НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ НАН УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА БЕЗПЕКА

МАТЕРІАЛИ XXIII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ВИПУСК 23

Київ – 2023

Рекомендовано до друку Вченою радою
Інституту проблем реєстрації інформації НАН України
(протокол № 11 від 26 грудня 2023 р.)

Інформаційні технології та безпека. Матеріали XXIII Міжнародної науково-практичної конференції ІТБ-2023. – Київ: Інжиніринг. – 202 с. ISBN: 978-966-2344-96-7

До збірника увійшли матеріали доповідей, представлених на XXIII Міжнародній науково-практичній конференції «Інформаційні технології та безпека» (ІТБ-2023, 30 листопада 2023 року, м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням створення і впровадження інформаційних технологій, актуальним проблемам забезпечення інформаційної та кібербезпеки, протидії інформаційним операціям і кібертероризму, інтелектуальним технологіям підтримки прийняття рішень, проведенню аналітичних досліджень на основі сучасних методів інтелектуального аналізу даних.

Для фахівців в області інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.

ISBN 978-966-2344-96-7

ЗМІСТ

інтересам. Розглянуті підходи до виявлення потенційних ризиків та вжиття проактивних заходів для пом’якшення цих ризиків.

Подальші дослідження передбачають розробку механізмів управління ризиками пов'язаними з розвитком і використанням штучного інтелекту.

Перелік посилань:

1. Artificial Intelligence and National Security, Bipartisan Policy Center and Georgetown University’s Center for Security and Emerging Technology (2020).
2. Brundage Miles, Avin Shahar, Clark Jack et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation (2018). Homepage, https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf, last accessed 2023/06/21.
3. China’s Rise In Artificial Intelligence And Future Military Capabilities. Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power, Nov. 1, pp. 8-32 (2017).
4. Amina Iqbal. China’s AI Military Revolution and its Security Implications (2023), Homepage, https://internationalaffairsbd.com/chinas-ai-military-revolution/, last accessed 2023/09/16.
5. Elsa B. Kania. “AI Weapons” In China's Military Innovation (2020). Homepage, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania.pdf.

ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ У СФЕРІ КІБЕРБЕЗПЕКИ: ІНФОРМАЦІЙНИЙ ПОШУК ТА ШТУЧНМЙ ІНТЕЛЕКТ

Олександр Пучков [1], Дмитро Ланде [1,2], Олександр Рибак

[1] Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна

[2] Інститут проблем реєстрації інформації НАН України, Київ, Україна

У цій роботі розглядається поєднання можливостей системи контент-моніторингу соціальних медіа CyberAggregator і системи генеративного штучного

інтелекту з метою покращення аналітичних можливостей корпоративної OSINT з проблем кібербезпеки, а саме засобів автоматичного формування зведенб (дайджестів), створення мереж понять (персон, термінів, об'єктів кібербезпеки).
Ключові слова: OSINT, генеративний штучний інтелект, інформаційний пошук, CyberAggregator, мережа понять, кібербезпека.

У сучасному світі кібербезпека стає все більш важливою сферою – кіберзагрози стають все складнішими та небезпечнішими. Для моніторингу стану кібербезпеки серед інших засобів застосовуються засоби розвідки у відкритих джерелах (Open Source INTelligence, OSINT) [1]. У той же час, невпинно розвивається штучний інтелект, який можливо використовувати для боротьби з загрозами в інформаційному просторі. Одним із шляхів застосування штучного інтелекту у сфері кібербезпеки є інтелектуалізація роботи із інформацією OSINT, узагальнення інформації з відкритих джерел.

Тому є актуальним завданням поєднання можливостей системи контент-моніторингу соціальних медіа з питань кібербезпеки CyberAggregator [1] з функціоналом генеративного штучного інтелекту [2]. CyberAggregator включає різні режими роботи, такі як пошук за конкретною тематикою та періодом входження документів та виведення окремих документів, отримання та аналіз динаміки інформації.

Поєднання цієї системи з можливостями utythfnbdyjuj штучного інтелекту (система Llama) спрямоване на покращення таких аспектів аналітичних режимів роботи системи, а саме формування:

1. Інформаційних зведень (дайджестів): комбінація технології пошуку з генеративним штучним інтелектом дозволяє автоматично аналізувати новинні повідомлення та створювати узагальнення, які надають зведену інформацію про події в інформаційному просторі.
2. Мережі персон, що враховує зв'язки між різними особами на основі їхньої активності в соціальних медіа та згадувань в інших джерелах інформації.
3. Мережі хакерських угрупувань, яка візуалізує зв'язки між окремими угрупуваннями, виявляє їх причетність до

кібератак, відношення до силових відомств окремих держав, тощо.

4. Мережі термінів, яка дозволяє автоматично аналізувати та визначати зв'язки між ключовими термінами, що сприяє кращому розумінню контексту інформації.

Пошуковий режим системи CyberAggregator базується на сучасній системі ElasticSearch [3]. Інтелектуальний режим використовує можливості генеративного штучного інтелекту, а саме моделі LLama-2 [4].

LLama-2 є великою мовною моделлю, 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.

Інтеграція CyberAggregator та LLama-2 надає можливості для автоматичного аналізу новинних статей, створення дайджестів та побудови мереж персон та слів. Всі ці можливості Ця інтеграція грає важливу роль в підвищенні рівня кібербезпеки та забезпеченні кращого розуміння інформаційного простору.

Висновки

Інтеграція CyberAggregator та LLama-2 надає можливості для автоматичного аналізу новинних повідомлень, створення дайджестів та побудови мереж персон та слів. Це поєднання сприяє підвищенню аналітичних можливостей системи, використанню наявних ресурсів інформаційного простору.

Перелік посилань

5. Dmytro Lande, Olexander Puchkov, Ihor Subach Method of Detecting Cybersecurity Objects Based on OSINT Technology. Selected Papers of the XXII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2022) — Vol-3503. — pp. 115-124.
6. Dmytro Lande, Leonard Strashnoy. GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now — Kyiv: Engineering, 2023. — 168 p. ISBN 978-966-2344-94-3

7. Pranav Shukla, Sharath Kumar M N. Learning Elastic Stack 7.0. Distributed Search, Analytics, and Visualization Using Elasticsearch, Logstash, Beats, and Kibana, 2nd Edition. Packt Publishing, 2019. ISBN 9781789958539, 1789958539. — 474 p.
8. Smith N. A., Hajishirzi H. Self-Instruct: Aligning Language Model with Self Generated Instructions // ArXiv.org — 2022. — arXiv:2212.10560

СТРУКТУРНА СКЛАДНІСТЬ КОМПЛЕКСНИХ ГРАФІВ

А. Снарський[1,2]
[1]Інститут реєстрації інформації НАН України, 03113, Київ, Україна
[2]Національний технічний університет «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна

Введено кількісну міру структурної складності графа (складна мережа тощо), засновану на процедурі, подібній до процесу перенормування, враховуючи різницю між фактичною та усередненою структурами графа в різних масштабах. Запропонована концепція структурної складності графа відповідає якісному розумінню складності. Запропоновану міру можна також отримати для зважених графіків.

Було виявлено структурні складності для різних типів графів – детермінованих графів нескінченного розміру та графів кінцевого розміру, штучних графів різної природи, включаючи перколяційні структури, і часових рядів серцевих ритмів, відображених у складні мережі за допомогою алгоритму параметричного графа видимості. Останні досягають максимуму поблизу формування гігантської компоненти на графіку або на порозі перколяції для 2D і 3D квадратних ґраток, коли виникає гігантський кластер, що має фрактальну структуру. Отже, структурна складність графів дозволяє виявити та дослідити процеси, подібні до фазових переходів другого роду в складних мережах.

Новий індекс центральності вузла, що характеризує структурну складність певного вузла в структурі графа, також може бути введений, що може служити хорошим допоміжним або узагальненням для локального коефіцієнта кластеризації.