

УДК 53+51+044  
ТЗЗ

*Рекомендовано Вченою радою НН ФТІ  
КПІ ім. Ігоря Сікорського  
(Протокол № 5/2024 від 25.05.2024 р.)*

**ТЗЗ Теоретичні і прикладні проблеми фізики, математики та інформатики:** матеріали XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (13–17 травня 2024 р., м. Київ, Україна) / Уклад.: Пономаренко С. М., Бех С. В., Степаненко В. М., Мирошникова І. Ю., Деркач О. Г., Козленко О. В., Мікава П. В. – Київ : КПІ ім. Ігоря Сікорського, Видавництво «Політехніка», 2024. – 377 с.  
ISBN 978-966-990-053-1

Матеріали конференції присвячені сучасним проблемам фізики та фізичних технологій, перспективним напрямкам фізики енергетичних систем, теорії кібербезпеки, криптографічного захисту інформації та криптоаналізу, захисту інформації в комп'ютерних мережах та комунікаціях, забезпеченню цілісності баз даних та їх обробки, захисту від витоку інформації по каналах побічного електромагнітного випромінювання, локальним мережам різної структури, технічного захисту об'єктів, а також науковим дослідженням фундаментального та прикладного характеру у сфері інформаційних наук.

Для студентів, аспірантів та молодих науковців вищих навчальних закладів і науково-дослідних установ, що працюють у різноманітних галузях математики та фізики, а також майбутніх фахівців із кібербезпеки.

Відповідальний за випуск: Пономаренко С. М.  
Дизайн та верстка збірника: Пономаренко С. М.  
Програма верстки: L<sup>A</sup>T<sub>E</sub>X 2<sub>ε</sub>

Офіційний сайт конференції: [conf.ipt.kpi.ua](http://conf.ipt.kpi.ua)

*Доповіді учасників конференції наведені в авторській редакції*

ISBN 978-966-990-053-1

© Автори статей, 2024 р.

© КПІ ім. Ігоря Сікорського (НН ФТІ), 2024 р.

3. Бумерангова еквівалентність S-блоків відносно різних алгебраїчних операцій . . . . .	194
<i>Р. В. Буржимський</i>	
4. Імовірності диференціалів LRX-перетворень спеціального виду . . . . .	198
<i>О. О. Галіца, С. В. Яковлев</i>	
5. Квантова атака розрізнення на розширену узагальнену мережу Фейстеля . . . . .	202
<i>Б. В. Дигас</i>	
6. Індeksi складності випадкових зростаючих графів . . . . .	205
<i>Д. М. Калитюк, І. І. Ніщенко</i>	
7. Побудова зведення задачі SVP до задачі пошуку основного стану гамільтоніану для алгоритму QAOA . . . . .	209
<i>М. А. Кістаєв</i>	
8. Диференціально-обертальний криптоаналіз ARX-криптосистем за операцією модульного додавання . . . . .	213
<i>Д. С. Кобець, С. В. Яковлев</i>	
9. Задача фільтрації для частково спостережуваного процесу міграції частинок в багатоурнній моделі Ернфестів . . . . .	216
<i>О. М. Ковальчук, І. І. Ніщенко</i>	
10. Криптоаналіз схем цифрового підпису «Вершина» та «Сокіл» . . . . .	220
<i>Ю. С. Литвиненко</i>	
11. Аналіз підходів до пошуку високоїмовірнісних усічених диференціалів спеціального вигляду . . . . .	224
<i>К. А. Медведцький, О. П. Якимчук</i>	
12. Побудова диференціальної атаки збоїв на модифікований шифр Qalqan . . . . .	228
<i>М. А. Недождій, С. В. Яковлев</i>	
13. Побудова квантового протоколу узгодження автентичного ключа QAKAP . . . . .	231
<i>Ю. С. Починок</i>	
14. Криптографічні атаки на AES на основі інформації з побічного каналу . . . . .	234
<i>Є. Ю. Толмачов</i>	
15. Імовірність атаки подвійної витрати для протоколу консенсусу Proof-of-Stake у випадку декількох слотлідерів в одному таймслоті . . . . .	238
<i>А. І. Яценко</i>	

---

Секція

---

## Системи та технології кібернетичної безпеки

---

1. Оцінка готовності кіберфізичної системи об'єкту критичної інфраструктури до досліджень методами форензики . . . . .	243
<i>А. М. Алькова, І. В. Стъопочкіна, О. С. Лиманюк</i>	
2. Ризики використання SSH та методи їх усунення . . . . .	247
<i>Д. Ю. Андреев, С. А. Смирнов</i>	
3. Покращення безпеки смарт-контрактів у мережі Ethereum . . . . .	249
<i>Д. О. Ващенко, Л. Ю. Гальчинський</i>	
4. Формування семантичної мапи кібер загроз із застосуванням штучного інтелекту . . . . .	252
<i>О. О. Гуменюк, І. М. Свобода, А. В. Комар, Д. В. Ланде</i>	
5. Автоматизований процес перевірки документів/файлів на наявність прихованого шкідливого по за допомогою онлайн сервісів аналізу файлів . . . . .	255
<i>І. О. Качур</i>	
6. Форензика у блокчейні Ethereum . . . . .	258
<i>Д. О. Ковбель, О. М. Барановський</i>	

7. Дослідження методів функціонування та розробки C&C агентів . . . . .	261
<i>Є. П. Кодак, О. М. Барановський</i>	
8. Виявлення аномалій в процесах автентифікації з використанням ELK Stack та Suricata . . . . .	263
<i>Т. Б. Корабельський, В. В. Демчинський</i>	
9. Пом'якшення наслідків атаки на нижньому рівні управління, як елемент резильєнтності об'єктів критичної інфраструктури . . . . .	265
<i>Д. А. Косарик, Л. Ю. Гальчинський</i>	
10. Детекція та протидія атакам Pass the hash OverPass the hash шляхом аналітики поведінки . . . . .	268
<i>О. С. Косигін, Л. Ю. Гальчинський</i>	
11. Система виявлення вторгень в SCADA-системи як елемент кібервідмовостійкості	272
<i>С. С. Літвінчук, Л. Ю. Гальчинський</i>	
12. Вразливості та захист Microsoft OAuth SSO . . . . .	275
<i>М. В. Маковська, В. В. Демчинський</i>	
13. Тестування безпеки WiFi за допомогою Wireshark . . . . .	279
<i>Д. О. Мартиненко, М. В. Коломицев</i>	
14. Роль методів OSINT в кібербезпеці та їх застосування під час воєнних конфліктів	282
<i>І. О. Мірошніченко, Д. В. Ланде</i>	
15. Оцінка методів виявлення надлишкових прав суб'єктів на об'єкти у хмарному середовищі Amazon AWS (на прикладі комерційного продукту Tenable Cloud Security) . . . . .	285
<i>О. І. Новак, Л. Ю. Гальчинський</i>	
16. Застосування алгоритмів машинного навчання для виявлення аномалій мережного трафіку . . . . .	288
<i>О. П. Подвисоцька, С. О. Носок</i>	
17. Розробка методу виявлення RAT троянів з C2C quic комунікацією . . . . .	291
<i>Н. Р. Пошивак, О. М. Барановський</i>	
18. Виявлення безпекових проблем в докерфайлах . . . . .	293
<i>М. В. Супрун, Л. Ю. Гальчинський</i>	
19. Захист системи керування контейнерами Kubernetes . . . . .	296
<i>Ю. П. Тимченко</i>	

---

Секція

---

## Математичне моделювання та аналіз даних

---

1. Використання SAT-розв'язувача в $n$ -ках Шура . . . . .	301
<i>В. В. Бичок, А. Васалатій, О. В. Циганкова, М. О. Хмельницький</i>	
2. Конденсація датасету зображень ОКТ методом відповідних градієнтів . . . . .	304
<i>О. А. Вергелюк, Н. В. Шаповал</i>	
3. Перенесення моделі машинного навчання для супутникового картографування концентрації хлорофілу-а . . . . .	308
<i>П. О. Геніцой, Б. Я. Яйлимов, А. Ю. Шелестов</i>	
4. Екстраполяція якості повітря в міському середовищі з обмеженою кількістю станцій	313
<i>Д. К. Городецька, Г. О. Яйлимова</i>	
5. Методи моніторингу та аналізу здоров'я лісів за супутниковими даними . . . . .	318
<i>В. Е. Іорданова, Г. О. Яйлимова</i>	
6. Методи і моделі розпізнавання образів, які отримані безпілотними літальними апаратами . . . . .	322
<i>Є. В. Кірсенко, В. В. Хайдуров</i>	

## ФОРМУВАННЯ СЕМАНТИЧНОЇ МАПИ КІБЕР ЗАГРОЗ ІЗ ЗАСТОСУВАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

О. О. Гуменюк<sup>1</sup>, І. М. Свобода<sup>1</sup>, А. В. Комар<sup>1</sup>, Д. В. Ланде<sup>1</sup>

<sup>1</sup> Навчально-науковий Фізико-технічний інститут

### Анотація

Формування семантичної мапи кібер загроз із застосуванням штучного інтелекту представляє новітній підхід для оперативного виявлення потенційних загроз в реальному часі. Розроблена система інтегрує алгоритми для збору, аналізу та класифікації даних, що забезпечує комплексний аналіз кіберзагроз і візуалізацію їх динаміки. Особливість методу полягає у виявленні зв'язків між кіберінцидентами та аналізі їх характеристик і трендів розвитку.

**Ключові слова:** кібербезпека, штучний інтелект, соціальні медіа, моніторинг, машинне навчання, обробка природної мови, telegram

### Вступ

На сучасному етапі розвитку інформаційних технологій, кібербезпека набуває особливого значення у зв'язку зі зростанням числа кіберзагроз, що еволюціонують і стають все складнішими. Соціальні медіа, особливо платформа Telegram, відіграють ключову роль у поширенні інформації [1], яка може включати шкідливі повідомлення та кібератаки. Значний обсяг даних, генерований користувачами, вимагає нових методів та технологій, заснованих на штучному інтелекті, машинному навчанні та обробці природної мови, для швидкого та точного аналізу. Це дослідження зосереджене на розробці та застосуванні передових технік для аналізу потенційних загроз кібербезпеки через моніторинг соціальних медіа, з акцентом на платформі Telegram, яка, з огляду на її широке використання та великий обсяг обміну інформацією, стає цінним джерелом для ідентифікації кіберзагроз. Це дозволяє оперативно реагувати на них та забезпечувати вищий рівень захисту інформації.

### 1. Розробка методології

Аналіз кіберзагроз на основі соціальних медіа включає декілька етапів: збір даних, виявлення подій, ідентифікація оригінальних подій, встановлення причинно-наслідкових зв'язків, аналіз і візуалізація мережі подій, а також кластеризація [2]. Нижче наведено детальний опис кожного з цих етапів.

**Збір даних.** Збір новинних повідомлень здійснюється за допомогою існуючих систем пошуку новин, які можуть бути як безкоштовними, так і платними. Відібрані повідомлення фільтруються за темою дослідження та очищуються від шуму і незначущих даних. Для цього процесу використовують наступну

формулу:

$$F_{\text{news}}(t, k, C) = \left\{ \begin{array}{l} \text{articles.date} \in [t_{\text{start}}, t_{\text{end}}] \wedge \\ \text{articles} \mid \text{keywords}(\text{articles}) \cap k \neq \emptyset \wedge \\ \text{articles.channel} \in C \end{array} \right\} \quad (1)$$

де:

- $t$  – часові параметри (дата початку та кінця),
- $k$  – набір ключових слів,
- $C$  – набір ідентифікаторів каналів.

**Виявлення подій.** Для виявлення подій у текстах новинних повідомлень застосовуються генеративні мовні моделі, такі як GenAI [3]. Цей процес включає формування масиву коротких позначень виявлених подій. Використовується наступна формула:

$$E_{\text{detect}}(\text{text}) = \{e_1, e_2, \dots, e_n \mid e_i \in \text{extract\_events}(\text{text})\} \quad (2)$$

де функція *extract\_events* використовує методи NLP для витягування подій із тексту.

**Встановлення причинно-наслідкових зв'язків.** Встановлення причинно-наслідкових зв'язків між подіями здійснюється за допомогою генеративних моделей, які аналізують події та визначають їхні взаємозв'язки. Для цього використовується формула:

$$C_{\text{link}}(E) = \{(e_i, e_j) \mid \text{cause}(e_i, e_j)\} \quad (3)$$

де функція *causecause* визначає пари подій, де подія  $e_i$  є причиною події  $e_j$ .

**Аналіз та візуалізація мережі подій.** Мережа подій аналізується для виявлення ключових подій, кластерів та ланцюгів, що їх зв'язують. Інтерактивна візуалізація мережі подій здійснюється за допомогою наступної формули:

$$S_{\text{map}}(E, L) = \{(e, \text{link}(e)) \mid e \in E \wedge \text{link}(e) \in L\}, \quad (4)$$

де кожна подія  $e$  пов'язана з URL або документальним посиланням  $link(e)$ .

**Кластеризація подій.** Для кластеризації подій застосовується метод максимізації модулярності. Модулярність ( $Q$ ) визначається як міра сили поділу мережі на модулі (або кластери):

$$Q = \frac{1}{2m} \sum_{ij} \left( S_{ij} - \left[ S_{ij} - \frac{k_i k_j}{2m} \right] \delta(C_i, C_j) \right), \quad (5)$$

де:

- $S_{ij}$  — елемент матриці схожості,
- $k_i$  і  $k_j$  — суми ваг ребер, прикріплених до вузлів  $i$  і  $j$ ,
- $m$  — сума всіх ваг у мережі,
- $C_i, C_j$  — спільноти вузлів  $i$  та  $j$
- $\delta$  — дельта Кронекера, який дорівнює 1, якщо  $i$  і  $j$ , знаходяться в одній спільноті, і 0 в іншому випадку.

Для оцінки якості кластеризації можна використати коефіцієнт силуєту, який розраховується за формулою:

$$s(i) = \frac{b(i) - a(i)}{\max\{a(i), b(i)\}} \quad (6)$$

де:

- $a(i)$  — середня відстань між  $i$  та всіма іншими точками у кластері, до якого належить  $i$ ,
- $b(i)$  — мінімальна середня відстань від  $i$  до всіх точок у будь-якому іншому кластері, членом якого  $i$  не є.

Коефіцієнт силуєту:

$$s(i) = \frac{b(i) - a(i)}{\max\{a(i), b(i)\}}. \quad (7)$$

Ця формула визначає коефіцієнт силуєту для кожної точки  $i$  у кластеризованій мережі подій. Вона використовує середню відстань до точок у тому ж кластері  $a(i)$  та найменшу середню відстань до точок у сусідніх кластерах  $b(i)$  для оцінки якості кластеризації.

**Візуалізація.** Результати аналізу візуалізуються за допомогою інтерактивних дашбордів, які демонструють зв'язки між подіями, динаміку змін загроз у часі та географічний розподіл кіберінцидентів [4]. Це дозволяє користувачам системи швидко оцінювати рівень загрози та відповідно реагувати.

## 2. Реалізація системи та приклад застосування методології

Система призначена для забезпечення ефективної обробки даних у реальному часі з використанням масштабованої та надійної архітектури. Вона складається з кількох ключових компонентів, кожен з яких відіграє важливу роль у процесі збору, обробки та аналізу інформації.

### Компоненти системи:

- **Модуль збору даних:** використовує API для постійного збору інформації з платформи Telegram. Цей модуль оснащений фільтрами, які налаштовуються відповідно до специфічних параметрів, таких як ключові слова, діапазони

дат та частота подій, що дозволяє збирати лише релевантну інформацію для подальшого аналізу.

- **Модуль обробки даних:** використовує алгоритми машинного навчання та інструменти обробки природної мови для аналізу текстової інформації. Він видаляє шум та нерелевантні дані, класифікує вміст за рівнями загроз та видобуває ключові тематичні елементи.
- **Управління базами даних:** відповідає за зберігання оброблених даних у структурованому форматі у безпечній, масштабованій базі даних, що дозволяє швидко отримувати доступ до інформації та ефективно нею управляти.
- **Інтеграція з платформами кібербезпеки:** система розроблена з урахуванням безперервної інтеграції з існуючими платформами моніторингу кібербезпеки через добре визначені API та рішення проміжного програмного забезпечення, що підвищує ефективність існуючих систем реагування на інциденти [5].
- **Інтерфейс користувача:** реалізований з використанням Flutter, дозволяє ефективно взаємодіяти з системою як технічним, так і нетехнічним користувачам. Інтерактивні дашборди та налаштовувані перегляди надають можливість користувачам отримувати необхідну інформацію відповідно до їхніх потреб.

**Інновації в аналізі даних.** Система використовує генеративні моделі штучного інтелекту для поліпшення інтерпретації і розпізнавання даних, а також розширює можливості для ефективного виявлення та реагування на кіберзагрози [6]. Планується подальше оновлення та інтеграція новітніх технологій для забезпечення актуальності та конкурентоспроможності у боротьбі з сучасними кібервикликами.

### 2.1. Приклад застосування методології

Застосуємо нашу методологію для аналізу новин за ключовим словом «vulnerability».

1. Збір даних: Використовуючи системи пошуку новин, збираються новини, що відповідають заданим параметрам часу, ключовим словам та каналам.

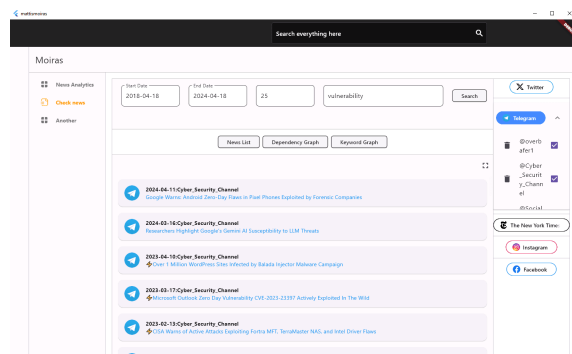


Рис. 1. Скріншот роботи клієнтського застосунку для введених параметрів

- Виявлення подій: Зібрані новини аналізуються для виявлення подій.
- Ідентифікація оригінальних подій: Ідентифікуються оригінальні події серед виявлених та вилучаються дублікати.
- Встановлення причинно-наслідкових зв'язків: Встановлюються причинно-наслідкові зв'язки між подіями.

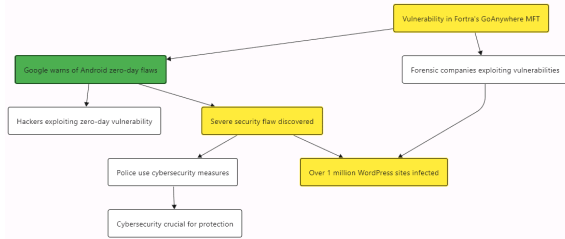


Рис. 2. Карта зв'язку між подіями у вигляді графу

- Аналіз та візуалізація мережі подій: Формується мережа подій та створюється інтерактивна візуалізація, використовуючи формулу (5), після чого здійснюється побудова графів, що відображають зв'язки між цими подіями.
- Кластеризація подій: Події кластеризуються для виявлення модулів у мережі за допомогою максимізації модулярності, використовуючи формулу (6). Кластеризація перевіряється за допомогою коефіцієнта силуету, використовуючи (7).

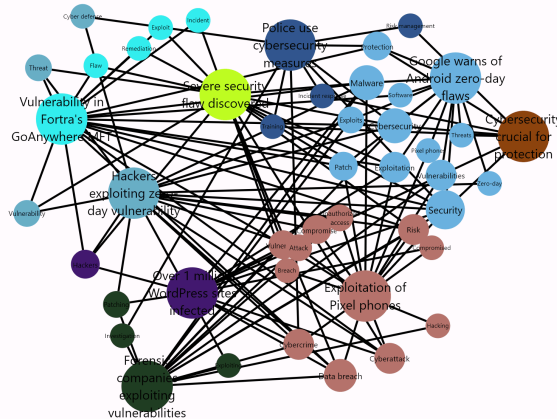


Рис. 3. Граф ключових слів до запити «vulnerability»

## Висновки

У результаті проведеного дослідження було розроблено нові методи аналізу та моніторингу кібер-

інцидентів через соціальні медіа, що дозволяють автоматизовано виявляти, ідентифікувати та аналізувати кіберзагрози, а також візуалізувати їх у реальному часі. Автоматизація цього процесу значно зменшує час та ресурси, необхідні для аналізу великих обсягів даних, дозволяючи оперативно досліджувати динаміку загроз та ефективно відреагувати на них. Запропонована методологія є гнучкою і адаптується до різних платформ соціальних медіа, що робить її універсальним інструментом для дослідження кіберзагроз. Використання штучного інтелекту сприяє виявленню нових тенденцій та причинно-наслідкових зв'язків між кіберінцидентами, що відкриває нові можливості для прогнозування майбутніх загроз та розробки ефективних стратегій кіберзахисту. Перспективи розвитку методології включають розширення джерел даних, розробку складніших інструментів візуалізації, використання машинного навчання для прогнозування атак, а також інтеграцію навчальних модулів для підвищення обізнаності у кібербезпеці.

## Перелік використаних джерел

- Detection and resolution of rumours in social media: A survey / A. Zubiaga, A. Aker, K. Bontcheva, M. Liakata, P. R // Natural Hazards and Earth System Sciences. — 2018. — Feb. — Vol. 21. — P. 10. — URL: <https://doi.org/10.1145/3161603>.
- Kruspe A., Kersten J., Klan F. Review article: Detection of actionable tweets in crisis events // ACM Computing Surveys. — 2021. — June. — Vol. 51. — P. 20. — URL: <https://doi.org/10.5194/nhess-21-1825-2021>.
- Lande D., Strashnoy L. GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now // Engineering. — 2023. — Vol. 2131. — P. 168. — URL: <https://ssrn.com/abstract=4541673>.
- Cherven K. Mastering Gephi Network Visualization // Packt Publishing. — 2015. — P. 378. — URL: <http://gephi.michalnovak.eu/Mastering%20Gephi%20Network%20Visualization.pdf>.
- Cyber-Attack Features for Detecting Cyber Threat Incidents from Online News / M. Abdullah, A. Zainal, M. Maarof, M. Nizam // Proceedings of the 2018 Cyber Resilience Conference. — 2018. — URL: <https://doi.org/10.1109/CR.2018.8626866>.
- Munkhdorj B., Yuji S. Cyber attack prediction using social data analysis // Journal of High Speed Networks. — 2017. — Vol. 23. — P. 26. — URL: <https://doi.org/10.3233/JHS-170560>.