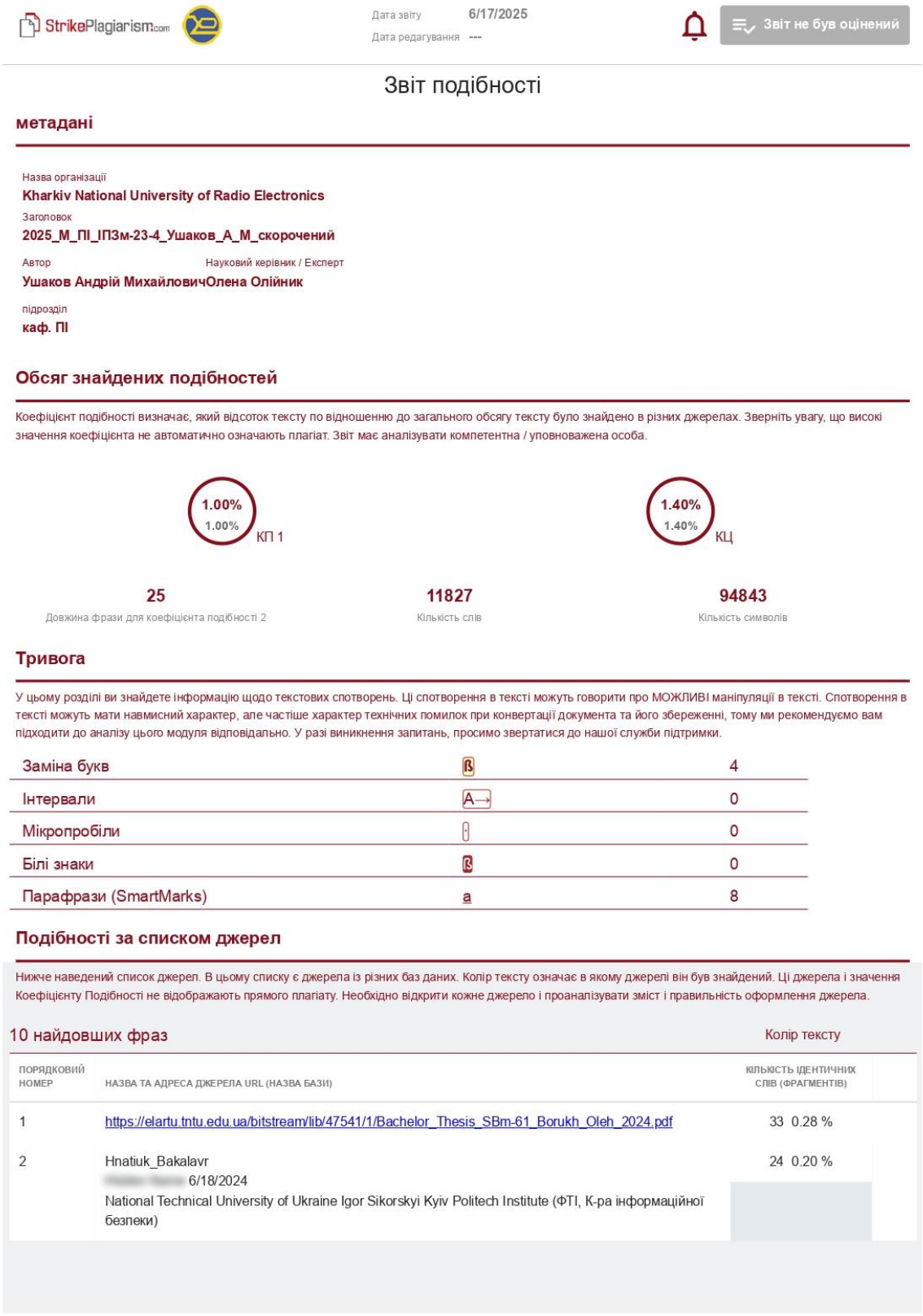
ДОДАТОК А

Звіт результатів перевірки на унікальність тексту в базі ХНУРЕ



StrikePlagiarism.com

Дата звіту 6/17/2025
Дата редагування ---

Звіт не був оцінений

Звіт подібності

метадані

Назва організації
Kharkiv National University of Radio Electronics
Заголовок
2025_М_ПІ_ІПЗм-23-4_Ушаков_А_М_скорочений
Автор Науковий керівник / Експерт
Ушаков Андрій МихайловичОлена Олійник
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.

1.00% 1.00% КП 1

1.40% 1.40% КЦ

25 Довжина фрази для коефіцієнта подібності 2

11827 Кількість слів

94843 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	4
Інтервали	A→	0
Мікропробіли	¶	0
Білі знаки	ß	0
Парафрази (SmartMarks)	a	8

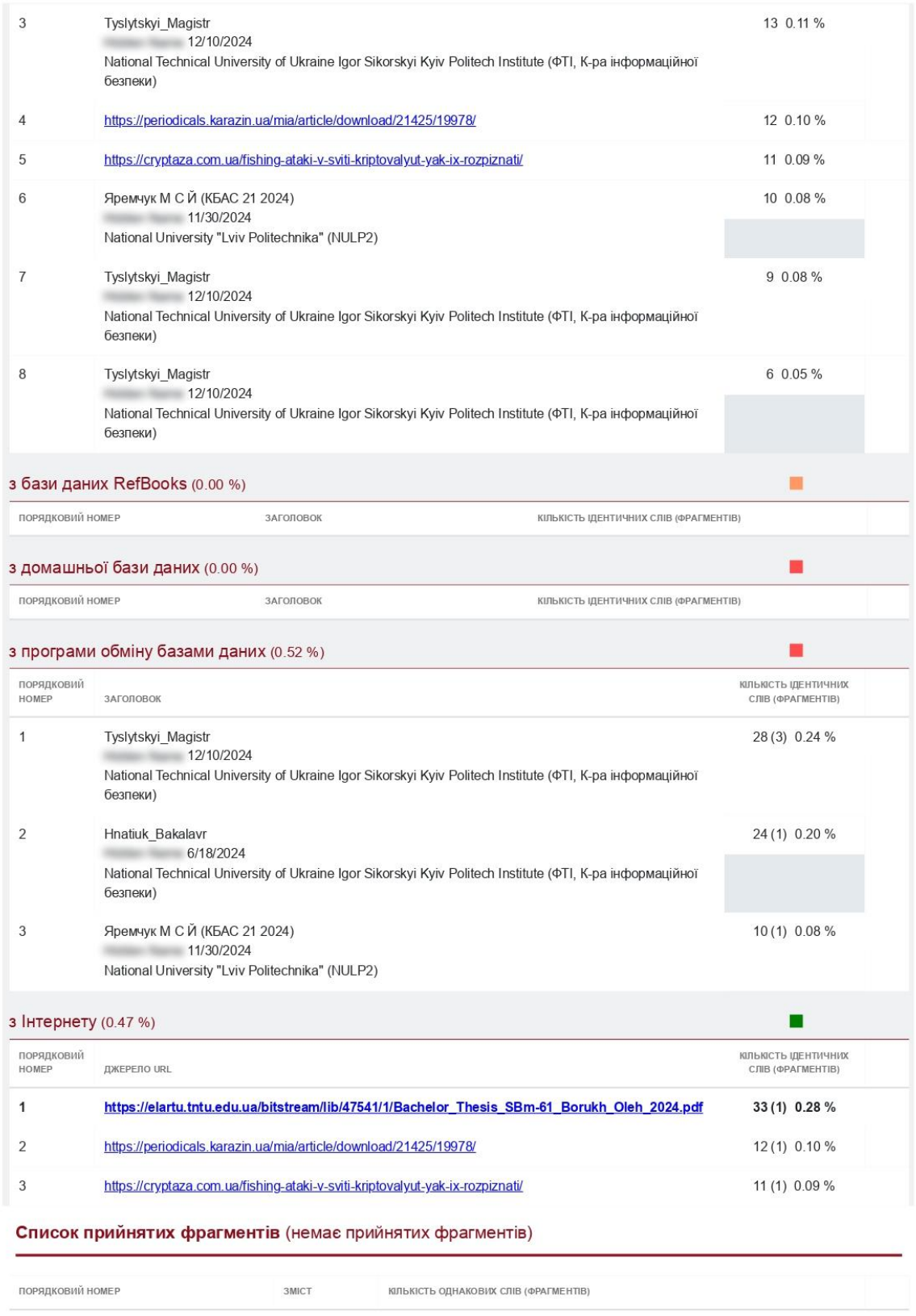
Подібності за списком джерел

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://elartu.tntu.edu.ua/bitstream/lib/47541/1/Bachelor_Thesis_SBm-61_Borukh_Oleh_2024.pdf	33 0.28 %
2	Hnatiuk_Bakalavr [redacted] 6/18/2024 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ФТІ, К-ра інформаційної безпеки)	24 0.20 %

Рисунок А.1 – Звіт результатів перевірки на унікальність тексту. Сторінка 1



3	Tyslytskyi_Magistr [redacted] 12/10/2024 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ФТІ, К-ра інформаційної безпеки)	13 0.11 %
4	https://periodicals.karazin.ua/mia/article/download/21425/19978/	12 0.10 %
5	https://cryptaza.com.ua/fishing-ataki-v-sviti-kriptovalyut-yak-ix-rozpiznati/	11 0.09 %
6	Яремчук М С Й (КБАС 21 2024) [redacted] 11/30/2024 National University "Lviv Politechnika" (NULP2)	10 0.08 %
7	Tyslytskyi_Magistr [redacted] 12/10/2024 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ФТІ, К-ра інформаційної безпеки)	9 0.08 %
8	Tyslytskyi_Magistr [redacted] 12/10/2024 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ФТІ, К-ра інформаційної безпеки)	6 0.05 %

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 (0.52 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Tyslytskyi_Magistr [redacted] 12/10/2024 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ФТІ, К-ра інформаційної безпеки)	28 (3) 0.24 %
2	Hnatiuk_Bakalavr [redacted] 6/18/2024 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ФТІ, К-ра інформаційної безпеки)	24 (1) 0.20 %
3	Яремчук М С Й (КБАС 21 2024) [redacted] 11/30/2024 National University "Lviv Politechnika" (NULP2)	10 (1) 0.08 %

з Інтернету (0.47 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	**https://elartu.tntu.edu.ua/bitstream/lib/47541/1/Bachelor_Thesis_SBm-61_Borukh_Oleh_2024.pdf**	**33 (1) 0.28 %**
2	https://periodicals.karazin.ua/mia/article/download/21425/19978/	12 (1) 0.10 %
3	https://cryptaza.com.ua/fishing-ataki-v-sviti-kriptovalyut-yak-ix-rozpiznati/	11 (1) 0.09 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

Рисунок А.2 – Звіт результатів перевірки на унікальність тексту. Сторінка 2

ДОДАТОК Б

Слайди презентації

Рисунок Б.1 – Слайд презентації 1

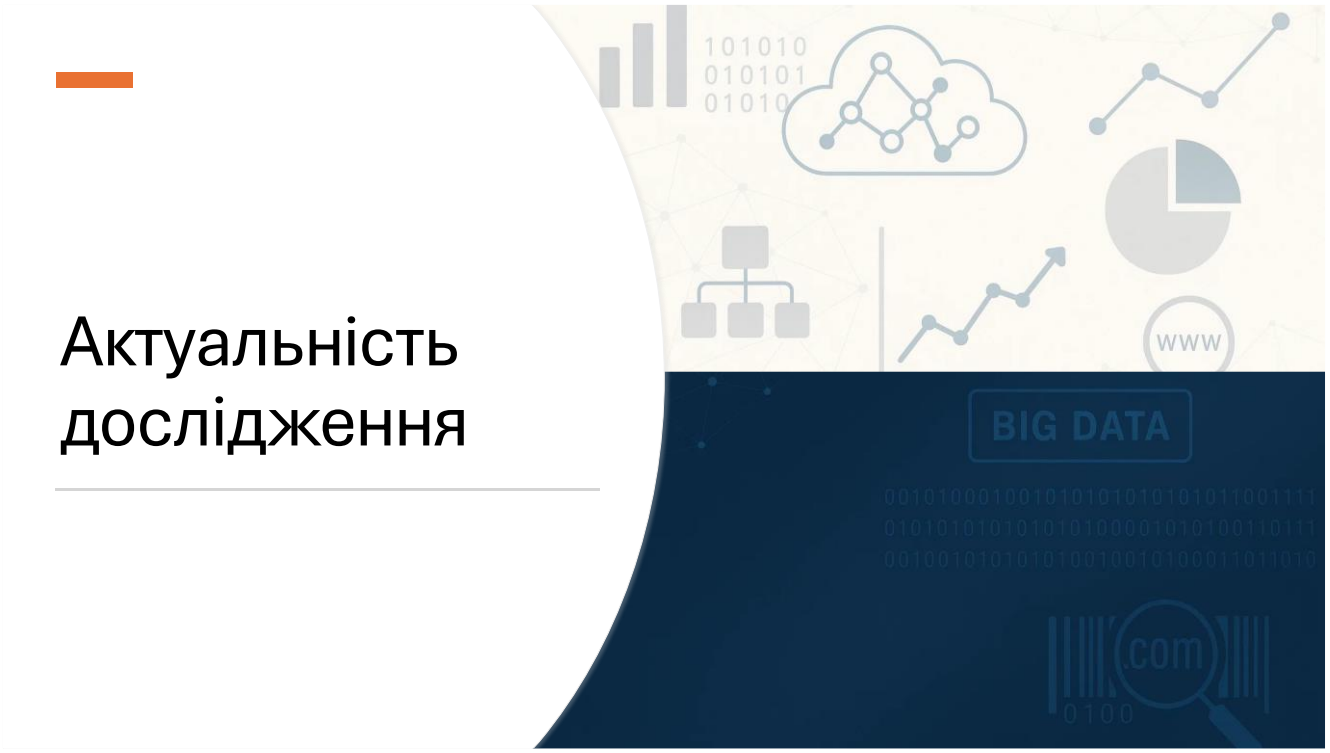


Рисунок Б.2 – Слайд презентації 2

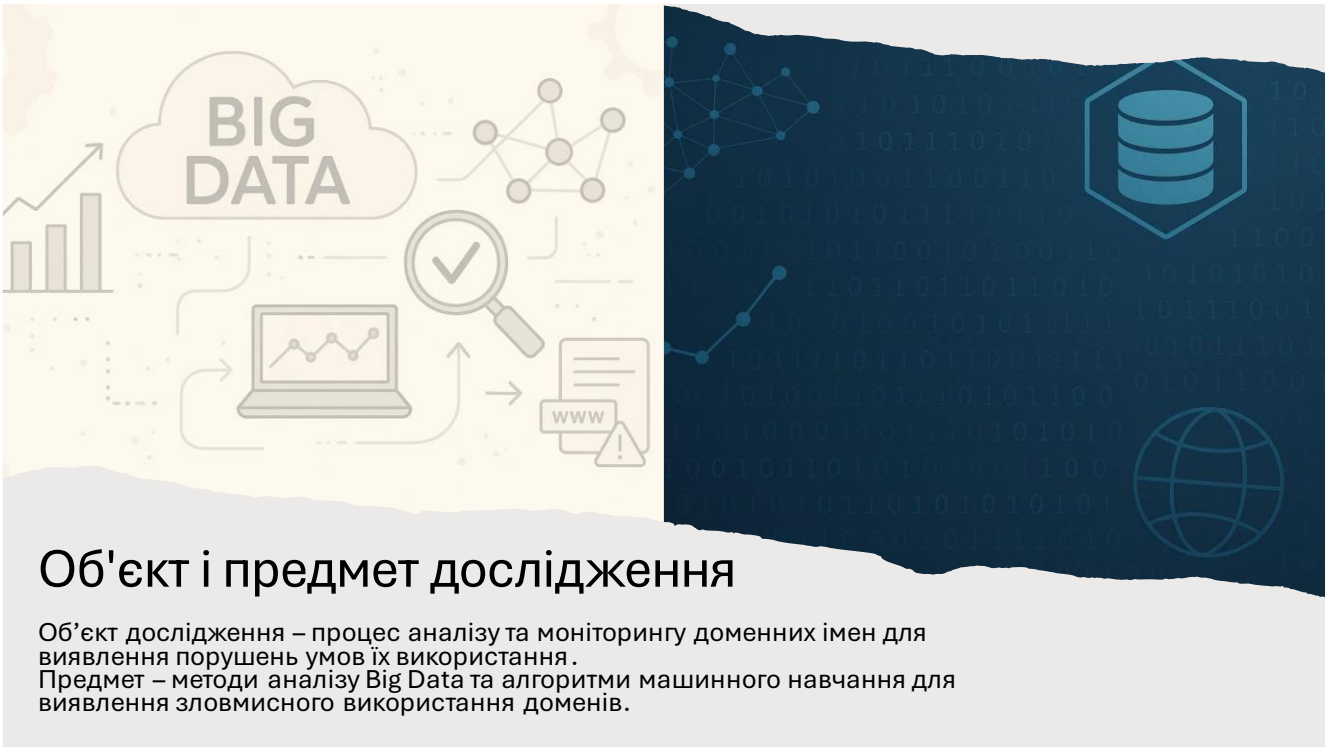
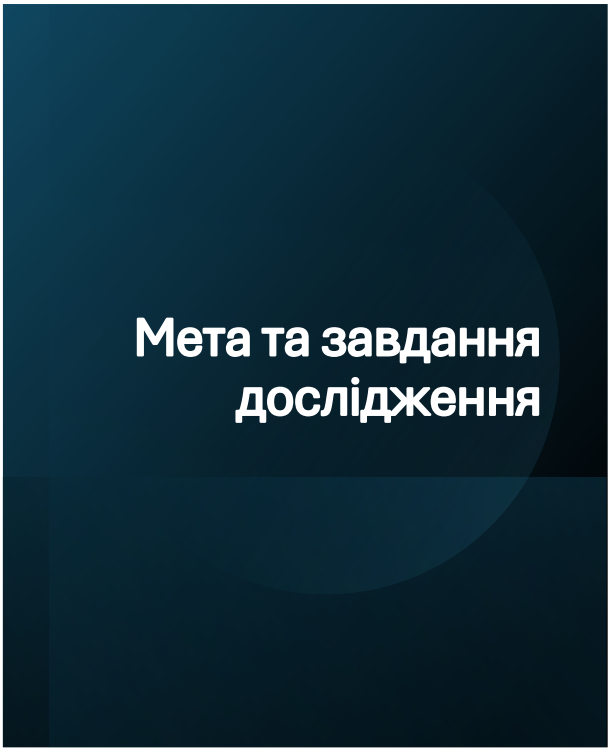


Рисунок Б.3 – Слайд презентації 3



Мета роботи — розробити прототип системи, що дозволяє проводити автоматизований аналіз доменних імен і прогнозувати їхню потенційну загрозу.

Для досягнення мети поставлено такі завдання:

- провести огляд сучасних методів аналізу доменів;
- дослідити можливості застосування технологій Big Data та машинного навчання;
- зібрати та підготувати навчальні дані;
- навчити модель класифікації;
- реалізувати веб-застосунок для інтерактивного аналізу.

Рисунок Б.4 – Слайд презентації 4

Аналіз предметної галузі

- Існуючі підходи до виявлення:
  - Чорні списки - статичні бази даних шкідливих доменів
  - Фільтрація за ключовими словами та шаблонами
  - Сигнатурний аналіз - пошук відомих характеристик загроз
- Недоліки класичних методів:
  - Затримки в оновленні баз даних
  - Низька адаптивність до нових типів загроз
  - Обмежена масштабованість при зростанні обсягів даних

Рисунок Б.5 – Слайд презентації 5

Роль Big Data і ML у сфері кібербезпеки

- Можливості аналізу великих обсягів даних для пошуку аномалій і прогнозування ризиків:
  - Аналіз DNS-запитів, WHOIS-даних та поведінкових патернів у режимі реального часу
- Автоматизація процесу моніторингу та ідентифікації шкідливих доменів:
  - Зменшення необхідності ручного втручання та прискорення реакції на загрози
- Підвищення точності й швидкості виявлення загроз порівняно з традиційними методами:
  - Сучасні алгоритми ML досягають точності понад 90% у класифікації доменних імен

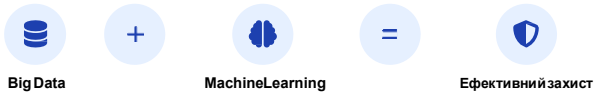


Рисунок Б.6 – Слайд презентації 6

Огляд та аналіз літературних, наукових джерел

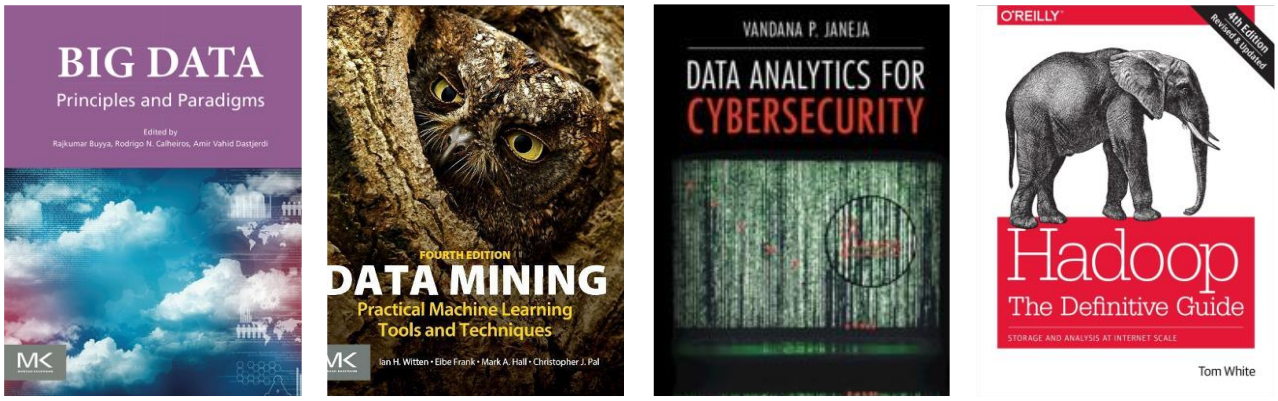


Рисунок Б.7 – Слайд презентації 7

Постановка задачі

- Здатність у реальному часі прогнозувати порушення у використанні доменів
- Забезпечення обробки великих обсягів даних (DNS, WHOIS)
- Висока точність прогнозування (не менше 90%)
- Інтерактивний користувацький інтерфейс
- Масштабованість та можливість інтеграції з іншими системами

Рисунок Б.8 – Слайд презентації 8

Архітектура системи

Frontend: React+Tailwind

Backend: FastAPI

ML-модель: Random Forest

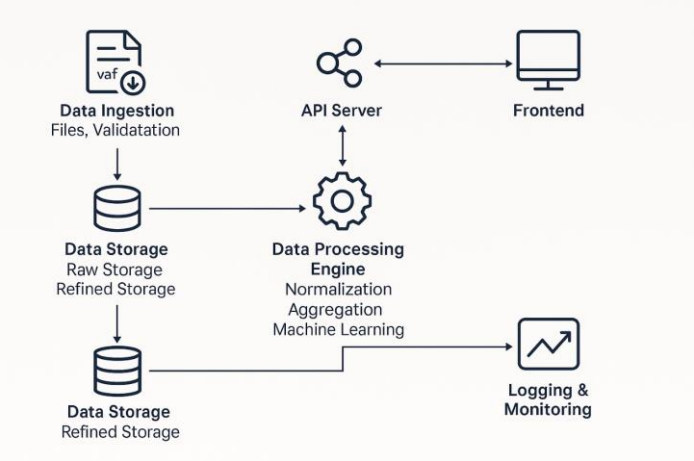


Рисунок Б.9 – Слайд презентації 9

Алгоритм роботи

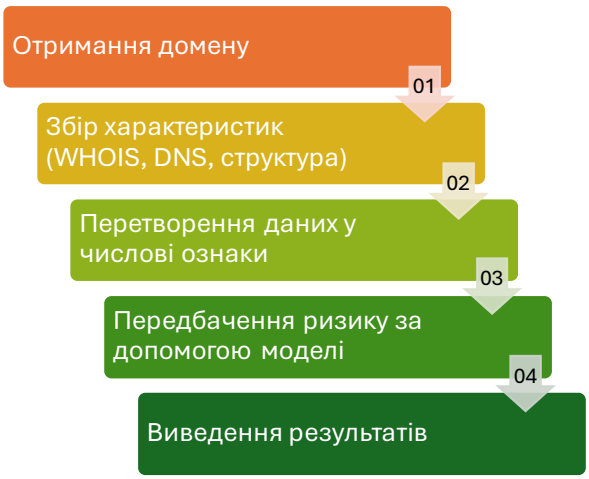


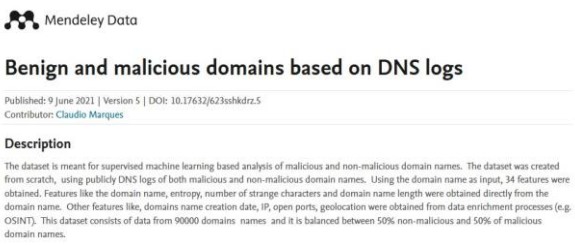
Рисунок Б.10 – Слайд презентації 10

Модель машинного навчання

Формування навчального датасету

Навчання моделі класифікації

Збереження моделі



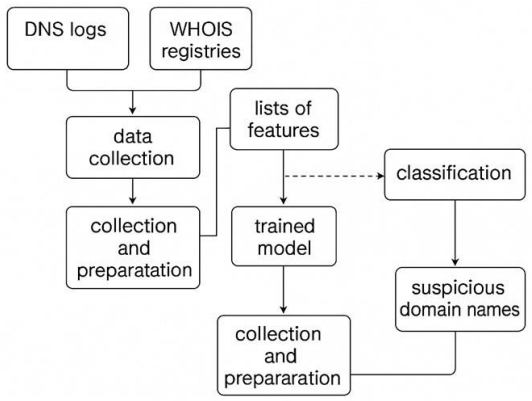
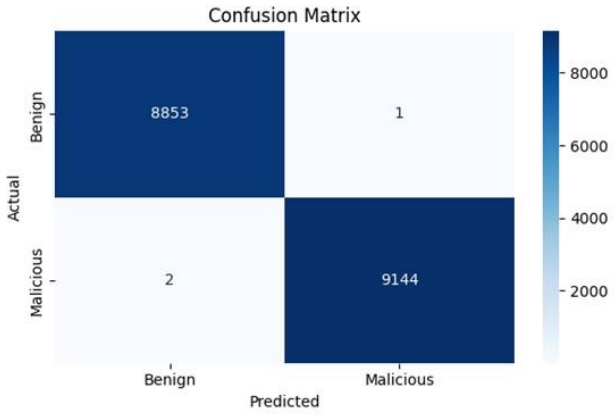


Рисунок Б.11 – Слайд презентації 11

Результати навчання моделі



	precision	recall	f1-score	support
0	0.999774	0.999887	0.999831	8854.000000
1	0.999891	0.999781	0.999836	9146.000000
accuracy	0.999833	0.999833	0.999833	0.999833
macro avg	0.999832	0.999834	0.999833	18000.000000
weighted avg	0.999833	0.999833	0.999833	18000.000000

Рисунок Б.12 – Слайд презентації 12

Рисунок Б.13 – Слайд презентації 13

Рисунок Б.14 – Слайд презентації 14

Головний дашборд

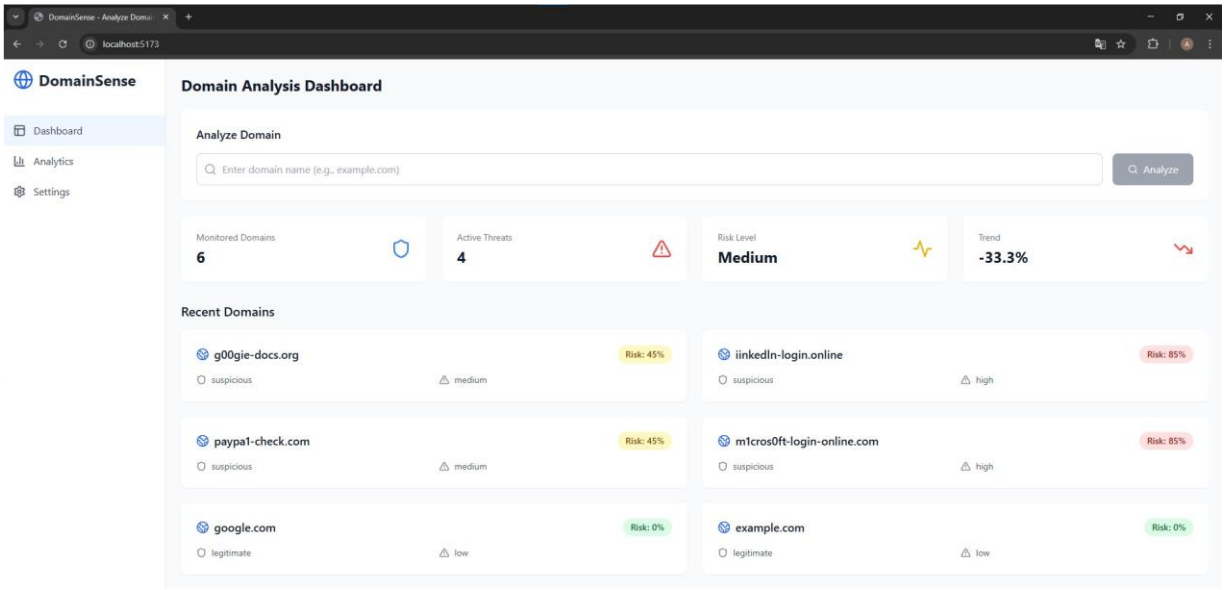


Рисунок Б.15 – Слайд презентації 15

Екран деталізації

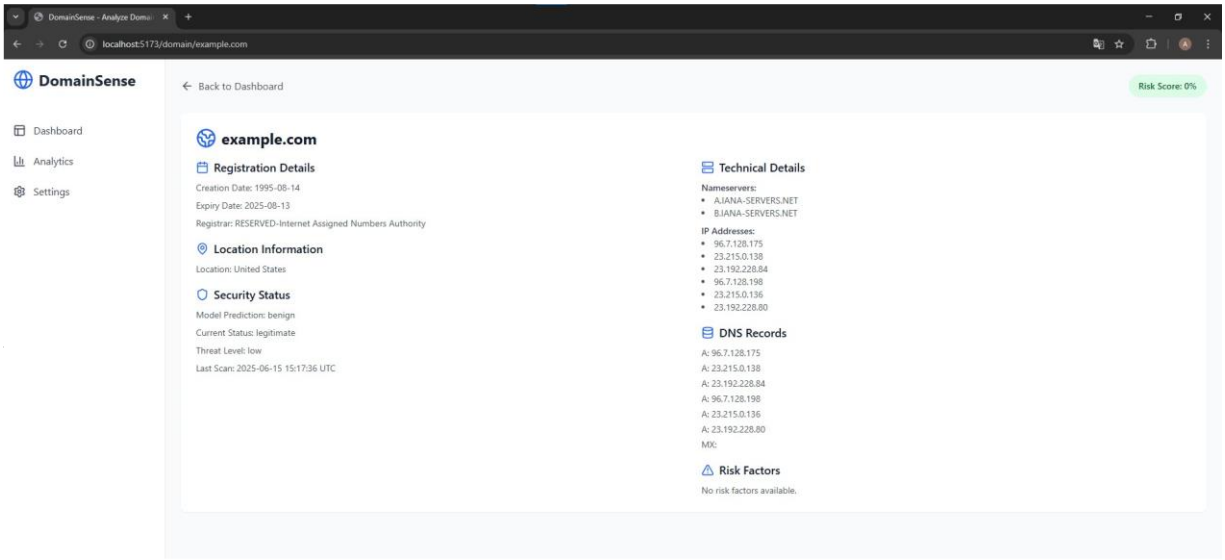


Рисунок Б.16 – Слайд презентації 16

Екран деталізації

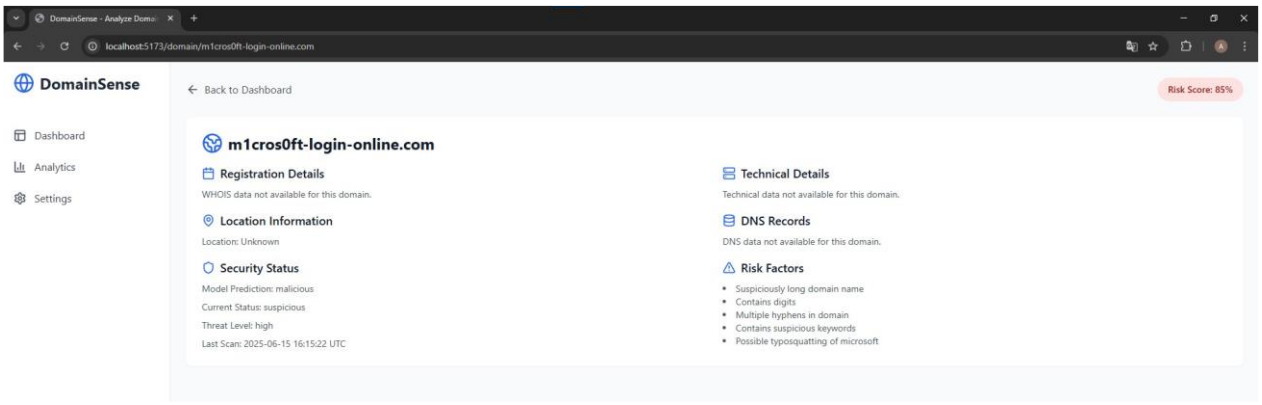


Рисунок Б.17 – Слайд презентації 17

Екран аналітики

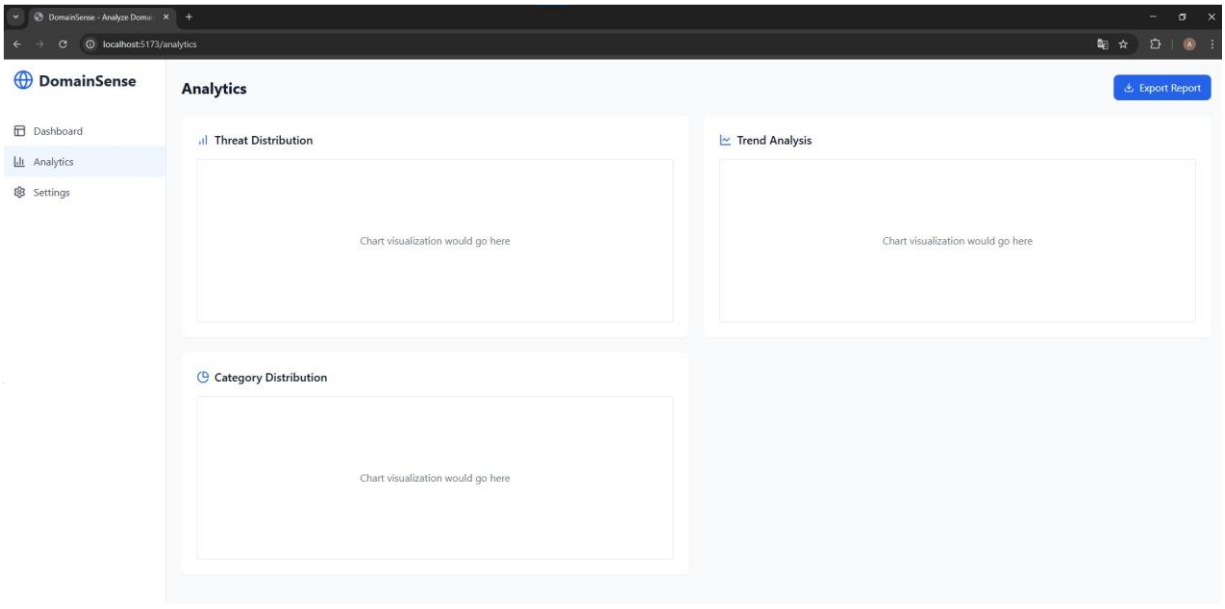


Рисунок Б.18 – Слайд презентації 18

Налаштування

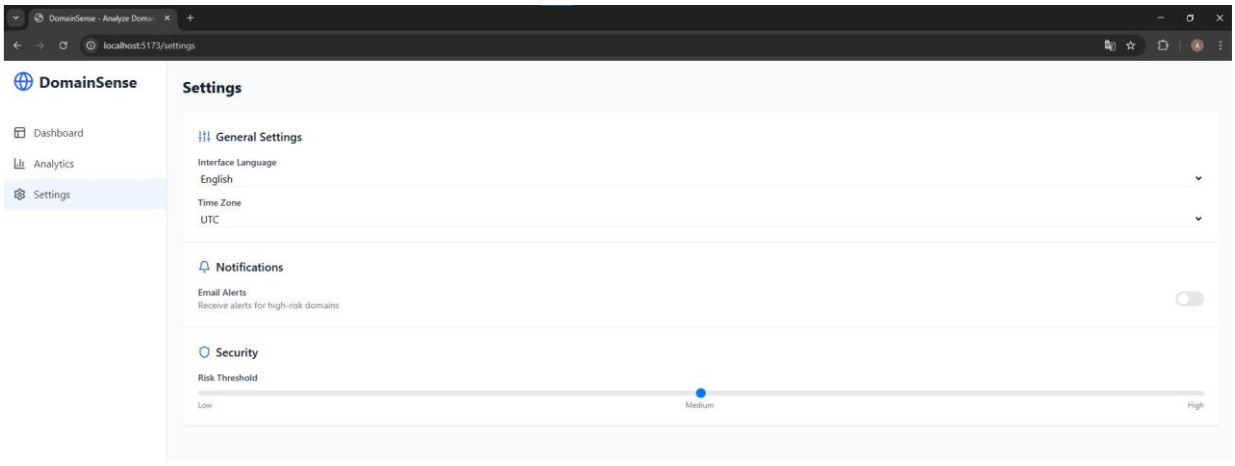


Рисунок Б.19 – Слайд презентації 19

Перспективи розвитку

- Підключення додаткових джерел даних
- Впровадження методів глибокого навчання та нейронних мереж для підвищення адаптивності
- Визначення конкретного типу загрози (фішинг/спам/тощо)
- Впровадження автоматичних механізмів реагування на загрози

Рисунок Б.20 – Слайд презентації 20

Публікація

Andrii Ushakov and Anatolii Rutkaş “Leveraging Big Data Technologies for Domain Name Security”,Modern Information Technologies and Artificial Intelligence Systems: Proceedings of the 1st International Scientific and Practical Conference. Part1, Kharkiv–Yaremche, May 19–22, 2025, ed. Yu.O. Romanenkov et al.– Kharkiv: NURE, 2025. – P. 202-205

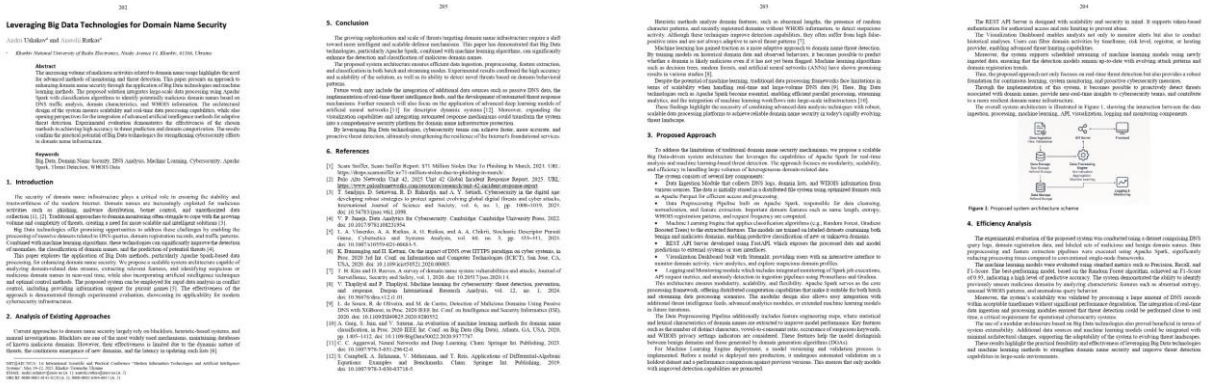


Рисунок Б.21 – Слайд презентації 21

Висновки

01 Досліджено сучасні тенденції та проблеми у сфері аналізу доменних імен

02 Ефективність використання Big Data і ML підтверджена експериментально

03 Система дозволяє точно й автоматизовано виявляти порушення в доменних іменах

04 Користувацький інтерфейс дозволяє візуалізувати результати у зручному форматі

05 Прототип готовий до масштабування й інтеграції з існуючими системами безпеки

Рисунок Б.22 – Слайд презентації 22

Демонстрація роботи програми

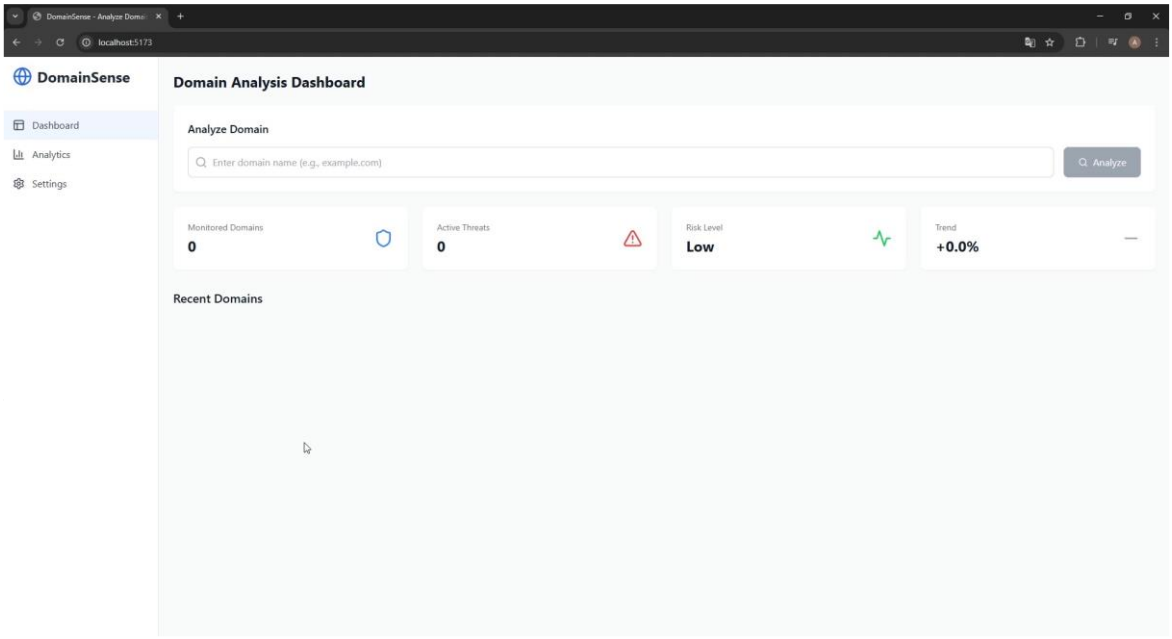


Рисунок Б.23 – Слайд презентації 23

Дякую за увагу!

Рисунок Б.24 – Слайд презентації 24

ДОДАТОК В

Апробація результатів роботи

Рисунок В.1 – Сертифікат про участь у конференції MIT@AIS-2025

Leveraging Big Data Technologies for Domain Name Security

Andrii Ushakov[a] and Anatolii Rutkas[a]

[a] *Kharkiv National University of Radio Electronics, Nauky Avenue 14, Kharkiv, 61166, Ukraine*

Abstract

The increasing volume of malicious activities related to domain name usage highlights the need for advanced methods of monitoring and threat detection. This paper presents an approach to enhancing domain name security through the application of Big Data technologies and machine learning methods. The proposed solution integrates large-scale data processing using Apache Spark with classification algorithms to identify potentially malicious domain names based on DNS traffic analysis, domain characteristics, and WHOIS information. The architectural design of the system ensures scalability and real-time data processing capabilities, while also opening perspectives for the integration of advanced artificial intelligence methods for adaptive threat detection. Experimental evaluation demonstrates the effectiveness of the chosen methods in achieving high accuracy in threat prediction and domain categorization. The results confirm the practical potential of Big Data technologies for strengthening cybersecurity efforts in domain name infrastructure.

Keywords

Big Data, Domain Name Security, DNS Analysis, Machine Learning, Cybersecurity, Apache Spark, Threat Detection, WHOIS Data

1. Introduction

The security of domain name infrastructure plays a critical role in ensuring the stability and trustworthiness of the modern Internet. Domain names are increasingly exploited for malicious activities such as phishing, malware distribution, botnet control, and unauthorized data collection [1], [2]. Traditional approaches to domain monitoring often struggle to cope with the growing volume and complexity of threats, creating a need for more scalable and intelligent solutions [3].

Big Data technologies offer promising opportunities to address these challenges by enabling the processing of massive datasets related to DNS queries, domain registration records, and traffic patterns. Combined with machine learning algorithms, these technologies can significantly improve the detection of anomalies, the classification of domain names, and the prediction of potential threats [4].

This paper explores the application of Big Data methods, particularly Apache Spark-based data processing, for enhancing domain name security. We propose a scalable system architecture capable of analyzing domain-related data streams, extracting relevant features, and identifying suspicious or malicious domain names in near-real time, while also incorporating artificial intelligence techniques and optimal control methods. The proposed system can be employed for rapid data analysis in conflict control, including providing information support for pursuit games [5]. The effectiveness of the approach is demonstrated through experimental evaluation, showcasing its applicability for modern cybersecurity infrastructures.

2. Analysis of Existing Approaches

Current approaches to domain name security largely rely on blacklists, heuristic-based systems, and manual investigations. Blacklists are one of the most widely used mechanisms, maintaining databases of known malicious domains. However, their effectiveness is limited due to the dynamic nature of threats, the continuous emergence of new domains, and the latency in updating such lists [6].

MIT@AIS'2025s: 1st International Scientific and Practical Conference "Modern Information Technologies and Artificial Intelligence Systems", May 19–22, 2025, Kharkiv-Yaremche, Ukraine
EMAIL: andrii.ushakov@nure.ua (A. 1); anatolii.rutkas@nure.ua (A. 2)
ORCID: 0000-0002-0141-8228 (A. 1); 0000-0002-6304-6837 (A. 2)

Рисунок В.2 – Текст публікації зі збірника матеріалів MIT@AISs-2025. Сторінка 1

Heuristic methods analyze domain features, such as abnormal lengths, the presence of random character patterns, and recently registered domains without WHOIS information, to detect suspicious activity. Although these techniques improve detection capabilities, they often suffer from high false-positive rates and are not always adaptive to novel threat patterns [7].

Machine learning has gained traction as a more adaptive approach to domain name threat detection. By training models on historical domain data and observed behaviors, it becomes possible to predict whether a domain is likely malicious even if it has not yet been flagged. Machine learning algorithms such as decision trees, random forests, and artificial neural networks (ANNs) have shown promising results in various studies [8].

Despite the potential of machine learning, traditional data processing frameworks face limitations in terms of scalability when handling real-time and large-volume DNS data [9]. Here, Big Data technologies such as Apache Spark become essential, enabling efficient parallel processing, streaming analytics, and the integration of machine learning workflows into large-scale infrastructures [10].

These findings highlight the necessity of combining advanced data analysis techniques with robust, scalable data processing platforms to achieve reliable domain name security in today's rapidly evolving threat landscape.

3. Proposed Approach

To address the limitations of traditional domain name security mechanisms, we propose a scalable Big Data-driven system architecture that leverages the capabilities of Apache Spark for real-time analysis and machine learning-based threat detection. The approach focuses on modularity, scalability, and efficiency in handling large volumes of heterogeneous domain-related data.

The system consists of several key components:

- Data Ingestion Module that collects DNS logs, domain lists, and WHOIS information from various sources. The data is initially stored in a distributed file system using optimized formats such as Apache Parquet for efficient access and processing.
- Data Preprocessing Pipeline built on Apache Spark, responsible for data cleansing, normalization, and feature extraction. Important domain features such as name length, entropy, WHOIS registration patterns, and request frequency are computed.
- Machine Learning Engine that applies classification algorithms (e.g., Random Forest, Gradient Boosted Trees) to the extracted features. The models are trained on labeled datasets containing both benign and malicious domains, enabling predictive classification of new or unknown domains.
- REST API Server developed using FastAPI, which exposes the processed data and model predictions to external systems or user interfaces.
- Visualization Dashboard built with Streamlit, providing users with an interactive interface to monitor domain activity, view analytics, and explore suspicious domain profiles.
- Logging and Monitoring module which includes integrated monitoring of Spark job executions, API request metrics, and anomaly detection in ingestion pipelines using Prometheus and Grafana.

This architecture ensures modularity, scalability, and flexibility. Apache Spark serves as the core processing framework, offering distributed computation capabilities that make it suitable for both batch and streaming data processing scenarios. The modular design also allows easy integration with additional threat intelligence feeds, advanced analytics modules, or extended machine learning models in future iterations.

The Data Preprocessing Pipeline additionally includes feature engineering steps, where statistical and lexical characteristics of domain names are extracted to improve model performance. Key features such as the number of distinct characters, vowel-to-consonant ratio, occurrence of suspicious keywords, and WHOIS privacy settings indicators are considered. These features help the model distinguish between benign domains and those generated by domain generation algorithms (DGAs).

For Machine Learning Engine deployment, a model versioning and validation process is implemented. Before a model is deployed into production, it undergoes automated validation on a holdout dataset and a performance comparison against previous versions. This ensures that only models with improved detection capabilities are promoted.

Рисунок В.3 – Текст публікації зі збірника матеріалів MIT@AISs-2025. Сторінка 2

The REST API Server is designed with scalability and security in mind. It supports token-based authentication for authorized access and rate limiting to prevent abuse.

The Visualization Dashboard enables analysts not only to monitor alerts but also to conduct historical analyses. Users can filter domain activities by timeframe, risk level, registrar, or hosting provider, enabling advanced threat hunting capabilities.

Moreover, the system supports scheduled retraining of machine learning models using newly ingested data, ensuring that the detection models remain up-to-date with evolving attack patterns and domain registration trends.

Thus, the proposed approach not only focuses on real-time threat detection but also provides a robust foundation for continuous learning, system monitoring, and proactive cybersecurity measures.

Through the implementation of this system, it becomes possible to proactively detect threats associated with domain names, provide near-real-time insights to cybersecurity teams, and contribute to a more resilient domain name infrastructure.

The overall system architecture is illustrated in Figure 1, showing the interaction between the data ingestion, processing, machine learning, API, visualization, logging and monitoring components.

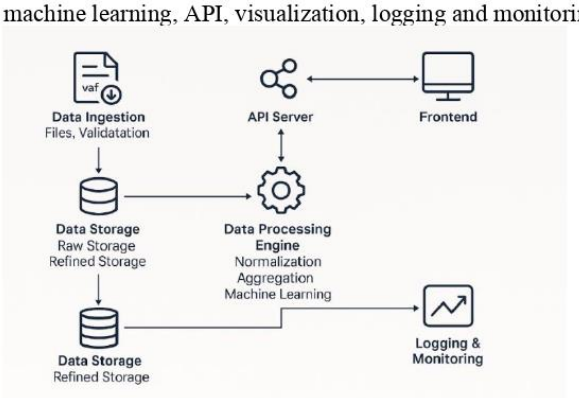


Figure 1: Proposed system architecture scheme

4. Efficiency Analysis

The experimental evaluation of the proposed system was conducted using a dataset comprising DNS query logs, domain registration data, and labeled sets of malicious and benign domain names. Data preprocessing and feature extraction pipelines were executed using Apache Spark, significantly reducing processing times compared to conventional single-node frameworks.

The machine learning models were evaluated using standard metrics such as Precision, Recall, and F1-Score. The best-performing model, based on the Random Forest algorithm, achieved an F1-Score of 0.93, indicating a high level of predictive accuracy. The system demonstrated the ability to identify previously unseen malicious domains by analyzing characteristic features such as abnormal entropy, unusual WHOIS patterns, and anomalous query behavior.

Moreover, the system's scalability was validated by processing a large amount of DNS records within acceptable timeframes without significant performance degradation. The integration of real-time data ingestion and processing modules ensured that threat detection could be performed close to real time, a critical requirement for operational cybersecurity systems.

The use of a modular architecture based on Big Data technologies also proved beneficial in terms of system extensibility. Additional data sources and machine learning models could be integrated with minimal architectural changes, supporting the adaptability of the system to evolving threat landscapes.

These results highlight the practical feasibility and effectiveness of leveraging Big Data technologies and machine learning methods to strengthen domain name security and improve threat detection capabilities in large-scale environments.

5. Conclusion

The growing sophistication and scale of threats targeting domain name infrastructure require a shift toward more intelligent and scalable defense mechanisms. This paper has demonstrated that Big Data technologies, particularly Apache Spark, combined with machine learning algorithms, can significantly enhance the detection and classification of malicious domain names.

The proposed system architecture ensures efficient data ingestion, preprocessing, feature extraction, and classification in both batch and streaming modes. Experimental results confirmed the high accuracy and scalability of the solution, as well as its ability to detect novel threats based on domain behavioral patterns.

Future work may include the integration of additional data sources such as passive DNS data, the implementation of real-time threat intelligence feeds, and the development of automated threat response mechanisms. Further research will also focus on the application of advanced deep learning models of artificial neural networks [11] for descriptor dynamic systems [12]. Moreover, expanding the visualization capabilities and integrating automated response mechanisms could transform the system into a comprehensive security platform for domain name infrastructure protection.

By leveraging Big Data technologies, cybersecurity teams can achieve faster, more accurate, and proactive threat detection, ultimately strengthening the resilience of the Internet's foundational services.

6. References

[1] Scam Sniffer, Scam Sniffer Report: $71 Million Stolen Due To Phishing In March, 2024. URL: https://drops.scamsniffer.io/71-million-stolen-due-to-phishing-in-march/.

[2] Palo Alto Networks Unit 42, 2025 Unit 42 Global Incident Response Report, 2025. URL: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report.

[3] T. Sendjaja, D. Setiawan, R. D. Rahardja, and A. Y. Setiadi, Cybersecurity in the digital age: developing robust strategies to protect against evolving global digital threats and cyber attacks, International Journal of Science and Society, vol. 6, no. 1, pp. 1008–1019, 2024. doi: 10.54783/ijsoc.v6i1.1098.

[4] V. P. Janeja, Data Analytics for Cybersecurity. Cambridge: Cambridge University Press, 2022. doi: 10.1017/9781108231954.

[5] L. A. Vlasenko, A. A. Rutkas, A. G. Rutkas, and A. A. Chikrii, Stochastic Descriptor Pursuit Game, Cybernetics and Systems Analysis, vol. 60, no. 3, pp. 433–441, 2024. doi: 10.1007/s10559-024-00684-5.

[6] K. Bumanglag and H. Kettani, On the impact of DNS over HTTPS paradigm on cyber systems, in Proc. 2020 3rd Int. Conf. on Information and Computer Technologies (ICICT), San Jose, CA, USA, 2020. doi: 10.1109/icict50521.2020.00085.

[7] T. H. Kim and D. Reeves, A survey of domain name system vulnerabilities and attacks, Journal of Surveillance, Security and Safety, vol. 1, 2020. doi: 10.20517/jsss.2020.14.

[8] V. Thapliyal and P. Thapliyal, Machine learning for cybersecurity: threat detection, prevention, and response, Darpan International Research Analysis, vol. 12, no. 1, 2024. doi: 10.36676/dira.v12.i1.01.

[9] L. de Souza, R. de Oliveira, and M. de Castro, Detection of Malicious Domains Using Passive DNS with XGBoost, in Proc. 2020 IEEE Int. Conf. on Intelligence and Security Informatics (ISI), 2020. doi: 10.1109/ISI49825.2020.9280552.

[10] A. Garg, S. Jain, and V. Saxena, An evaluation of machine learning methods for domain name classification, in Proc. 2020 IEEE Int. Conf. on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 1405–1412. doi: 10.1109/BigData50022.2020.9377787.

[11] C. C. Aggarwal, Neural Networks and Deep Learning. Cham: Springer Int. Publishing, 2023. doi: 10.1007/978-3-031-29642-0.

[12] S. Campbell, A. Ilchmann, V. Mehrmann, and T. Reis, Applications of Differential-Algebraic Equations: Examples and Benchmarks. Cham: Springer Int. Publishing, 2019. doi: 10.1007/978-3-030-03718-5.

Рисунок В.5 – Текст публікації зі збірника матеріалів MIT@AISs-2025. Сторінка 4

ДОДАТОК Г

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

1

Експертний висновок результатів перевірки кваліфікаційної роботи

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

Андрій УШАКОВ
(прізвище, ім'я, по батькові)

Зауваження

Пункт ДСТУ 3008-2015	Зміст пункту	Сторінка кваліфікаційної роботи
1	2	3
	7.1 Загальні положення	
	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.	31-32
	7.7 Переліки	
	7.8 Примітки	
	7.9 Виноски	
	7.10 Формули та рівняння	
	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.	Оформлення тексту заяви щодо самостійного виконання кваліфікаційної роботи та можливості її публікації в електронному архіві відкритого доступу ElArKhNURE не відповідає вимогам методичних вказівок (зразок тексту в шаблоні, стор.6).	6

Рисунок Г.1 – Експертний висновок результатів перевірки кваліфікаційної роботи на відповідність оформлення вимогам ДСТУ 3008:2015. Сторінка 1

Методичні вказівки до виконання кваліфікаційної роботи магістра… ЗАТВЕРДЖЕНО кафедрою ІП 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 ІП протокол № 12 від 03.02.2025 р.	Рисунок повинен розміщуватися одразу після його згадування у тексті, або на наступній сторінці. Під рисунком повинен бути підпис із словом Рисунок, порядковим номером цього рисунку, через тире з великої літери – назва рисунку. **В круглих дужках вказується джерело з якого взят цей рисунок, приклад: (за даними [2]), або то, що він виконаний самостійно, приклад: (рисунок створено самостійно). Шаблон стор.18 -19**	41, далі за текстом
Методичні вказівки до виконання кваліфікаційної роботи магістра… **ЗАТВЕРДЖЕНО кафедрою ІП 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 ІП протокол № 12 від 03.02.2025 р.**	Назву таблиці друкують з великої літери і розміщують над таблицею з абзацного відступу. **В круглих дужках вказується джерело з якого взята ця таблиця, приклад: (таблиця виконана за даними [2]), або то, що вона виконана самостійно, приклад: (таблиця виконана самостійно). Шаблон стор.15**	31, далі за текстом

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

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

18.06.2025

Рисунок Г.1 – Експертний висновок результатів перевірки кваліфікаційної роботи на відповідність оформлення вимогам ДСТУ 3008:2015. Сторінка 2