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

підрозділів кримінального аналізу. Стрімке зростання обсягів відеоконтенту, який безперервно надходить із регіональних платформ відеоспостереження типу «Безпечне місто», відомчих ІТ-екосистем, приватних контурів безпеки та нагрудних відеореєстраторів працівників поліції, унеможливлює його ефективне дешифрування виключно в ручному режимі. Пасивний моніторинг моніторів операторами супроводжується критичним впливом «*людського фактора*» – прогресуючим зниженням концентрації уваги, втомою та високою ймовірністю пропуску важливих тактичних індикаторів або розшукуваних об'єктів. Впровадження інтелектуальних систем відеоаналітики на основі штучного інтелекту й нейромережевих архітектур дозволяє трансформувати сирий, лінійний відеопотік у структуровану, індексовану базу аналітичних даних. Це мінімізує часові витрати при зборі доказової бази, оптимізує алгоритми розкриття кримінальних правопорушень та підвищує загальну ефективність оперативно-розшукової діяльності [1; 2].

Практичне застосування *SMART-функцій* (*IVS-алгоритмів*) у кримінальному аналізі: Замість пасивного моніторингу периметра, сучасні інтелектуальні детектори інтегруються безпосередньо в оперативно-розшукову та превентивну діяльність поліції для вирішення конкретних тактичних завдань:

– Перетинання лінії (*Line Crossing Detection*) та Детекція вторгнення (Intrusion Detection): Використовуються аналітиками для автоматичної фіксації руху транспортних засобів у забороненому чи зустрічному напрямках, контролю залізничних переїздів, а також миттєвого виявлення несанкціонованого проникнення осіб на режимні або кримінально вразливі об'єкти. Налаштування часового порогу реагування (*Threshold*) та відсоткової площі об'єкта (*Percentage*) дозволяє ігнорувати дрібні завади (птахи, тіні) й фокусуватися виключно на людях чи автомобілях.

– Виявлення видалення та залишення предметів (*Object Removal / Unattended Baggage Detection*): Застосовуються як технічні інструменти для охорони об'єктів інфраструктури, банкоматів чи безпосередньо матеріальних доказів від викрадення, а також для виявлення потенційно небезпечних

предметів (вибухових пристроїв) у місцях масового скупчення людей (вокзали, площі).

– Аудіодетекція виключень (*Audio Exception Detection*): Акустичний модуль дозволяє в автоматичному режимі, незалежно від напрямку камери, фіксувати звуки пострілів, вибухів, криків чи ДТП, мінімізуючи час реагування нарядів поліції [3].

Спеціалізоване програмне забезпечення для ретроспективного аналізу: Для структурування та швидкого пошуку в терабайтних масивах відеоданих, вилучених із реєстраторів, мобільних телефонів та камер спостереження, аналітики застосовують передові ШІ-платформи:

– Платформа *BriefCam*: Завдяки технології *Video Synopsis* накладає рухомі об'єкти, зафіксовані в різний час, на один короткий відеоряд. Це скорочує час перегляду багатогодинних архівів до кількох хвилин. Система здійснює глибоку класифікацію об'єктів за типами (людина, група, вантажівка тощо) та колірними атрибутами, що спрощує аналіз маршрутів руху підозрюваних автомобілів через інтеграцію з підсистемою «Гарпун» ІПНП.

– Платформа *Veritone Identify*: Спеціалізована модульна архітектура («Управління справами», «Докази», «Підозрювані»), що дозволяє здійснювати автоматизовану фільтрацію та високоточний пошук осіб за розширеними біометричними й антропологічними параметрами: приблизний вік, стать, раса, статура, особливості ходи, колір волосся/бороди, елементи одягу та ручна поклажа. Об'єкти без збігів автоматично заносяться до динамічних реєстрів невпізнаних осіб для ретроспективного пошуку в майбутньому [2].

Тактичні особливості та правові обмеження: У практичній діяльності підрозділів кримінального аналізу встановлений алгоритмами ШІ збіг не може бути єдиною підставою для винесення підозри або пред'явлення обвинувачення. Ідентифікація за допомогою розпізнавання обличь розглядається виключно як один із допоміжних інструментів. Для підтвердження причетності особи обов'язково здійснюється комплексне розслідування, що включає судово-криміналістичну експертизу або процедуру ідентифікації за участю трьох і більше

осіб. Крім того, збір та обробка інформації (зокрема, використання відео з нагрудних реєстраторів патрульних відповідно до Інструкції № 100) мають суворо відповідати Закону України «Про захист персональних даних» та Конституції України (ст. 32, 34), забезпечуючи баланс між ефективністю розслідування та дотриманням прав людини [2].

Ефективність кримінального аналізу в сучасному динамічному безпековому середовищі прямо корелює з рівнем технологічного впровадження інтелектуальних систем відеоаналітики. Застосування багатофакторного нейромережевого трекінгу та аналітичних платформ (*BriefCam, Veritone Identify*) кардинально прискорює виявлення аномальних подій і розкриття резонансних злочинів «по гарячих слідах». Проте успішна та легітимна практична інтеграція цих технологій у площину правоохоронної діяльності потребує:

– Розробки уніфікованих відомчих стандартів та інструкцій щодо поводження з цифровими метаданими ШІ;

– Масштабування обчислювальних можливостей серверного обладнання для обробки великих масивів даних (Big Data);

– Чіткого дотримання правових та етичних меж захисту особистої інформації громадян [1, 2].

Список використаних джерел

1. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України : матеріали наук.-практ. конф. (Львів, 20 груд. 2024 р.) / упоряд. Т. В. Магеровська. Львів : ЛьвДУВС, 2025. 137 с.

2. Мордвинцев М. В., Пашнєв Д. В., Наконечний В. С. Особливості використання технологій відеоаналізу та програмного забезпечення з розпізнавання обличь у кримінальному аналізі. *Право і безпека*. 2025. № 1 (96). С. 90–103.

3. Мирошниченко В. О., Махницький О. В., Кочеткова І. Б. Використання відеоаналітики у роботі Національної поліції : метод. рекомендації / Дніпропетровський державний університет внутрішніх справ. Дніпро : ДДУВС, 2020. 38 с.