ЕКОГІНТОКС
НАУКОВИЙ ЦЕНТР Л.І. МЕДВЕДЯ 1994

CyberLab
Комп'ютерна криміналістика

УКР ТЕЛЕРАДІОПРЕСІНСТИТУТ

Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором

МІЖВІДОМЧА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

27 березня 2024 року, м. Київ

УКРАЇНСЬКИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ СПЕЦІАЛЬНОЇ ТЕХНІКИ ТА СУДОВИХ ЕКСПЕРТИЗ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ВПРОВАДЖЕННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ ТА МОДЕРНІЗАЦІЯ ТЕХНІЧНОЇ СКЛАДОВОЇ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ ЯК ВАГОМИЙ ЧИННИК У БОРОТЬБІ З АГРЕСОРОМ

Збірник матеріалів міжвідомчої науково-практичної конференції

27 березня 2024 року

м. Київ

УДК 351.746.1+351.86]:[004:001.95]](477-651.2:470-651.1)(06)
В80

Рекомендовано до друку Науково-технічною радою ІСТЕ СБУ
(протокол № 4 від 29 травня 2024 року)

В80 Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором : зб. матеріалів міжвідомчої науково-практичної конференції, 27 березня 2024 р., Київ / [відп. ред. Парфило О.А.] ; Укр. наук.-дослід. ін.-т спец. техніки та судових експертиз Служби безпеки України. — Київ : ІСТЕ СБУ, 2024. — 298 с.

ISBN 978-617-8013-62-2

Збірник сформований за матеріалами доповідей і презентацій учасників міжвідомчої науково-практичної конференції «Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором», що відбулася 27 березня 2024 року.

Автори розглянули питання використання новітніх технологій, зокрема штучного інтелекту при розробці та застосуванні роботизованих комплексів і безпілотних літальних апаратів (БПЛА), впровадження сучасних інструментів для OSINT розвідки тощо.

Розраховано на представників суб'єктів сектору безпеки і оборони України, співробітників судових, правоохоронних органів і спеціальних служб, установ судової експертизи, науковців, викладачів, аспірантів, ад'юнктів та докторантів закладів вищої освіти.

ISBN 978-617-8013-62-2

УДК 351.746.1+351.86]:[004:001.95]](477-651.2:470-651.1)(06)

ЛАНДЕ Дмитро Володимирович,
доктор технічних наук, професор,
керівник наукового центру НДІ
інформатики і права НАПрН України

ФОРМУВАННЯ, АНАЛІЗ І ВІЗУАЛІЗАЦІЯ МЕРЕЖ ПОДІЙ У СФЕРІ КІБЕРБЕЗПЕКИ НА ОСНОВІ ЗАСТОСУВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Виявлення нових подій у текстових новинних повідомленнях є традиційною задачею в області обробки природної мови, на розв'язання якої було спрямовано значну кількість наукових досліджень [1; 2]. У галузі кібербезпеки також вивчалися завдання виявлення подій, що перетинаються між кібербезпекою та комп'ютерною лінгвістикою [3; 4].

Крім того, завдяки революції у сфері штучного інтелекту (GenAI) та появі великих лінгвістичних моделей, тепер можливо не лише виявляти події, а й створювати каузальні мережі подій, де явно відображені причинно-наслідкові зв'язки. Для вирішення цієї задачі наразі можуть використовуватись великі лінгвістичні моделі, такі як ChatGPT (https://chat.openai.com/), Llama-2 (https://www.llama2.ai/), Gemini (https://gemini.google.com/app), Deep Seek (https://deepseek.com). Додатковий розгляд мережі подій дає можливість виявляти групи та послідовності подій, які схожі на ті, що визначаються в сценарному аналізі [5]. Основна ідея нового підходу полягає у тому, що замість традиційних концептів вузлами каузальних мереж є події. Запропонована методологія дозволяє розглядати певні події як вузли. Сформовані мережі можуть служити орієнтирами у світі подій і використовуватись для проведення досліджень і розслідувань, зокрема в галузі парламентського контролю. Аналіз і візуалізація сформованих каузальних мереж подій можуть здійснюватись за допомогою стандартних інструментів аналізу мереж, зокрема, таких як Gephi [6] або GraphViz [7]. При цьому, подібно до традиційних каузальних мереж, можуть виділятися вузли з найбільшою кількістю зв'язків, і встановлюватися ланцюжки різної довжини, де кожна ланка складається з подій, що є наслідками багатьох причин. Деякі події можуть виступати як "посередники", які зв'язують багато причин і наслідків, функціонуючи як зв'язкові ланки для одночасно багатьох причин і наслідків.

Процес створення мережі подій з новинних повідомлень про кібербезпеку включає такі кроки:

1. Отримання повідомлень, що відповідають деякій цільовій тематиці за допомогою наявних систем пошуку новин (вільних або пропрієтарних).

2. За допомогою засобів GenAI здійснюється виявлення подій, що містяться у вибраних повідомленнях, створення масиву позначень цих подій.

3. Виявлення оригінальних подій серед відібраного масиву.

4. Зв’язування подій причинно-наслідковими зв’язками.

5. Формування і візуалізація семантичної мапи за допомогою графічного інструменту на основі бібліотеки GraphViz.

6. Виявлення концептів (ключових слів), що відповідають вибраним подіям.

7. Формування і візуалізація об’єднаної не спрямованої мережі подій і концептів.

8. Кластеризація подій на основі аналізу об’єднаної мережі.

Слід зазначити, що система Gephi дозволяє візуалізувати, виявляти кластери, проводити підрахунок і аналіз параметрів сформованих каузальних мереж, а програма побудовані на основі GraphViz дозволяють створювати інтерактивні семантичні мапи за рахунок застосування графічного формату SVG. У цьому випадку кожний вузол або ребро мережі може містити гіперпосилання на ресурси мережі Інтернет, зокрема на пошукові системи Google, Google News, Bing, Bing News тощо, або корпоративні новинні системи.

Розглянемо приклад, що стосується подій у сфері кібербезпеки і їх інтерпретацій. Для цього на першому етапі формується масив цільових документів, для чого у базі даних системи контент-моніторингу виконується запит вигляду «кібератаки». Серед отриманих документів розглядається документ з таким вмістом:

Як українські банки захищаються від кібератак в умовах війни: розповідає Євген Балютов, директор з інформаційної безпеки Райффайзен Банку

З початком повномасштабної війни кількість кібератак на Україну зросла щонайменше удесятеро. Втім, реальні масштаби проблеми можуть бути навіть більшими, каже директор з питань інформаційної безпеки Райффайзен Банку Євген Балютов. Як банківський сектор впорався із викликами кібервійни, які нові види кібервтручань з'явились в українському ландшафті, про наслідки кібератаки на Київстар для фінустанов, а також про особливості переїзду банків у хмару - читайте в ексклюзивному інтерв'ю Євгена Балютова для UA.NEWS.//

На другому етапі для знайдених документів застосовується запит (промпт):

В тексті описані деякі події. Детектуй їх, назви мені у вигляді нумерованого списку. Кожна подія 4-5 слів. Ось текст: Як українські банки захищаються від кібератак в умовах війни: розповідає Євген Балютов, директор з інформаційної безпеки Райффайзен Банку
З початком повномасштабної війни кількість кібератак на Україну зросла щонайменше удесятеро…

У результаті множинного виконання цього промпту у різних системах штучного інтелекту (Gemini, ChatGPT, DeepSeec) формується масив позначень подій, ні всі серед яких є оригінальними. Тобто можливі повтори, перекази різними словами:

1. «Початок повномасштабної війни»
2. «Зростання кількості кібератак на Україну»
3. «Збільшення кількості кіберінцидентів з 2021 року»

4. «З'явлення нового тренду в атаках на рівні держави»
5. «Зміна у ландшафті кіберзагроз.

На третьому етапі здійснюється фільтрація подій, тобто обираються оригінальні, для чого весь масив відібраних позначень подій надається системі GenAI та виконується промпт:

Із названих подій обери оригінальні і найважливіші. Дублікати вилучай.
Ось події:
1. «Початок повномасштабної війни»
2. «Зростання кількості кібератак на Україну»
3. «Збільшення кількості кіберінцидентів з 2021 року»
4. «З'явлення нового тренду в атаках на рівні держави» …

На четвертому етапі система генеративного штучного інтелекту формує причинно-наслідкові зв'язки серед виявлених оригінальних подій, для чого виконується промпт:

Видай пари взаємопов'язаних подій за принципом причина-наслідок. Ось події:
1. Початок повномасштабної війни
2. Збільшення кількості кібератак на Україну
3. Підготовча фаза перед початком повномасштабної війни
4. Зростання технічних можливостей для відбиття кібератак у банківській індустрії України …

Відповідь, зокрема, системах ChatGPT і Gemini на цей промпт:

«Зростання кількості кібератак на Україну; Збільшення технічних можливостей для відбиття кібератак у банківській індустрії України»
«Підготовча фаза перед початком повномасштабної війни; Кібератака на Київстар та її наслідки для банківської інфраструктури»
«Використання технік соціальної інженерії у кібератаках; Проблеми з доставкою SMS на фінансові номери Київстар» …

На п'ятому етапі відібрані події групуються у CSV-файл, записи якого мають формат «подія-причина; подія-наслідок». Цей файл може завантажуватись у програму аналізу і візуалізації мереж CSV2Graph (https://bigsearch.space/uli.html), розроблену на базі бібліотеки GraphViz. У результаті виконання цієї програми формується відображення графу подій (Рис. 1) Кожне ребро і вузол цього графа є гіперпосиланням із відповідними запитами до систем Google або Bing.

Задача кластеризації подій потребує формування простору параметрів, у якості якого запропоновано застосовувати множину ключових слів, що відповідають подіям. Для виявлення ключових слів для кожної визначеної події було відпрацьовано відповідний промпт, що включав запит і назву події, наприклад:

Назви 10 ключових слів, пов'язаних з подією: Зростання кількості кібератак на Україну

Після отримання множини ключових слів, кожна подія і кожне відповідне ключове слово розглядалась як вузли мережі, а зв’язками між ними виступало відношення приналежності ключового слова події (одне ключове слово при цьому може відноситись до декількох подій).

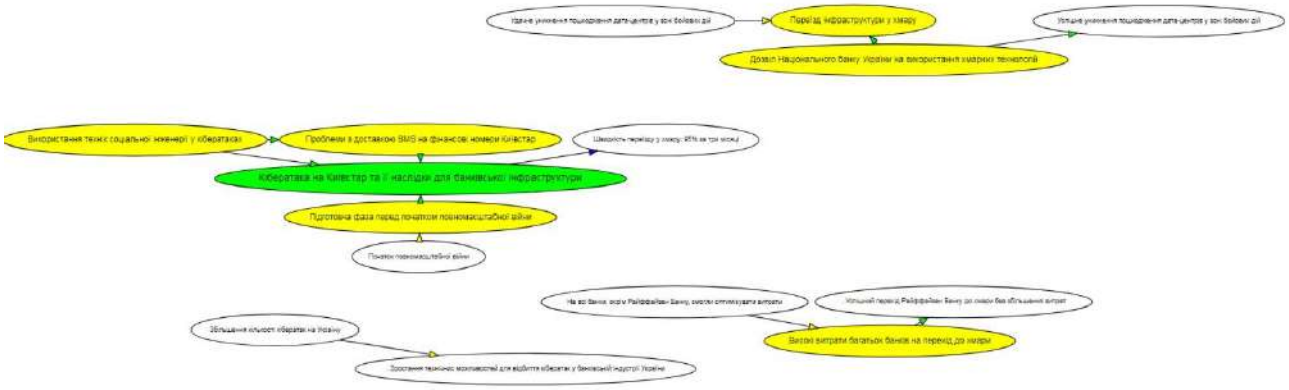

Рисунок 1 – Фрагмент графа, що відповідає мережі подій

Крім того, у цій мережі враховувались визначені раніше причинно-наслідкові зв’язки між подіями. Цю мережа також спочатку було представлено як файл у форматі CSV, після чого її було завантажено у систему Gephi (https://gephi.org). У середовищі цієї системи проведено фільтрацію створеної мережі (вилучені всі вузли із ступенем 1), а також кластеризацію за критерієм модулярності. Отриману мережа, що містить 38 вузлів і 105 зв’язків, наведено на Рис. 2, на якому кожному кластеру відповідає свій колір вузлів.

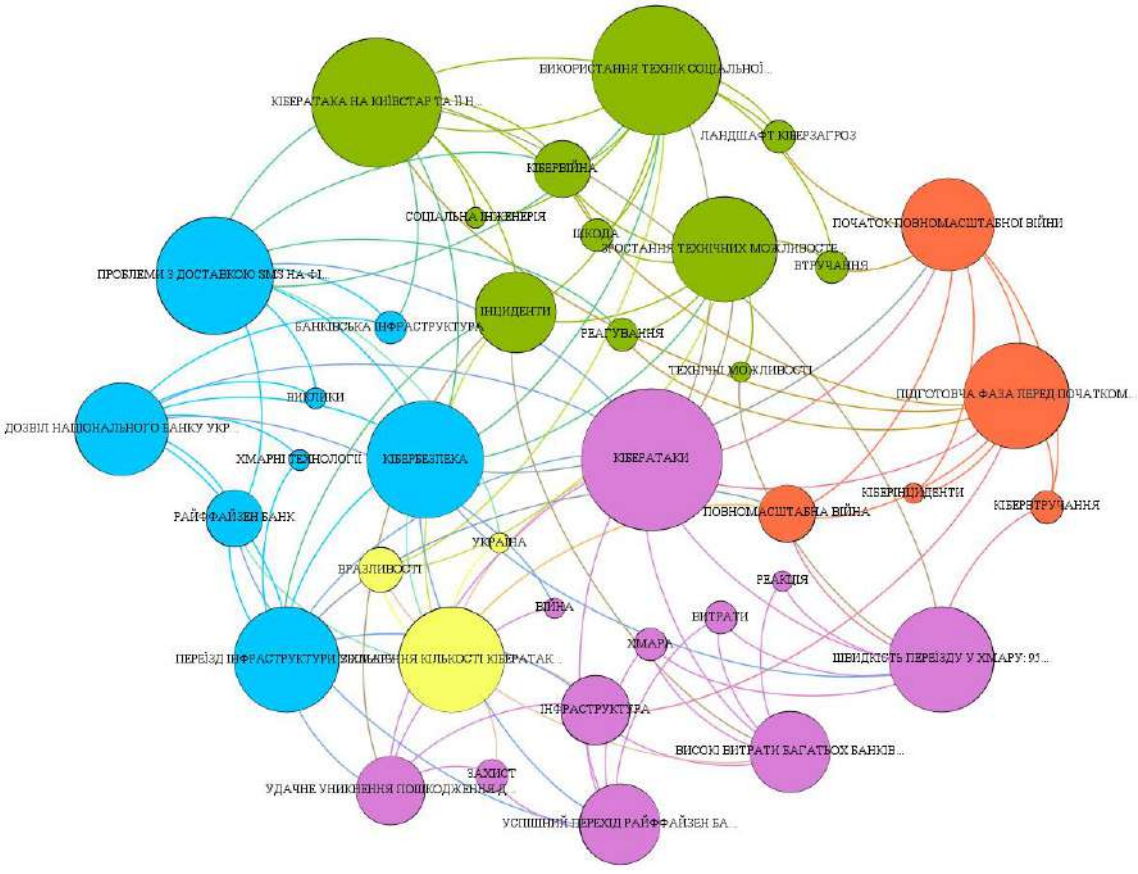

Рисунок 2 – Кластери в мережі подій у середовищі системі Gephi

Після аналізу наведених результатів кластеризації експертним шляхом вибрано п’ять подій, що відповідають визначеним кластерам, а саме:

1. Підготовча фаза перед початком повномасштабної війни.
2. Збільшення кількості кібератак на Україну.
3. Кібератака на Київстар та її наслідки для банківської інфраструктури.
4. Успішний перехід Райффайзен Банку до хмари без збільшення витрат.
5. Дозвіл Національного банку України на використання хмарних технологій.

У роботі наведено методологію побудови і кластеризації мереж подій в новинних повідомленнях на основі GenAI. Наведено приклад застосування цієї методології. Завдяки використанню генеративного штучного інтелекту отримані зручні методи екстрагування подій із текстів правової спрямованості, їх фільтрації, кластеризації. Виявлення причинно-наслідкових зв’язків також здійснюється із застосуванням GenAI, що значно спрощує роботу з природною мовою, алгоритми якої вбудовано у великі лінгвістичні моделі. На прикладі показано можливість і ефективність застосування наведеної методики для аналізу текстів, які мають пряме відношення до сфери кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Samaneh Karimi, Azadeh Shakery and Rakesh M. Verma. Enhancement of Twitter event detection using news streams. Natural Language Engineering , Volume 29 , Issue 2 , March 2023 , pp. 181 – 200. DOI: https://doi.org/10.1017/S1351324921000462 (дата звернення 20.03.2024).
2. Lande D.V., Prishchepa S.V. The automatic detection of the information operations event basis. Preprint arXiv:1807.03360. DOI: https://doi.org/10.48550/arXiv.1807.03360 (дата звернення 20.03.2024).
3. Hyejin Shin, WooChul Shim, Jiin Moon, Jae Woo Seo, Sol Lee, Yong Ho Hwang. Cybersecurity event detection with new and re-emerging words. ASIA CCS '20: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. October 2020. Pages 665–678. https://doi.org/10.1145/3320269.3384721 (дата звернення 20.03.2024).
4. Quentin Le Sceller, ElMouatez Billah Karbab, Mourad Debbabi, Farkhund Iqbal. SONAR: Automatic Detection of Cyber Security Events over the Twitter Stream. ARES '17: Proceedings of the 12th International Conference on Availability, Reliability and SecurityAugust 2017Article No.: 23. Pages 1–11. DOI: https://doi.org/10.1145/3098954.3098992 (дата звернення 20.03.2024).
5. Oleh Dmytrenko, Dmitry Lande, Oleh Andriichuk. Method for Searching of an Optimal Scenario of Impact in Cognitive Maps during Information Operations Recognition. Preprint arXiv:1904.13308 DOI: https://doi.org/10.48550/arXiv.1904.13308 (дата звернення 20.03.2024).
6. Ken Cherven. Mastering Gephi Network Visualization. Packt Publishing, 2015. – 378 p.
7. Lambert M. Surhone, Mariam T. Tennoe, Susan F. Henssonow. Graphviz. VDM Publishing, 2010. – 108 p.