DOI 10.20535/2411-1031.2023.11.2.293789
УДК 004.8

ОЛЕКСАНДР ПУЧКОВ,
ДМИТРО ЛАНДЕ,
ІГОР СУБАЧ,
ОЛЕКСАНДР РИБАК

ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ ІНФОРМАЦІЙНОГО ПОШУКУ І ШТУЧНОГО ІНТЕЛЕКТУ В ГАЛУЗІ КІБЕРБЕЗПЕКИ

У роботі розглядається можливість інтеграції традиційних систем розвідки у відкритих інформаційних джерелах (OSINT) із передовими технологіями генеративного штучного інтелекту (ГШІ), які стають ключовим фактором у розвитку аналітичних систем. Головна увага дослідження спрямована на вдосконалення функціонування системи контент-моніторингу соціальних медіа з питань кібербезпеки CyberAggregator. У роботі визначається ряд аналітичних компонентів, де застосування технології ГШІ є найбільш ефективним, серед яких засоби формування мережі ключових слів та персон, виявлення топонімів та узагальнення інформації (побудова зведень, дайджестів). Практичний аспект у дослідженні присвячено інтеграції системи контент-моніторингу з великою мовною моделлю Llama-2. Наведені кроки цієї інтеграції, описано процес взаємодії між системою пошуку інформації та Llama-2. Детально описано встановлення залежностей та відпрацювання запитів, які трансформуються в промпти для системи ГШІ. Ця інтеграція відкриває широкі можливості використання великої мовної моделі для вирішення семантичних завдань, що в свою чергу підвищує аналітичні можливості розвідувальних систем. Робота визначає перспективи використання ГШІ для подальшого розвитку та удосконалення систем аналізу інформації у відкритих джерелах, що відкриває нові можливості для розширення розуміння та ефективного використання технологій штучного інтелекту в контексті завдань та забезпечення кібернетичної і інформаційної безпеки.

Ключові слова: розвідка з відкритих джерел, система контент-моніторингу, семантичні поняття, кібербезпека, аналіз новинних документів, узагальнення масивів документів, генеративний штучний інтелект, Llama-2, CyberAggreghator.

Постановка проблеми. Забезпечення безпеки в кібернетичному просторі на сьогоднішній день є важливою та актуальною проблемою. Зростання кількості та складність кібератак породжують потребу у нових та ефективних рішеннях із захисту інформаційно-комунікаційних систем. Відтак, фахівці у галузі кібербезпеки повинні реагувати на цей виклик, шукаючи нові інноваційні підходи та технології.

Інтеграція технологій інформаційного пошуку та генеративного штучного інтелекту (ГШІ) [1], процесів моніторингу та аналізу інформації представляє собою одне з рішень цієї проблеми. Цей підхід спрямований на забезпечення ефективного виявлення та відвертання інформаційних та кіберзагроз, що може сприяти створенню більш точних інформаційних зведень для оперативного реагування на можливі загрози і атаки, розуміння їх характеру, передбачення потенційного впливу.

Аналіз останніх досліджень та публікацій. Можна виділити декілька важливих напрямків, пов'язаних з питаннями інтеграції технологій інформаційного пошуку та штучного інтелекту в галузі кібербезпеки. До напрямку виявлення та реагування на кіберзагрози можна віднести роботу, присвячену розробці системи виявлення та реагування на кіберзагрози на основі таких технологій [2]. Система, що описується, дозволяє виявляти

потенційні кіберзагрози на основі аналізу великих обсягів даних, що надходять з різних джерел, а також на основі використання алгоритмів машинного навчання. У роботі [3] пропонується методологія побудови семантичних мережевих структур. Методологія базується на використанні системи ChatGPT, великої мовної моделі, навченої на величезному наборі даних із тексту та коду та включає візуалізацію сформованих мереж за допомогою програмного забезпечення Gephi. У статті [4] описується методика формування мереж понять, пов'язаних із правовими документами і поняттями предметної галузі "Інформаційне право", що показує приклад роботи ГШІ із певною областю досліджень. Багато дослідників зараз вивчають нові технології ГШІ, щоб зрозуміти їх функціональність і обмеження. У роботі [5] наведено аналіз думок користувачів системи ChatGPT щодо кібербезпеки.

Метою роботи є обґрунтування і опис процесу інтеграції технологій інформаційного пошуку і генеративного штучного інтелекту, завдяки чому здійснюється інтелектуалізація системи контент-моніторингу новинної інформації з питань кібербезпеки.

Виклад основного матеріалу дослідження

Як базова інформаційно-пошукова система в цій роботі розглядається система контент-моніторингу соціальних медіа CyberAggreghator [6], яка була розроблена для автоматизованого аналізу та обробки інформації з питань кібербезпеки**.** Пошуковий механізм цієї системи базується на застосуванні елементів технологічного стеку Elastic [7] – ElasticSearch і Kibana, які забезпечують масштабованість та надійність при роботі з інформаційними масивами із соціальних медіа великого обсягу (Big Data) [8].

Аналітичний блок системи CyberAggreghator

Система CyberAggreghator, також надає можливість пошуку необхідної інформації за певною тематикою за визначений період часу (рис. 1). Саме цей процес дозволяє формувати масиви новинних даних для побудови семантичних карт та інформаційних портретів у конкретних змістовних областях.

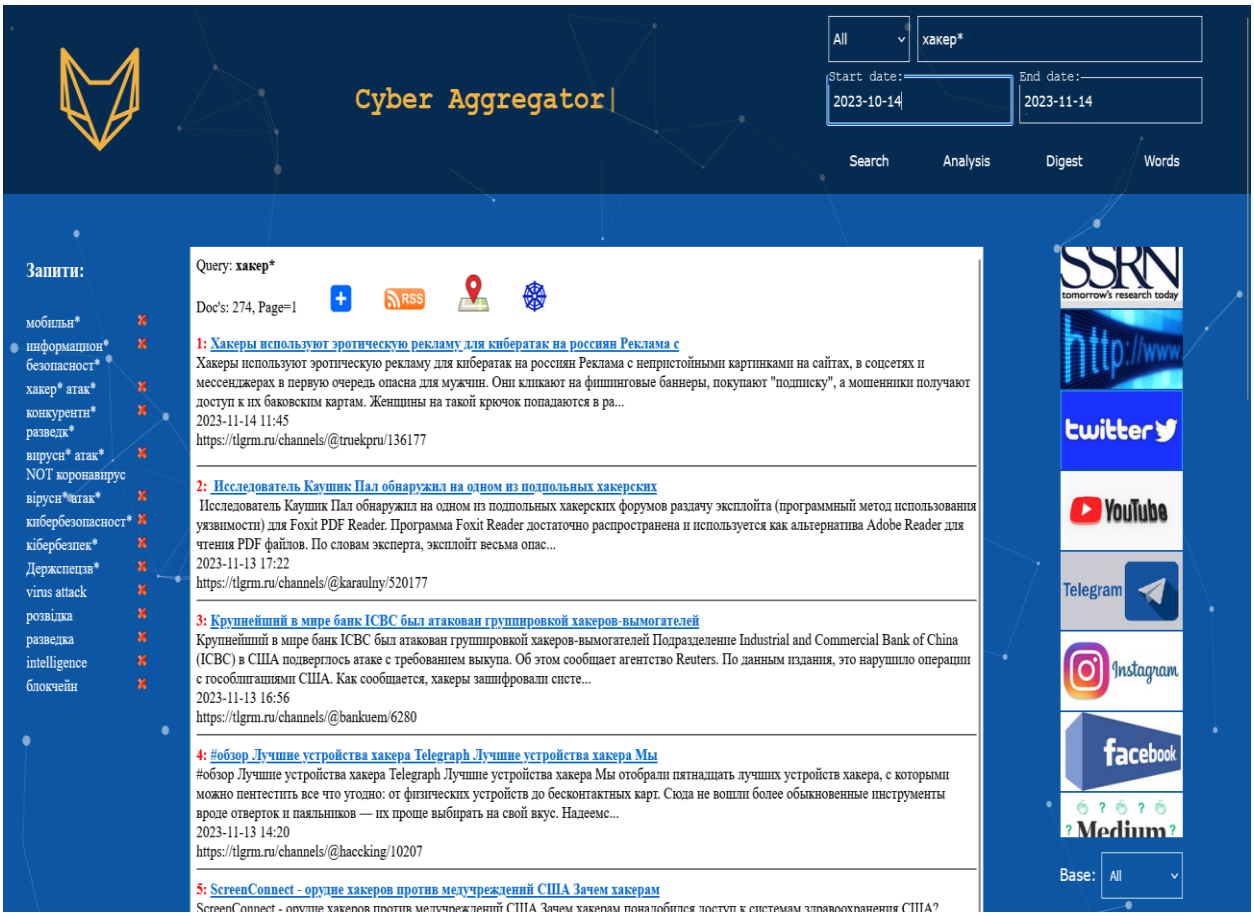

Рисунок 1 – Фрагмент пошукового інтерфейсу системи CyberAggreghator

Крім традиційних пошукових режимів, таких як пошук за ключовими словами, іншими параметрами для отримання динаміки публікацій, що відповідають запитам, за часом, маніпулювання запитами, тощо, в системі CyberAggreghator реалізовано
функціональні можливості, які відповідають так званому "аналітичному блоку", та які можуть бути удосконалені шляхом застосування технологій ГШІ, а саме:

1. Побудова дайджестів (інформаційних зведень): комбінування технологій інформаційного пошуку з генеративним штучним інтелектом при цьому дозволить автоматично аналізувати новинні статті та створювати дайджести, які надають зведену інформацію щодо подій в інформаційному просторі, які відповідають тематичному запиту.
2. Формування мереж персон і організацій: ця функція допомагає створити мережу зв'язків між різними особами або персонами на основі їх спільного згадування в соціальних медіа.
3. Формування мережі понять: ця функція дозволяє аналізувати та автоматично визначати зв'язки між поняттями, вираженими ключовими словами, що сприяє кращому розумінню контексту інформації та може бути основою для побудови семантичної мережі, навігатором у предметній галузі.
4. Виявлення топонімів (локацій): автоматичний пошук географічних та адміністративних локацій, пов'язаних із заданою тематикою.

Крім того, ГШІ може застосовуватись ще на етапі формування бази даних традиційної системи контент-моніторингу. За його допомогою може проводитись семантичне індексування первинних документів, проведення їх макроопису а саме:

1. Виявлення загальної тематичної спрямованості;
2. Додавання до документів ключових слів;
3. Переклад ключових слів різними мовами;
4. Виявлення емоційного забарвлення документів;
5. Попереднє виявлення топонімів;
6. Попереднє виявлення осіб і фірм;
7. Виявлення «прямої мови», цитат у документах;

Застосування системи ГШІ Llama-2

Для реалізації наведених аналітичних функцій запропоновано застосування системи генеративного штучного інтелекту. Для цього вирішується завдання вибору частково навченої великої мовної моделі, призначеної для розуміння та генерації тексту, що буде застосовуватись. У загальному випадку навчання такої моделі базується на великому корпусі даних, і надалі навчена модель може застосовуватися для різних задач, таких як машинний переклад, створення чат-ботів, формування творчого контенту та аналіз текстової інформації у різноманітних застосунках.

У рамках дослідження було розглянуто різні мовні моделі на основі ГШІ. Більшість з цих моделей характеризуються двома основними обмеженнями: або вони є пропрієтарними, або недостатньо розвиненими [9]. У результаті проведеного аналізу вибір був здійснений на користь моделі з відкритим вихідним кодом Llama-2 (https://llama2.ai), яка має наступні переваги:

1. Можливість аналізу та розуміння складних зв'язків між окремими словами, словосполученнями та фразами;
2. Можливість тонкого налаштування та постійного вдосконалення за рахунок додаткового навчання, розширення корпусу навчальних даних [10];
3. Система Llama-2 як сервіс доступна в Інтернеті і надає вільні можливості для перевірки виконання запитів;
4. Система Llama-2 є безкоштовною для використання у некомерційних цілях;
5. Код системи Llama-2 є відкритим і доступним на GitHub (https://github.com/dataprofessor/llama2, https://github.com/topics/llama-2, https://github.com/ggerganov/llama.cpp), що дозволяє його розширювати та вдосконалювати.

Оскільки система Llama-2 є проєктом з відкритим програмним кодом, це надає можливості для розгортання її на власному сервері та навчання/донавчання на власних даних. Такий підхід дозволяє встановлювати сервер з цією системою у внутрішній корпоративній мережі, незалежно від режиму доступу до Інтернету, що ідеально підходить для інтеграції з наявною системою CyberAggregator.

Для взаємодії з моделлю використовується проєкт “lama.cpp” (https://github.com/ggerganov/llama.cpp), що охоплює відкритий вихідний код, який можна використовувати для розробки власних застосунків, що використовують Llama -2. Також можна використовувати його для тренування власної версії системи Llama -2 на власних наборах даних. Проєкт доступний для завантаження та використання на GitHub абсолютно безкоштовно. За допомогою llama.cpp є можливості створювати промпти, зберігати їх та подавати на обробку за допомогою моделі Llama -2.

Промпти до системи ГШІ та їх опрацювання

Для подальшого деталізації наведених вище функціональних завдань мають застосовуватись спеціальні промпти для виконання конкретних змістовних запитів. Термін “промпт” [11], [12] (від англ. “prompt” – “підказка”) визначає фрагмент текстового входу, наданого моделі, який служить напрямком для формування відповіді. Промпт може представляти собою запитання, твердження чи набір інструкцій та використовується для налаштування напрямку генерації тексту моделлю. Змістовна, інструктивна частина цих промптів прикріплюється на початок масиву з новинними документами, що отримуються від системи інформаційного пошуку, служачи поясненням до того, як слід їх опрацьовувати, наприклад:

Проведи аналіз поданого тексту. Знайди ключові слова, що відповідають поняттям, та пари найбільш зв’язаних інформаційно насичених ключових слів. Кожна пара має бути наведена у форматі "слово 1; слово 2" тощо. Кожен зв’язок виводь з нового рядка.

Текст:
Стало відомо що одна з хакерських груп запустила хробака на ім'я 'LitterDrifter' , що стрімко розповсюджується світом. Він передається з заражених USB-дисків на інші USB-накопичувачі, таємно встановлюючи шкідливе програмне забезпечення, яке працює на своїх господарів…

Після отримання наведеного промпту система Llama-2 починає його опрацьовувати, виконуючі наступні кроки:

1. Токенізація**:**

– текст розбивається на токени (найменші лексичні одиниці, визначені в конкретній мовній моделі);

– текст із промпту розкладається на окремі елементи для подальшого аналізу.

2. Витяг ключових слів:

– використовуються алгоритми для визначення важливих слів у тексті;

– зазвичай, враховуються частота вживання слова, його контекст та вага в реченні, в документі.

3. Визначення семантичних взаємозв'язків:

– використовуються алгоритми обробки природної мови (NLP) для визначення семантичної близькості між словами та фразами;

– зазвичай застосовуються методи векторної репрезентації слів, які враховують контекст та семантику;

– на основі виділених ключових слів та їх семантичних зв'язків формуються пари понять, що відображають важливі аспекти тексту;

– при визначенні понять і зв'язків можуть застосовуватись відношення синонімії, антоніми, частота спільного вживання або контексту.

Для наведеного прикладу промпта, система Llama-2 дозволяє отримати такі зв’язані пари понять:

хакерські групи; 'LitterDrifter'

хробак; 'LitterDrifter'

'LitterDrifter'; USB

...

Кількість можливих зв’язків, може бути різною, це залежить від об’єму тексту та від самої мовної моделі, її налаштувань. Проте при створенні промпту, можемо обмежити їх кількість, наприклад, добавивши наступне:

Надай 20 найбільш зв’язаних пар понять.

Застосування засобів ГШІ в системі CyberAggregator

Наведені вище функціональні можливості інтегрованої інформаційно-аналітичної системи реалізовані шляхом використання промптів, що містять таки інструктивні частини:

1. Виявлення пар персон. Виконай аналіз поданого тексту. Виділи всі особи та встанови між ними взаємозв'язки у формі пар. Кожна пара осіб повинна представлятися у форматі "особа 1; особа 2". Кожен зв’язок виводь з нового рядка.
2. Виявлення пар понять. Проведи аналіз поданого тексту. Знайди ключові слова, що відповідають поняттям, та виведи пари найбільш зв’язаних інформаційно-насичених ключових слів. Кожна пара має бути наведена у форматі "слово 1; слово 2" тощо. Кожен зв’язок виводь з нового рядка.
3. Виявлення топонімів. Проведи аналіз поданого тексту. Знайди всі географічні локації та поверни їх перелік.
4. Аналіз текстів та створення інформаційних зведень, дайджестів. Проведи аналіз зазначеного списку новинних документів. Вибери 20 найважливіших новин та надай конденсовану інформацію для кожної з них.

Кроки формування мережі понять з інтегрованою системою генеративного штучного інтелекту (рис. 2) полягають у наступному:

1. **Пошук інформації (новинних документів).** Використовуючи традиційні пошукові засоби системи CyberAggregator здійснюється пошук інформації за тематичним запитом. У результаті отримується масив релевантних новинних документів.
2. **Звернення до великої мовної моделі Llama-2.** Реалізація кроку здійснюється шляхом передачі зібраної інформації до моделі у формі списку документів та виконання конкретного промпту. Автоматично опрацьований через API генеративним штучним інтелектом промпт повертається у вигляді зв’язаних пар понять, які виступають основою семантичної мережі.
3. **Візуалізація.** Використовуючи наявні засоби відображення і аналізу графових структур (GraphViz, D3.js), реалізується графічне представлення мережі понять, розраховуються мережеві показники.

Послідовне виконання цих кроків забезпечує комплексний процес функціонування системи.

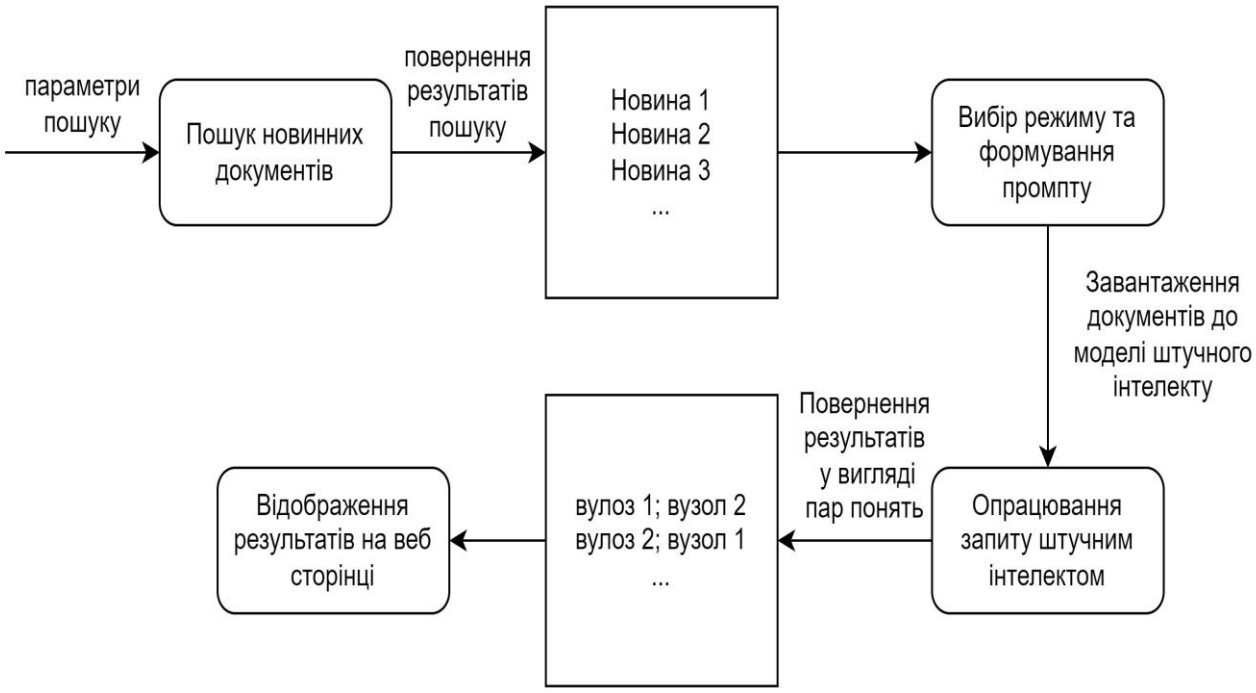

Рисунок 2 – Кроки формування мережі понять з інтегрованою системою генеративного штучного інтелекту

В інтегрованій системі кожний сервіс, що відповідає наведеним вище функціональним задачам, міститься у вкладці “Analysis” і йому відповідає окрема кнопка у системі CyberAggreghator. Відповідно

першому промпту відповідає кнопка “Persons”;

другому – кнопка “Words”;

третьому – кнопка “Geo Tags”;

четвертому – кнопка “Digest”.

Основна проблема, що завжди виникала при проведенні сценарного аналізу на основі причино-наслідкових мереж полягає саме у створенні таких мереж, що у традиційних випадках потребує великих ресурсних витрат, залучення експертів. Саме застосування систем ГШІ поєднаних із інформаційними системами типу OSINT може допомогти вирішити цю проблему. В роботі [13] наведено приклад ієрархічного формування такої мережі шляхом виконання послідовності промптів.

Аналіз створених мереж є важливим методом для розуміння взаємозв’язків між об’єктами та виявлення зв’язків між ними, що може значно полегшити дослідження конкретної сфери, зокрема, кібербезпеки. Для проведення аналізу та візуалізації мереж, спільно з системами ГШІ, можна використовувати сучасні графові інструменти, такі як Neo4j та Gephi [14]. Проте використання таких програмних продуктів стикає аналітиків з двома труднощами: необхідністю встановлення програм, що не завжди можливо, особливо при обмеженнях на встановлення стороннього програмного забезпечення, і необхідністю ретельно вивчати особливості функціонування цих систем, а також розібратися в численних параметрах, режимах розміщення графів, кластеризації тощо.

Для вирішення проблеми використовуючи бібліотеку системи GrahViz [15], створено програму CSV2Graph (рис. 3), яку можна знайти за адресою https://bigsearch.space/uli.html. Цей сервіс, розроблений на основі вказаної програми, призначений для первинного аналізу та відображення графів. Інформація надана у форматі CSV, де кожен запис представляє пару сутностей, піддається візуалізації. Програма генерує відображення орієнтованих графів, в яких вузли впорядковані за ступенем, розфарбовані, визначена товщина і напрямок ребер.

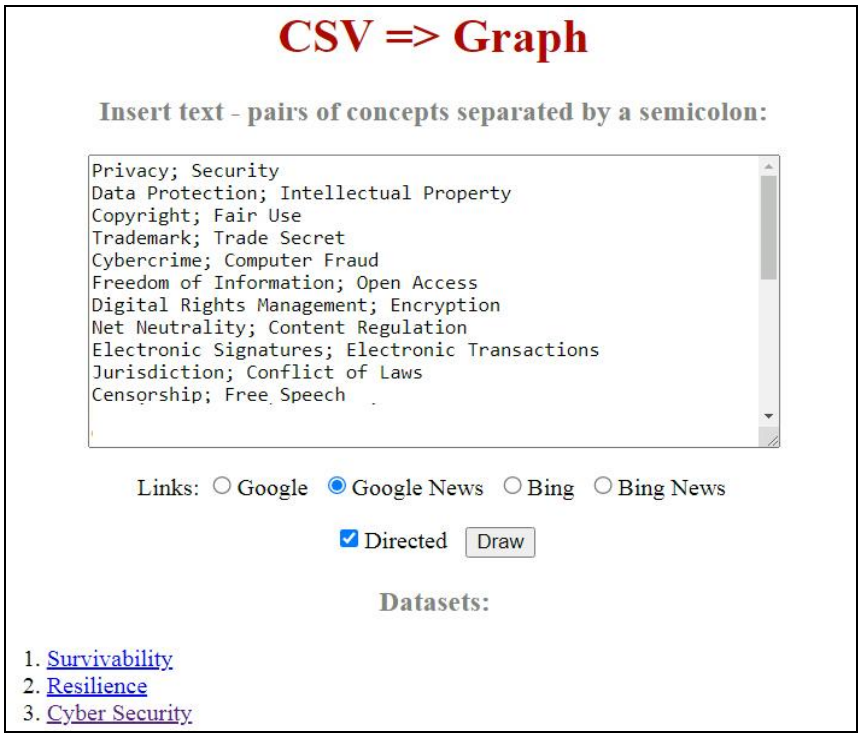

Рисунок. 3 – Інтерфейс системи CSV2Graph

На рис. 4 показано фрагмент семантичної мережі, який було сформовано на ресурсі сервісу CSV2Graph. У наведеній мережі кожний вузол і ребро виступають гіперпосиланнями на традиційну інформаційно-пошукову систему. При активізації кожного гіперпосилання здійснюється перехід на сторінку з результатами пошуку. Реалізація гіперпосилань надає користувачу можливість перегляду переліку релевантних документів, що надає розкриття вибраного поняття або зв'язку.

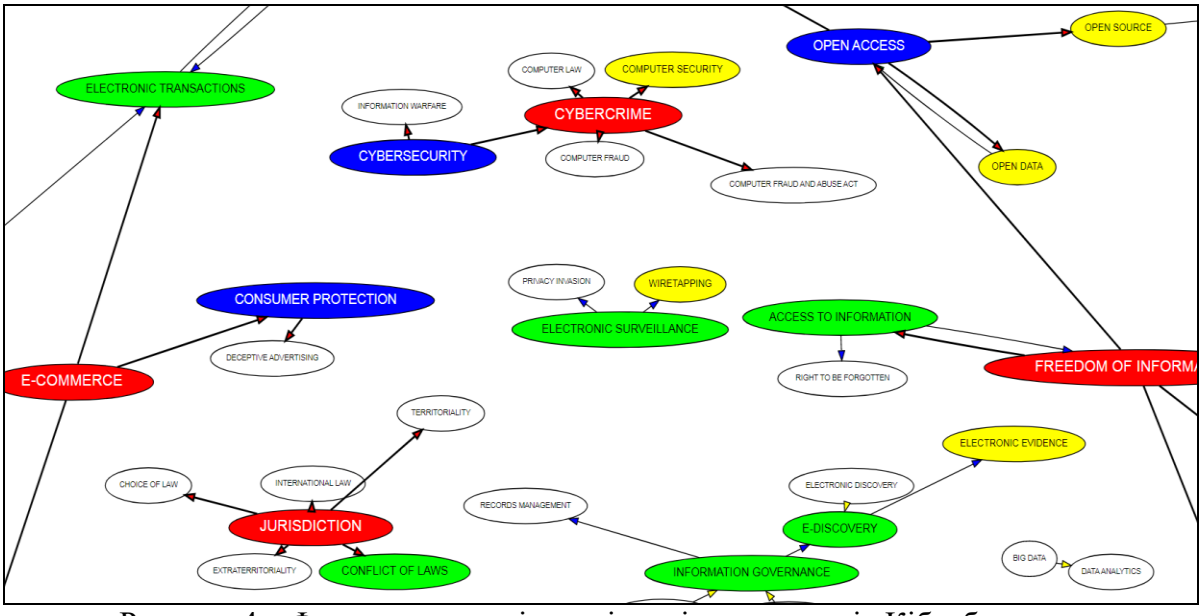

Рисунок 4 – Фрагмент мережі, що відповідає тематиці «Кібербезпека»

Висновки. Сучасний стан розвитку штучного інтелекту дозволяє виконувати за допомогою великих мовних моделей більшість аналітичних задач в системах розвідки у відкритих інформаційних джерелах. При цьому до традиційних систем OSINT додаються таки можливості систем штучного інтелекту, як автоматичний переклад, аналіз емоційного

забарвлення на основі машинного навчання, узагальнення інформації, формування зведень, дайджестів, екстрагування понять, персон, організацій, топонімів, формування семантичних, у тому числі, причинно-наслідкових (каузальних) мереж. Останнє відкриває нові можливості для побудови систем підтримки прийняття рішень шляхом формування і оцінювання важливості сценарних ланцюжків у результаті аналізу таких мереж. Всі ці можливості можуть бути реалізованими як в системах кібернетичної і інформаційній безпеки (наприклад, в системі CyberAggreghator), так і в інших важливих галузях для підтримки прийняття важливих стратегічних рішень на основі як відкритої інформації, так і інформації, що накопичується в корпоративних мережах (при встановленні корпоративного сервера для системи ГШІ).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] St. Wolfram, *What Is ChatGPT Doing ... and Why Does it Work?*, Champaign, IL, USA: Wolfram Media, Inc., 2023.

[2] N. Kumar, A. Sen, V. Hordiichuk, M. Jaramillo, B. Molodetskyi, and A. Kasture, "AI in Cybersecurity: Threat Detection and Response with Machine Learning", *Tuijin Jishu / Journal of Propulsion Technology*, vol. 44, no. 3, pp. 38-46, 2023. doi: https://doi.org/10.52783/tjjpt.v44.i3.237.

[3] D. Lande, and L. Strashnoy, "Concept Networking Methods Based on ChatGPT & Gephi", *SSRN Preprint (April 17, 2023)*. 12 p. doi: https://doi.org/10.2139/ssrn.4420452.

[4] Д. Ланде, та Л. Страшной, "Формування мереж понять в галузі права за допомогою системи штучного інтелекту", *Інформація і право*, № 2 (45), с. 88-93, 2023. doi: https://doi.org/10.37750/2616-6798.2023.2(45).282326.

[5] O. D. Okey, E. U. Udo, R. L. Rosa, D. Z. Rodríguez, and J. H. Kleinschmidt, "Investigating ChatGPT and cybersecurity: A perspective on topic modeling and sentiment analysis", *Computers & Security*, vol. 135, art. 103476, 2023. doi: https://doi.org/10.1016/j.cose.2023.103476.

[6] Д. Ланде, О. Пучков, та І. Субач, "Система аналізу великих обсягів даних з питань кібербезпеки із соціальних медіа", *Information Technology and Security*, vol 8, iss. 1 (14), pp. 4-18, 2020. doi: https://doi.org/10.20535/2411-1031.2020.8.1.217993.

[7] S. Pranav, and K. M. N. Sharath, *Learning Elastic Stack 7.0: Distributed search, analytics, and visualization using Elasticsearch, Logstash, Beats, and Kibana, 2nd Edition*, Birmigham, UK: Packt Publishing, 2019.

[8] Д. В. Ланде, І. Ю. Субач, та А. Я. Гладун, *Оброблення надвеликих масивів даних (Big Data): навчальний посібник*, Київ, Україна, 2021. [Електронний ресурс]. Доступно: https://ela.kpi.ua/handle/123456789/46129.

[9] H. Touvron et al., "Llama 2: Open Foundation and Fine-Tuned Chat Models", *ArXiV Preprint arXiv:2307.09288*, 2023. doi: https://doi.org/10.48550/arXiv.2307.09288.

[10] Z. Zhao, Z. Zhang, and F. Hopfgartner, "A Comparative Study of Using Pre-trained Language Models for Toxic Comment Classification", in *Proc. WWW '21: The Web Conference 2021*, pp. 500-507, April 2021. doi: https://doi.org/10.1145/3442442.3452313.

[11] "Prompt engineering", *OpenAI*. [Online]. Available: https://platform.openai.com/docs/guides/prompt-engineering. Accessed on: June 18, 2023.

[12] "Best practices for prompt engineering with OpenAI API", *OpenAI*. [Online]. Available: https://help.openai.com/en/articles/6654000-best-practices-for-prompt-engineering-with-openai-api. Accessed on: June 20, 2023.

[13] Д. Ланде, Л. Страшной, О. Дрямов, та А. Фегер, "Формування сценаріїв діяльності на базі сервісів генеративного штучного інтелекту", *Штучний інтелект*, № 97 (3), с. 94-103, 2023. doi: https://doi.org/10.15407/jai2022.01.08..

[14] K. Cherven, *Mastering Gephi Network Visualization*, Birmigham, UK: Packt Publishing, 2015.

[15] T. Triantoro, “Graph Viz: Exploring, Analyzing, and Visualizing Graphs and Networks with Gephi and ChatGPT”, *ODSC Community*, 2023. [Online]. Available: https://opendatascience.com/graph-viz-exploring-analyzing-and-visualizing-graphs-and-networks-with-gephi-and-chatgpt. Accessed on: June 20, 2023.

Стаття надійшла 23.10.2023.

REFERENCE

[1] St. Wolfram, *What Is ChatGPT Doing ... and Why Does it Work?*, Champaign, IL, USA: Wolfram Media, Inc., 2023.

[2] N. Kumar, A. Sen, V. Hordiichuk, M. Jaramillo, B. Molodetskyi, and A. Kasture, “AI in Cybersecurity: Threat Detection and Response with Machine Learning”, *Tuijin Jishu / Journal of Propulsion Technology*, vol. 44, no. 3, pp. 38-46, 2023. doi: https://doi.org/10.52783/tjjpt.v44.i3.237.

[3] D. Lande, and L. Strashnoy, “Concept Networking Methods Based on ChatGPT & Gephi”, *SSRN Preprint (April 17, 2023)*. 12 p. doi: https://doi.org/10.2139/ssrn.4420452.

[4] D. Lande, and L. Strashnoy, “Formation of networks of concepts in the field of law with the help of an artificial intelligence system”, *Information and law*, no. 2 (45), pp. 88-93, 2023. doi: https://doi.org/10.37750/2616-6798.2023.2(45).282326.

[5] O. D. Okey, E. U. Udo, R. L. Rosa, D. Z. Rodríguez, and J. H. Kleinschmidt, “Investigating ChatGPT and cybersecurity: A perspective on topic modeling and sentiment analysis”, *Computers & Security*, vol. 135, art. 103476, 2023. doi: https://doi.org/10.1016/j.cose.2023.103476.

[6] D. Lande, O. Puchkov, and I. Subach, “System for analysing of big data on cybersecurity issues from social media”, *Information Technology and Security*, vol 8, iss. 1 (14), pp. 4-18, 2020. doi: https://doi.org/10.20535/2411-1031.2020.8.1.217993.

[7] S. Pranav, and K. M. N. Sharath, *Learning Elastic Stack 7.0: Distributed search, analytics, and visualization using Elasticsearch, Logstash, Beats, and Kibana, 2nd Edition*, Birmigham, UK: Packt Publishing, 2019.

[8] D. Lande, I. Subach, and A. Gladun, *Processing of extremely large data sets (Big Data): a tutorial*, Kyiv, Ukraine, 2021. [Online]. Available: https://ela.kpi.ua/handle/123456789/46129.

[9] H. Touvron et al., “Llama 2: Open Foundation and Fine-Tuned Chat Models”, *ArXiV Preprint arXiv:2307.09288*, 2023. doi: https://doi.org/10.48550/arXiv.2307.09288.

[10] Z. Zhao, Z. Zhang, and F. Hopfgartner, “A Comparative Study of Using Pre-trained Language Models for Toxic Comment Classification”, in *Proc. WWW '21: The Web Conference 2021*, pp. 500-507, April 2021. doi: https://doi.org/10.1145/3442442.3452313.

[11] “Prompt engineering”, *OpenAI*. [Online]. Available: https://platform.openai.com/docs/guides/prompt-engineering. Accessed on: June 18, 2023.

[12] “Best practices for prompt engineering with OpenAI API”, *OpenAI*. [Online]. Available: https://help.openai.com/en/articles/6654000-best-practices-for-prompt-engineering-with-openai-api. Accessed on: June 20, 2023.

[13] D. Lande, and L. Strashnoy, O. Driamov, and A. Feger, “Formation of activity scenarios based on generative artificial intelligence services”, *Artificial Intelligence*, no. 97 (3), pp. 94-103, 2023. doi: https://doi.org/10.15407/jai2022.01.08..

[14] K. Cherven, *Mastering Gephi Network Visualization*, Birmigham, UK: Packt Publishing, 2015.

[15] T. Triantoro, “Graph Viz: Exploring, Analyzing, and Visualizing Graphs and Networks with Gephi and ChatGPT”, *ODSC Community*, 2023. [Online]. Available: https://opendatascience.com/graph-viz-exploring-analyzing-and-visualizing-graphs-and-networks-with-gephi-and-chatgpt. Accessed on: June 20, 2023.

OLEKSANDR PUCHKOV,
DMYTRO LANDE,
IHOR SUBACH,
OLEKSANDR RYBAK

INTEGRATION OF INFORMATION SEARCH TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE IN THE FIELD OF CYBERSECURITY

The paper explores the possibility of integrating traditional intelligence systems in open-source intelligence (OSINT) with advanced generative artificial intelligence (GAI) technologies, which are becoming a key factor in the development of analytical systems. The main focus of the research is on improving the functionality of the social media content monitoring system for cybersecurity issues, called CyberAggregator. The study identifies several analytical components where the application of GAI technology is most effective, including the creation of networks of key words and persons, identification of toponyms, and information summarization (building summaries, digests). The practical aspect of the research is dedicated to integrating the content monitoring system with the large language model Llama-2. The steps of this integration are provided, and the interaction process between the information search system and Llama-2 is described. The installation of dependencies and processing of queries transformed into prompts for the GAI system are detailed. This integration opens up broad possibilities for utilizing the large language model to address semantic tasks, thereby enhancing the analytical capabilities of intelligence systems. The paper identifies perspectives for using GAI to further develop and enhance information analysis systems in open sources, providing new opportunities to expand the understanding and effective use of artificial intelligence technologies in the context of tasks and ensuring cyber and information security.

Keywords: open-source intelligence, content monitoring system, semantic concepts, cybersecurity, analysis of news documents, summarization of document arrays, generative artificial intelligence, Llama-2, CyberAggregator.

Пучков Олександр Олександрович, кандидат філософських наук, професор, начальник, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-8585-1044, iszzi@iszzi.kpi.ua.

Ланде Дмитро Володимирович, доктор технічних наук, професор, завідувач кафедри, Навчально-науковий фізико-технічний інститут Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0003-3945-1178, dwlande@gmail.com.

Субач Ігор Юрійович, доктор технічних наук, професор, завідувач кафедри, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-9344-713X, igor_subach@ukr.net.

Рибак Олександр Олегович, аспірант**,** Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0009-0004-1033-1599, rybak.oleksandr01@gmail.com.

Puchkov Oleksandr, PhD in philosophy, professor, head of the Institute of special communication and information protection at the National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Lande Dmytro, doctor of technical sciences, professor, chair of the department, Educational and scientific physico-technical institute at the National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Subach Ihor, doctor of technical sciences, professor, chair of the department, Institute of special communication and information protection at the National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Rybak Oleksandr, postgraduate student, Institute of special communication and information protection at the National technical university of Ukraine "gor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.