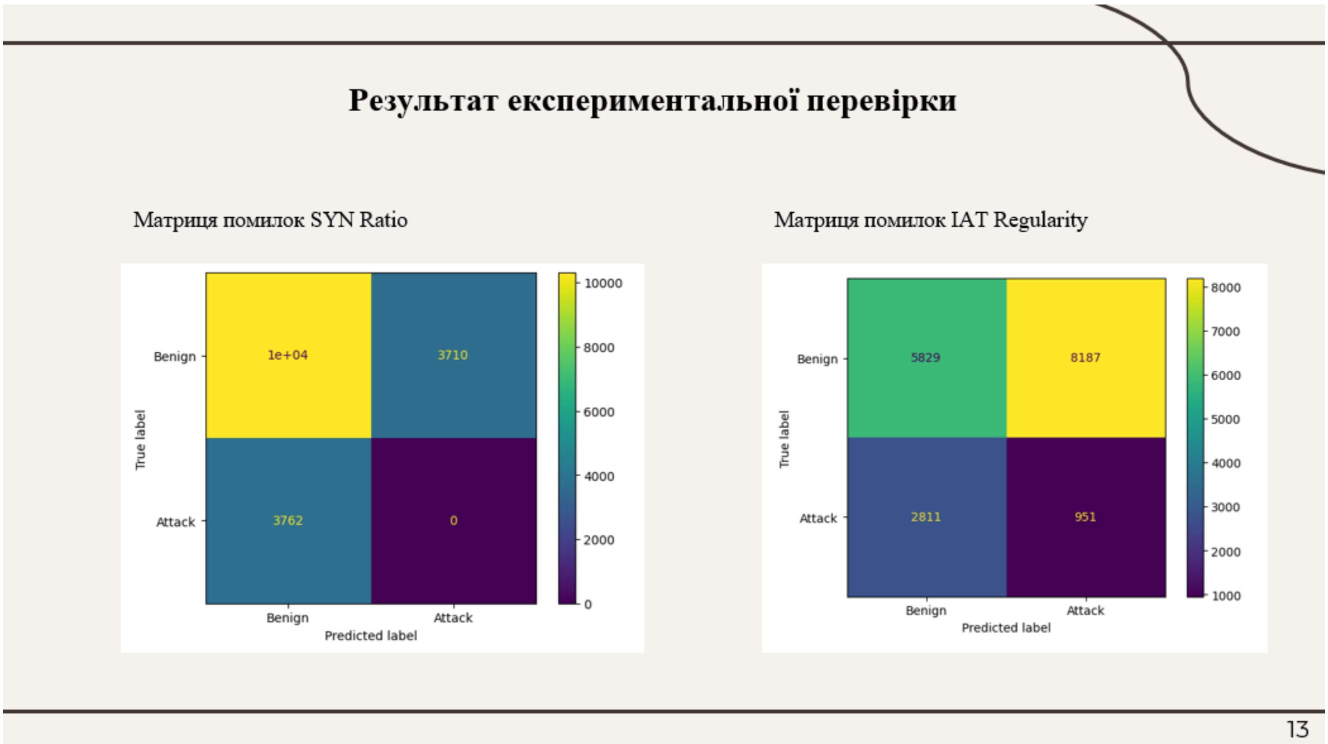


Рисунок Б.13 – слайд 13 (рисунок виконано самостійно)

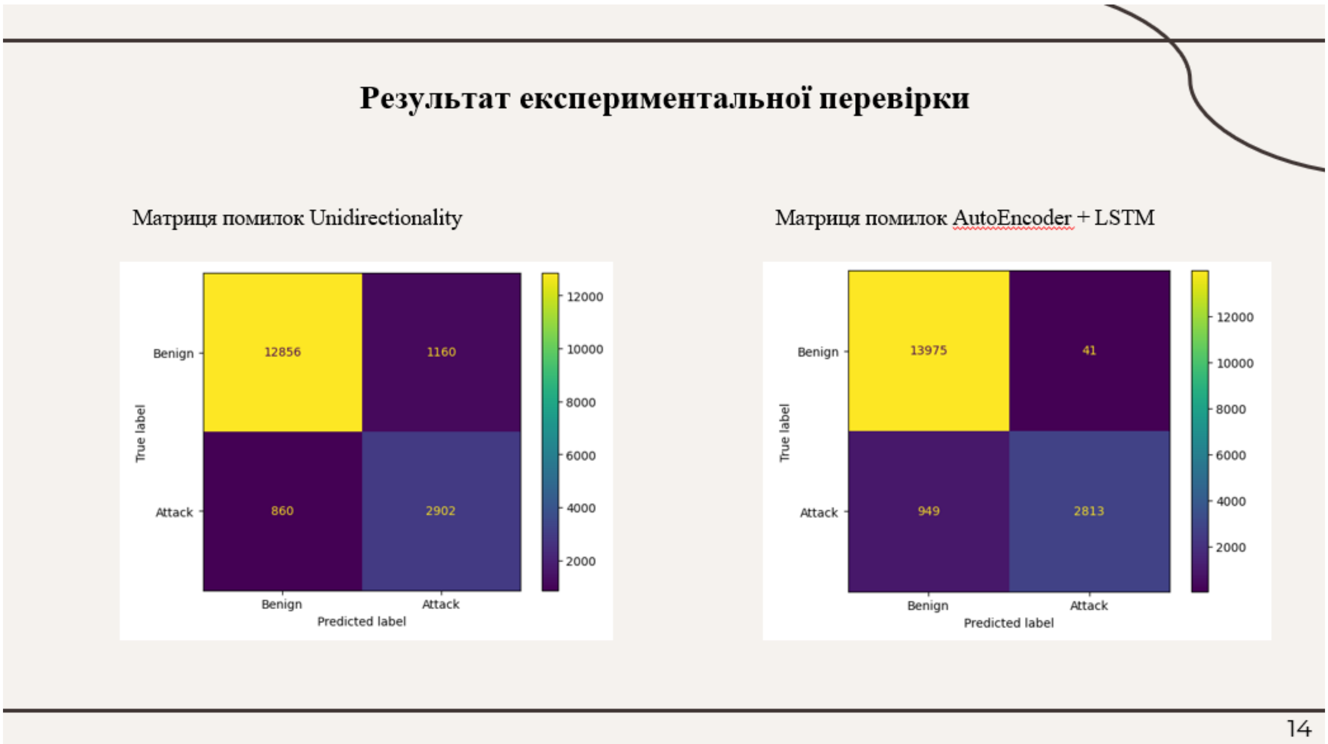
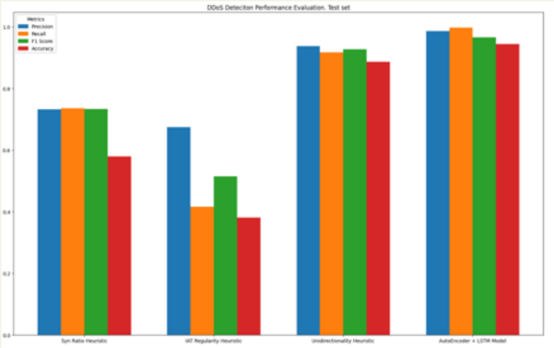


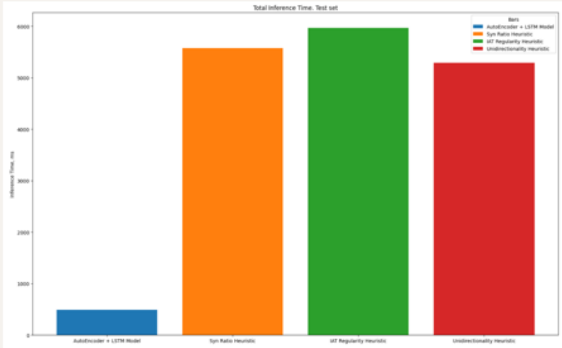
Рисунок Б.14 – слайд 14 (рисунок виконано самостійно)

Результат експериментальної перевірки

Порівняння метрик усіх підходів



Порівняння швидкодії всіх підходів



15

Рисунок Б.15 – слайд 15 (рисунок виконано самостійно)

Підсумки

Запропоновано гібридну багаторівневу модель AutoEncoder + RNN, яка працює виключно з потоковими ознаками та враховує часові шаблони в поведінці трафіку. У тестах досягнуто точності виявлення понад 94 % при затримці обробки < 0.03 мс на послідовність.

Реалізовано прототип системи зі збором, агрегацією та аналізом потоків: інструмент обробляє до 700 000 потоків/с, зберігає сирі дані в InfluxDB та результати класифікації в PostgreSQL. Усі сервіси розгортаються в хмарі й взаємодіють через єдиний REST API.

Отримані показники підтверджують готовність рішення до впровадження в SOC-середовищах для реального часу детекції DDoS-атак у зашифрованому TLS-трафіку без розшифрування пакетів.

16

Рисунок Б.16 – слайд 16 (рисунок виконано самостійно)

Рисунок Б.17 – слайд 17 (рисунок виконано самостійно)

Рисунок Б.18 – слайд 18 (рисунок виконано самостійно)

ДОДАТОК В

Апробація результатів роботи


isu-conference.com

ISU
INTERNATIONAL SCIENTIFIC UNITY

CERTIFICATE
of conference participant

it is hereby certified, that
ANDRIY TRYPILKA
took part in the 2nd International Scientific and Practical Conference
«THE FUTURE OF SCIENCE, TECHNOLOGY AND ECONOMY»

June 11-13, 2025, Sofia, Bulgaria
24 Hours of Participation
(0,8 ECTS credits)

Head of the
organizing committee

Viktoriia Tsiundyk

ISU-25/0611-143

7. Allamanis M. Learning to Represent Programs with Graphs [Електронний ресурс] / M. Allamanis, M. Brockschmidt, M. Khademi // arXiv. – Режим доступу: https://arxiv.org/abs/1711.00740 (дата звернення: 10.06.2025).

USING DEEP LEARNING FOR DETECTION OF ENCRYPTED DDOS ATTACKS IN CLOUD ENVIRONMENTS

Kravets Natalia
Candidate of Technical Sciences, Associate Professor
Trypilka Andriy
Second-year graduate student (Master's degree)
Department of Software Engineering
Kharkiv National University of Radio Electronics, Ukraine

The rapid growth of cloud computing and increased reliance on encrypted traffic presents significant challenges for network security, particularly regarding the detection of Distributed Denial-of-Service (DDoS) attacks. Traditional methods such as signature-based and deep packet inspection (DPI) have become largely ineffective due to encryption standards like TLS/SSL, which prevent access to payload data. Consequently, cybersecurity researchers are turning to alternative detection techniques that focus primarily on metadata analysis, including packet size distributions, timing intervals, connection rates, and session durations [1].

Encrypted DDoS attacks are especially problematic because they effectively mimic legitimate user behavior and complicate anomaly detection. Attackers increasingly leverage encryption protocols to mask their activities, thus bypassing traditional network monitoring and intrusion detection systems. This approach makes distinguishing malicious traffic from legitimate traffic particularly challenging, as standard detection systems rely on recognizing known attack signatures or inspecting packet contents, both of which become ineffective under encryption [2].

Recent advances in machine learning, particularly deep learning techniques, offer promising solutions to this challenge. Autoencoders, a specific type of unsupervised neural network, have shown significant potential in detecting anomalous patterns within encrypted traffic. Autoencoders operate by learning to accurately reconstruct benign traffic patterns during training. When confronted with previously unseen malicious traffic, such as DDoS attack patterns, these networks exhibit high reconstruction errors due to deviations from learned benign patterns. This property allows autoencoders to detect anomalies effectively even in highly dynamic cloud environments, where comprehensive labeling of malicious traffic is difficult [3].

However, using autoencoders alone might not adequately capture temporal aspects inherent in network traffic data, which is crucial for accurately identifying attacks like DDoS, characterized by distinctive temporal patterns such as repetitive packet bursts or synchronized traffic spikes. To address this limitation, recurrent neural networks (RNNs), including Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU), have been introduced into anomaly detection frameworks. These networks are specifically designed to process sequential data and capture temporal dependencies, making them highly suitable for analyzing time-series traffic data. Studies demonstrate that RNN architectures significantly improve the detection accuracy of temporally patterned attacks when integrated into anomaly detection systems [4].

Hybridizing autoencoders with RNN models has emerged as a robust approach, combining the unsupervised detection capabilities of autoencoders with the sequence modeling strengths of RNNs. Such hybrid models first identify suspicious traffic flows using autoencoders and subsequently apply RNNs to analyze these flows in more detail, effectively classifying the nature and type of detected anomalies. This combination results in higher accuracy, lower false-positive rates, and improved adaptability to previously unknown attack patterns compared to traditional single-model systems [5].

The effectiveness of this combined methodology is supported by recent studies. Experiments utilizing hybrid deep learning architectures, particularly combinations of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM), conducted on widely recognized datasets such as CIC-DDoS2019 and CSE-CIC-IDS2018, report accuracy levels exceeding 99% in detecting encrypted DDoS attacks, accompanied by notably low false-positive rates [6]. These results highlight the substantial potential of deep learning approaches, particularly because these models operate solely on traffic metadata without needing access to packet payloads, thus maintaining user privacy and ensuring compliance with data protection regulations.

However, several challenges remain to be addressed before widespread deployment of these methods can be achieved in real-world cloud infrastructures. Deep learning models, particularly hybrid models involving RNNs, typically demand substantial computational resources and require careful tuning to balance precision, recall, and operational efficiency. Furthermore, maintaining model accuracy over time requires continuous retraining on fresh datasets reflecting evolving traffic patterns and attack techniques, raising questions of scalability and resource allocation within enterprise environments.

Future research should thus focus on enhancing computational efficiency, facilitating real-time processing capabilities, and optimizing these models for deployment in practical cloud environments. Advances in distributed deep learning architectures and cloud-native implementations present valuable directions for making these sophisticated methods practically viable. Additionally, research into explainability and transparency in deep learning systems is essential, as the opaque nature of neural network-based methods often complicates trust and acceptance by security analysts.

In conclusion, despite existing technical and operational challenges, deep learning techniques, particularly hybrid architectures employing autoencoders and recurrent neural networks, represent a significant advancement for the detection of encrypted

DDoS attacks within cloud environments. Continued research and development in this area promise substantial improvements in cybersecurity practices, offering viable alternatives to traditional detection mechanisms and significantly enhancing the resilience of cloud-based infrastructure against modern cyber threats.

References

1. Callado, A., Scheirer, W. J., Rozanski, E. W., Shaikh, A., Molling, J., & Molling, C. (2009). A survey on internet traffic identification. IEEE Communications Surveys & Tutorials, 11(3), 37–52. https://doi.org/10.1109/SURV.2009.090304
2. Bhatia, S., Behal, S., & Ahmed, I. (2021). Distributed denial of service attacks and defense mechanisms: Current landscape and future directions. In T. D. Malik & V. K. Agrawal (Eds.), Proceedings of the 7th International Conference on Cyber Security and Cloud Computing (pp. 45–62). Springer. https://link.springer.com/chapter/10.1007/978-3-319-97643-3_3
3. Makhzani, A., Shlens, J., Jaitly, N., & Goodfellow, I. (2015). Adversarial autoencoders. arXiv. https://arxiv.org/abs/1511.05644
4. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418
5. Lotfollahi, M., Jafari Siavoshani, M., Shirali Hossein Zade, R., & Saberian, A. (2019). Deep packet: A novel approach for encrypted traffic classification using deep learning. Soft Computing, 24(3), 1999–2012. https://doi.org/10.1007/s00500-019-04030-2
6. Ain, N. U., Sardaraz, M., Tahir, M., Abo Elsoud, M. W., & Alourani, A. (2025). Securing IoT networks against DDoS attacks: A hybrid deep learning approach. Sensors, 25(5), 1346. https://doi.org/10.3390/s25051346

ДОДАТОК Г

Експертний висновок результатів перевірки кваліфікаційної роботи на відповідність оформлення вимогам ДСТУ 3008: 2015

Експертний висновок результатів перевірки кваліфікаційної роботи

студент	програмної інженерії	ІПЗм-23-4
(посада)	(кафедра)	(група)

Андрій ТРИПІЛКА

(прізвище, ім'я, по батькові)

Зауваження

Пункт ДСТУ 3008-2015	Зміст пункту	Сторінка кваліфікаційної роботи
1	2	3
	7.1 Загальні положення	
7.1.11	Рекомендовано на сторінках звіту використовувати береги такої ширини: верхній і нижній — не менше ніж 20 мм, лівий — не менше ніж 25 мм, правий — не менше ніж 10 мм.	По тексту
	7.3 Нумерація сторінок звіту	
	7.5 Рисунки	
	7.6 Таблиці	
7.6.9	Якщо рядки або колонки таблиці виходять за межі формату сторінки, таблицю поділяють на частини, розміщуючи одну частину під іншою або поруч, чи переносять частину таблиці на наступну сторінку. У кожній частині таблиці повторюють її головку та боковик. У разі поділу таблиці на частини дозволено її головку чи боковик заміняти відповідно номерами колонок або рядків, нумеруючи їх арабськими цифрами в першій частині таблиці. Слово «Таблиця » подають лише один раз над першою частиною таблиці. Над іншими частинами таблиці з абзацного відступу друкують «Продовження таблиці » або «Кінець таблиці ____ » без повторення її назви.	38
	7.7 Переліки	
	7.8 Примітки	
	7.9 Виноски	
	7.10 Формули та рівняння	
7.10.6	Пояснення познак, які входять до формули чи рівняння, треба подавати безпосередньо під формулою або рівнянням у тій послідовності, у якій їх наведено у формулі або рівнянні. Пояснення познак треба подавати без абзацного відступу з нового рядка, починаючи зі слова «де» без двокрапки. Познаки, яким встановлюють визначення чи пояснення, рекомендовано ви-рівнювати у вертикальному напрямку.	35
	7.11 Посилання	
	7.13 Список авторів	
	7.14 Скорочення та умовні познаки	
	7.15 Додатки	

Методичні вказівки до виконання кваліфікаційної роботи магістра… ЗАТВЕРДЖЕНО кафедрою ПІ протокол № 12 від 03.02.2025 р 3.2 Оформлення пояснювальної записки згідно з ДСТУ 3008:2015 Звіти у сфері науки і техніки. Структура та правила оформлювання. **Шаблон**:ЗАТВЕРДЖЕНО кафедрою ПІ протокол № 12 від 03.02.2025 р.	Увага! встановлені фіксовані береги: лівий – 25 мм., правий – 10 мм, верхній і нижній – 20 мм.	По тексту

Експерт ______ (підпис) Вадим НЕЧВОЛОД (прізвище, ініціали)

Робота з перевірки оформлення пояснювальної записки кваліфікаційної роботи на нормоконтроль виконана у програмі Word Microsoft 365. Версія 2504 (збірка 18730.20220)

19.06.2025