

*Приурочено до 125-ї річниці створення
Національного технічного університету України
“Київський політехнічний інститут імені Ігоря Сікорського”*

МАТЕРІАЛИ
VI науково-практичної конференції курсантів (студентів),
аспірантів, докторантів та молодих учених
“АКТУАЛЬНІ ПИТАННЯ
ЗАСТОСУВАННЯ СПЕЦІАЛЬНИХ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ”

23 листопада 2023 року

Київ – 2023

Матеріали VI науково-практичної конференції курсантів (студентів), аспірантів, докторантів та молодих учених “Актуальні питання застосування спеціальних інформаційно-комунікаційних систем”. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2023. 394 с.

У матеріалах VI науково-практичної конференції курсантів (студентів), аспірантів, докторантів та молодих учених “Актуальні питання застосування спеціальних інформаційно-комунікаційних систем” опубліковано тези доповідей, в яких висвітлюються питання дослідження, аналізу й узагальнення нових теоретичних і практичних результатів у сферах кібербезпеки та кіберзахисту, інформаційної безпеки держави, інформаційних технологій та електронних комунікацій, а також залучення здобувачів вищої освіти до активної наукової діяльності.

РЕЦЕНЗЕНТИ:

Олександр ПУЧКОВ	К.філос.н., професор
Сергій КОНЮШОК	К.т.н., доцент
Владислав ГОЛЬ	К.т.н., професор
Вадим РОМАНЕНКО	К.т.н., доцент
Дмитро МОГИЛЕВИЧ	Д.т.н., професор
Ігор СУБАЧ	Д.т.н., доцент
Ярослав ЗІНЧЕНКО	К.т.н., с.н.с.

Рекомендовано до друку Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського (протокол № 4 від 22.11.2023).

Секція № 4 “Актуальні питання забезпечення кібербезпеки”

Олександр РИБАК; Олександр ПУЧКОВ; Дмитро ЛАНДЕ Поєднання технологій пошуку інформації та штучного інтелекту у сфері кібербезпеки.....	311
Іван ГОРНІЙЧУК; Ігор ПИСКУН Інформаційна технологія автентифікації користувачів за їх рукописним підписом.....	313
Володимир ОНИЩЕНКО; Микола ХОМІК Аналіз вразливостей вихідного коду репозиторія на основі моделей нейронних мереж.....	315
Олександр ВЛАСЕНКО; Ігор СУБАЧ Функціональне моделювання SIEM-системи для кіберзахисту баз даних.....	316
Віра ГИРДА; Дмитро ЛАНДЕ Визначення фейків за допомогою ChatGPT.....	318
Анатолій ГЛАДУН; Катерина ХАЛА Методи та моделі побудови роїв БПЛА на основі онтологічних технологій.....	319
Борис ГОРЛИНСЬКИЙ; Віктор ГОРЛИНСЬКИЙ Національний вимір кіберпростору як передумова формування системи кібербезпеки.....	321
Артем ЖИЛІН; Ольга ШЕВЧУК Напрями посилення захисту програмного забезпечення.....	323
Роман ЗАЙЦЕВ; Ольга ШЕВЧУК Модель інтеграції розвідки кіберзагроз у системах реагування на кіберінциденти в Україні.....	324
Андрій МАКСИМЕЦЬ; Юлія КОЖЕДУБ Концептуальний вплив штучного інтелекту для систем підтримки прийняття рішень на кібербезпеку.....	325
Сергій МІТІН; Сергій ОБРАШКО Система виявлення інформаційних атак у соціальних мережах.....	327
Кирило МУЖЕСЬКИЙ; Андрій КАРПЕНКО; Василь ВОЛОШИН Системний аналіз протоколу квантового цифрового підпису.....	328
Святослав ПАРШУКОВ Сучасні системи збірки та їх роль в процесі створення складних програмних проєктів.....	329
Артем СОБОЛЄВ; Дмитро ЛАНДЕ Інтегрований підхід добування інформації із соціальних мереж.....	330

Олександр РИБАК;
Олександр ПУЧКОВ, к.філос.н., професор
Дмитро ЛАНДЕ, д.т.н., професор

ПОЄДНАННЯ ТЕХНОЛОГІЙ ПОШУКУ ІНФОРМАЦІЇ ТА ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ КІБЕРБЕЗПЕКИ

Анотація. У цій роботі розглядається поєднання можливостей системи контент-моніторингу соціальних медіа cyberaggregator з можливостями генеративного штучного інтелекту задля покращення автоматичної побудови дайджестів, створення мережі персон та мережі слів.

Summary. This work explores the combination of the capabilities of the social media content monitoring system cyberaggregator with those of generative artificial intelligence to enhance the automatic generation of digests, the creation of personal networks, and the networks of words.

Ключові слова: кібербезпека, технології пошуку інформації, штучний інтелект, аналіз даних, cyberaggregator.

У сучасному світі кібербезпека стає все більш важливою сферою, оскільки кіберзагрози стають все складнішими та небезпечнішими. В цей же час, невинно розвивається штучний інтелект, який можливо використовувати для боротьби з загрозами в інформаційному просторі. Також, важливим ресурсом для виявлення та захисту від цих загроз, а також при роботі зі штучним інтелектом є інформація, якої вдалося отримати у відкритих джерелах.

У даній роботі розглядається поєднання можливостей системи контент-моніторингу соціальних медіа cyberaggregator (рис. 1) з функціоналом генеративного штучного інтелекту. Cyberaggregator включає різні режими роботи, такі як пошук та виведення окремих документів, отримання та аналіз динаміки інформації. Можливий пошук за конкретною тематикою та періодом входження документів.

Поєднання цієї системи з можливостями штучного інтелекту спрямоване на покращення таких аспектів роботи:

1. Побудова дайджестів: комбінування технології пошуку з генеративним інтелектом дозволяє автоматично аналізувати новинні статті та створювати дайджести, які надають зведену інформацію про події в інформаційному просторі.

2. Формування мережі персон: ця інтеграція допомагає створити мережу зв'язків між різними особами на основі їхньої активності в соціальних медіа та інших джерелах інформації.

3.Формування мережі слів: Інтеграція дозволяє автоматично аналізувати та визначати зв'язки між ключовими термінами та словами, що сприяє кращому розумінню контексту інформації.

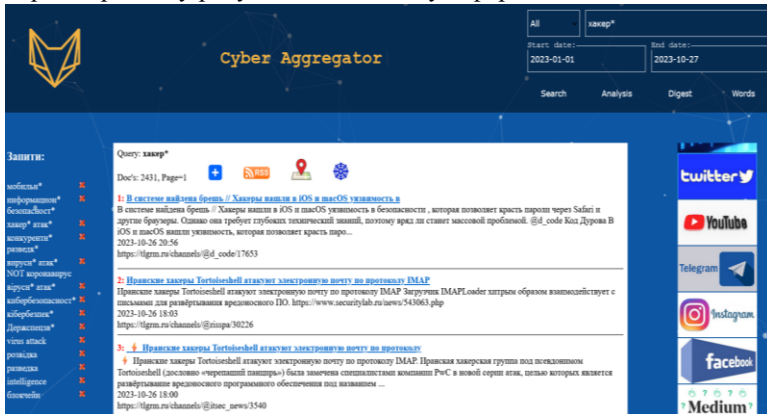


Рисунок 1. Система контент-моніторингу соціальних медіа cyberagggregator

Пошуковий режим системи cyberagggregator базується на сучасній системі elasticsearch, що надає розподілений, багатоклієнтський повнотекстовий пошуковий рушій. Інтелектуальний режим використовує можливості генеративного штучного інтелекту, а саме моделі Llama-2, створеної командою a vesocoder з Великобританії.

Llama-2 є великою мовною моделлю (LLM), яка має декілька переваг:

- 1.Розуміння складних зв'язків: Вона може аналізувати та розуміти складні зв'язки між словами та фразами.
- 2.Навчання на великому наборі даних: Модель може вдосконалюватися за рахунок великої кількості даних.
- 3.Безкоштовне використання: Llama-2 є безкоштовною для використання.
- 4.Відкритий код: Код Llama-2 доступний на github, що робить його доступним для розширення та покращення.

Висновки. Інтеграція cyberagggregator та Llama-2 надає можливості для автоматичного аналізу новинних статей, створення дайджестів та побудови мереж персон та слів. Ця інтеграція відіграє важливу роль у підвищенні рівня кібербезпеки та поліпшенні розуміння інформаційного простору.