Школьніков Владислав Ігорович,
завідувач кафедри кримінології
та інформаційних технологій
Національної академії внутрішніх справ,
доктор філософії в галузі права, доцент;
Гуськова Віра Геннадіївна,
доцент кафедри штучного інтелекту
Інституту прикладного системного
аналізу Національного технічного
університету України «КПІ ім. Ігоря
Сікорського», доктор філософії в галузі
комп'ютерних наук, доцент

ВИКОРИСТАННЯ RAG (RETRIEVAL-AUGMENTED GENERATION) ПІД ЧАС ЗДІЙСНЕННЯ КРИМІНАЛЬНОГО АНАЛІЗУ

На сучасному етапі розвитку кримінального аналізу опрацювання великих обсягів даних із різноманітних джерел (матеріалів кримінальних проваджень, оперативно-розшукових справ, відомостей із державних реєстрів та відкритих джерел тощо) є повсякденною роботою працівників правоохоронних органів України. Обробка та аналіз даних із різною структурою та форматами потребують значного часового ресурсу для виявлення прихованих зв'язків між особами, подіями та фактами. Тому використання можливостей штучного інтелекту дозволяє автоматизувати рутинні процеси, обробляти дані за лічені секунди, розпізнавати небезпечні тенденції та автоматизувати обробку великих обсягів даних.

Одним із перспективних способів розв'язання цієї проблеми є використання технології Retrieval-Augmented Generation (RAG) [1]. На відміну від звичайної генеративної моделі, яка формує відповідь переважно на основі знань, отриманих під час навчання, RAG спочатку знаходить релевантні фрагменти у зовнішніх джерел інформації, а потім використовує їх для отримання відповіді від великої мовної моделі (LLM).

Класична RAG-система складається з доступу до зовнішньої бази даних, векторної бази даних, інструментів обробки та пошуку релевантної інформації, великої мовної моделі. Спочатку дані, які потрапляють в RAG-системи повинні бути нормалізовані та розділені на відносно невеликі фрагменти

(так звані chunks). Для кожного chunk створюється числове векторне представлення, яке відображає його зміст. Після отримання запиту система знаходить семантично близькі chunks, передає їх великій мовній моделі як контекст і формує відповідь. Під час здійснення кримінального аналізу принципово важливо, щоб відповідь містила посилання на документи, сторінки або конкретні фрагменти, з яких було отримано відповідні відомості.

RAG-системи можуть опрацювати як структуровані, так і неструктуровані дані, до яких можна віднести оцифровані протоколи проведення слідчих та негласних слідчих (розшукових) дій, висновки експертів, аналітичні довідки, відомості з відкритих джерел та дані отримані за результатами тимчасового доступу до речей і документів тощо. Окремим перспективним напрямом використання RAG-систем під час здійснення кримінального аналізу є опрацювання великих обсягів інформації з відкритих джерел.

З урахуванням вищезазначеного, RAG-системи можуть знаходити спільні та відмінні ознаки між даними, виявляти закономірності та групувати інформацію за тематичними ознаками.

Перспективним напрямком є поєднання RAG із графовим аналізом (Graph RAG). Поєднання класичного RAG із графами знань (Knowledge Graphs) усуває ключові недоліки стандартного пошуку, дозволяючи штучному інтелекту бачити приховані зв'язки між документами та розуміти контекст на рівні цілісної мережі даних.

Застосування RAG пов'язане з низкою ризиків. Велика мовна модель може неправильно інтерпретувати знайдений фрагмент, сформувати твердження, якого немає у джерелах. Передавання інформації зовнішнім хмарним сервісам може створювати ризик розголошення даних оперативно-розшукової діяльності та досудового розслідування. Документи з ненадійних джерел можуть містити приховані шкідливі інструкції для великої мовної моделі (атаки типу prompt injection) [2]. Крім того, відповідь від RAG-системи не може розглядатися як допустимий доказ. Такі системи є допоміжним аналітичним інструментом, а наведені факти мають перевірятися з оригінальними матеріалами.

Безпечне впровадження RAG-систем потребує комплексу технічних та організаційних заходів [3]. Доцільно використовувати локальне або контрольоване середовище, шифрування даних, рольове розмежування доступу, багатофакторну автентифікацію та

журналювання дій. Система повинна зберігати текст запиту, перелік використаних документів, версії моделей і параметри пошуку.

RAG має потенціал для використання під час здійснення кримінального аналізу. Дана технологія може прискорити пошук, систематизацію, порівняння та узагальнення даних, допомогти у побудові хронологій та виявленні зв'язків. Водночас RAG-системи мають використовуватися як допоміжний інструмент для прийняття працівникам правоохоронних органів України обґрунтованих управлінських рішень.

Список використаних джерел

1. Lewis P., Perez E., Piktus A. et al. Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks. *Advances in Neural Information Processing Systems.* 2020. Vol. 33. P. 9459–9474. URL: https://arxiv.org/abs/2005.11401.

2. OWASP Foundation. LLM Prompt Injection Prevention Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/LLM_Prompt_Injection_Prevention_Cheat_Sheet.html.

3. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. NIST AI 600-1. 2024. URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf.

4. Europol. AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement. Luxembourg: Publications Office of the European Union, 2024. URL: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing.

Щербакова Людмила Іванівна,
начальник Управління кримінального
аналізу Головного управління
Національної поліції в Черкаській області

ВІДЕОАНАЛІТИКА В КРИМІНАЛЬНОМУ АНАЛІЗІ: ПРАКТИЧНИЙ ІНСТРУМЕНТАРІЙ І ТАКТИКО-ПРАВОВІ АСПЕКТИ ЗАСТОСУВАННЯ ШІ

У сучасній парадигмі правоохоронної діяльності, що базується на аналітичній розвідці (*Intelligence-led Policing – ILP*), автоматизована обробка великих масивів неструктурованих даних є базовою умовою для оптимізації функціонування