

Едуард РИЖКОВ, професор кафедри інформаційних технологій, Дніпровський державний університет внутрішніх справ, кандидат юридичних наук, професор

АРХІТЕКТУРА МЕТОДИКИ «OSINT+» У КОНТЕКСТІ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасна архітектура національної безпеки перебуває на етапі безпрецедентної технологічної сингулярності. В умовах тотальної цифровізації, експоненційного зростання обсягів неструктурованих даних (Big Data) та переходу транснаціональної злочинності у площину Web3.0, традиційні методи оперативно-розшукової діяльності виявляють свою гносеологічну та функціональну обмеженість. Як свідчить практика, сьогодні понад 80% критично важливої для слідства інформації генерується та зберігається поза межами закритих відомчих баз даних — у соціальних мережах, месенджерах, реєстрах та криптовалютних транзакціях [1].

Ще у 2008 році розробники перших потужних інтегрованих систем МВС у Луганській області (ІАС «АРМОР», «СОВА», «АРГУС») зазначали, що розрізненість баз даних та неможливість простежити взаємозв'язки між об'єктами обліку є головним бар'єром ефективності правоохоронців [2, с. 71]. Сьогодні цей бар'єр пролягає не між внутрішніми підрозділами, а між відомчим контуром (Інформаційний портал Національної поліції України — ІПНП) та глобальним інформаційним простором (OSINT).

Вирішення цієї проблеми лежить у площині впровадження авторської методики «OSINT+», яка базується на синергії закритих державних реєстрів, автоматизованих засобів розвідки відкритих джерел та моделей штучного інтелекту (ШІ) [3].

Деконструюючи досвід створення луганського інтегрованого банку даних, варто виокремити фундаментальні рішення, які випередили свій час і сьогодні є базисом для побудови архітектури «OSINT+».

По-перше, це відмова від жорсткої ієрархії на користь зв'язків типу «багато-до-багатьох» (Схема «Особа-Адреса-Подія») [2, с. 78]. По-друге, це запровадження візуального та графового аналізу в системі «СОВА», що дозволило автоматизувати виявлення логічних закономірностей зв'язків об'єктів (наприклад, аналіз телефонних трафіків ОЗГ) [2, с. 61, 100]. По-третє, спроба алгоритмізувати біометричну ідентифікацію через підсистему «АРГУС» (переведення «словесного портрета» у базу даних) [2, с. 116].

Проте ці системи були замкнутими. Вони чекали, поки оперативний працівник внесе інформацію вручну. З позиції сучасного архітектурного проектування, ІПНП сьогодні має стати не просто сховищем, а активним аналітичним ядром, де відомчі дані виступають лише початковим «зерном» (Seed) для автоматичного розгортання графа зв'язків у відкритому середовищі.

За нашою позицією, методика «OSINT+» — це гібридна епістемологічна модель та технологічний фреймворк, що передбачає автоматизоване двостороннє збагачення даних: від закритого контуру (ІПНП) до відкритих джерел (OSINT), із подальшою їх верифікацією та структуруванням за допомогою технологій штучного інтелекту (AI Processing) [4].

Розвиваючи концепцію «OSINT+» до вимог сьогодення, її архітектура, на наш погляд, має складатися з трьох автоматизованих рівнів:

1. Ініціація (Seed Level), яка реалізується через запит слідчого або оперативника в ІПНП (ПІБ, номер телефону, ПІН, фотографія, криптогаманець).

2. Автоматизований збір (Collection Engine) інформації орієнтуючого характеру реалізується через запуск оркестратора скриптів (на базі Python, API-інтерфейсів), який без участі людини опитує соціальні мережі, реєстри (YouControl, Опендатабот), витіки баз даних (Data Leaks) та спеціалізовані пошукові системи (Shodan, Censys).

3. III-Процесинг (AI Verification Cycle) запускається через використання Large Language Models (LLM) для вилучення сутностей з текстів (Named Entity Recognition) та алгоритмів комп'ютерного зору для розпізнавання обличчя і атрибутів на зібраних медіафайлах.

Як варіант на підставі створеного концепту модернізації, ми пропонуємо можливі практичні кроки інтеграції за пріоритетними напрямками діяльності поліції:

1. Впровадження модулю автоматичного збагачення сутності «Особа» (SOCMINT & PII Automation). При створенні або запиті картки особи в ПНП (наявність номеру телефону чи email), система повинна автоматично звертатися до відкритих OSINT-фреймворків (аналогів SpiderFoot [4], Holehe, Maigret). Це дозволить миттєво підтягувати до досьє особи її цифрові сліди: акаунти в Telegram, Instagram, історію зміни аватарів, геотеги та пов'язані IP-адреси. Замість ручного пошуку, працівник поліції отримує готовий граф цифрового профілю.

2. Еволюція інформаційної підсистеми «Гарпун» та відеоаналітики через Computer Vision. Перехід від класичного ручного «словесного портрета» до III-біометрії. Інтеграція загальнодержавної системи відеомоніторингу [5] з підсистемами ПНП має базуватися на нейромережових ембедингах (FaceNet, YOLO). Оператор (ситуаційний аналітик) повинен мати змогу формувати запит не лише за номером авто чи обличчям, а за семантичним описом (наприклад, «особа з червоним рюкзаком, що рухалась у напрямку...»). Система «OSINT+» автоматично порівнюватиме ці відеодані з відкритими масивами фотографій у соціальних мережах для встановлення особи (аналоги PimEyes/FindClone).

3. Протидія кримінальній токенизації (FININT/Crypto-OSINT). У відповідь на перехід ОЗГ до розрахунків у криптовалютах [1], ПНП має бути доповнений модулем On-chain аналітики («Follow the Code»). Методика «OSINT+» передбачає автоматичне зіставлення адрес криптогаманців, виявлених під час обшуків чи в даркнеті, з OSINT-маркерами (згадки гаманців на хакерських форумах, у Telegram-каналах) для деанонізації кінцевого бенефіціара та зв'язку його з легальними рахунками підприємств через реєстри.

4. Впровадження локальних (On-Premise) LLM-моделей для обробки неструктурованих даних. Сьогодні оперативники та слідчі генерують колосальний обсяг неструктурованих текстів (рапорти, протоколи допитів, фабули Журналу реєстрації заяв (повідомлень) про злочини та інш.). Пропонується інтегрувати в ПНП локальну «поліцейську» нейромережу для автоматичного аналізу цих текстів. III (через NLP) самостійно вилучатиме імена, адреси, номери телефонів та автоматично будуватиме неочевидні зв'язки між різними кримінальними провадженнями, позбавляючи слідчого необхідності ручного введення реквізитів.

Таким чином, на підставі вищезазначеного сформулюємо наступні висновки:

1. Використання інформаційних технологій у правоохоронній діяльності має еволюціонувати від концепції «електронної картотеки» до концепції «проактивного предиктивного аналізу» (Predictive Policing), поступово змінюючи суть самої парадигми діяльності поліції. Інформаційний портал Національної поліції України не повинен бути ізольованим архівом; він має стати ядром екосистеми, що безперервно взаємодіє з відкритим інформаційним простором.

2. Наша авторська методика «OSINT+», яка за визначенням поєднує закриті бази (ПНП), автоматизований збір відкритих даних (OSINT) та машинну обробку (III), дозволяє нівелювати «людський фактор», ліквідувати інформаційний шум та скоротити час від збору даних до прийняття процесуального рішення у десятки разів. Таким чином, синергія «OSINT+» поступово повинна сприйматися як новий стандарт у інформаційно-аналітичній діяльності поліції.

3. Впровадження автоматизованих скриптів та III вимагає імплементації протоколів верифікації (на кшталт Протоколу Берклі [6]), щоб алгоритмічні висновки системи («OSINT+») мали належну доказову силу, а зібрані цифрові сліди могли бути легалізовані в рамках вітчизняного кримінального процесу та вдосконалили оперативно-розшукову діяльність.

Список використаних джерел

1. Ryzhkov E., Ohrimenco S. Criminal tokenization in the era of financial market transformation: challenges, strategies, and counteraction tactics / Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали X Міжнар. наук.-практ. конф. (м. Дніпро, 16 бер. 2026 р.) ; у 2-х ч. Дніпро : Дніпров. держ. ун-т внутр. справ, 2026. Ч. II. С. 362-365.
2. Гуславский В. С., Задорожний Ю. А., Розовский Б. Г. Информационно-аналитическое обеспечение раскрытия и расследования преступлений : монография. Луганск : Изд-во «Элтон-2», 2008. 136 с.
3. Рижков Е.В. Методика "OSINT+": синергія відкритих та відомчих інформаційних ресурсів у діяльності оперативних підрозділів Національної поліції України / Е.В. Рижков / Роль OSINT-досліджень у підвищенні рівня національної безпеки України : матер. кр. столу (м. Львів, 07 травня 2025 р.). / упорядник: І. О. Ревак. Львів: Львівськ. держ. ун-т внутр. справ, 2025. С. 192-199.
4. Рижков Е.В. Перспективи комплексного використання автоматизованих систем (фреймворків) та моделей штучного інтелекту в процесі OSINT / Е.В. Рижков / Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України, наук.-практ. конфер.: матер. Всеукр. науково-практ. конф. (м. Львів, 26 грудн. 2025 р.). / упорядник: Т.В. Магеровська. Львів: Львівськ. держ. ун-т внутр. справ, 2026. – С. 59-62
5. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 13.06.2018 № 497 (зі змінами від 22.11.2023). URL: <https://zakon.rada.gov.ua/laws/show/z0787-18#Text>
6. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. URL: <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf>

Ольга ОГІРКО, професор кафедри інформаційних технологій, Львівський державний університет внутрішніх справ, кандидат технічних наук, доцент.

Наталія ГАЛАЙКО, старший викладач кафедри інформаційних технологій, Львівський державний університет внутрішніх справ

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АДМІНІСТРУВАННІ ІНФОРМАЦІЙНИХ СИСТЕМ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Сучасна система глобальної безпеки зазнає суттєвих змін під впливом стрімкого розвитку цифрових технологій. Для України, яка протистоїть повномасштабній агресії, впровадження інноваційних рішень у діяльність правоохоронних органів є важливою умовою забезпечення національної безпеки та ефективного захисту держави. Одним із найбільш перспективних напрямів цифрової трансформації є використання потенціалу штучного інтелекту (ШІ) у безпековому секторі.

У науковій літературі штучний інтелект визначається як сукупність методів і технологій, що дають змогу комп'ютерним системам виконувати окремі функції, властиві людському мисленню [1]. Йдеться про здатність аналізувати інформацію, навчатися на основі отриманих даних, розпізнавати мовлення, прогнозувати події та приймати рішення.