12. Turner J. I. Managing digital discovery in criminal cases. *Journal of Criminal Law and Criminology*. 2019. Vol. 109. No. 2. P. 237–312. URL: https://scholarlycommons.law.northwestern.edu/jclc/vol109/iss2/3

13. Постанова Об'єднаної палати Касаційного кримінального суду у складі Верховного Суду від 29 березня 2021 р. у справі № 554/5090/16-к, провадження № 51-1878кмо20. ЄДРСР. № 96074938. URL: https://reyestr.court.gov.ua/Review/96074938

14. Court of Justice of the European Union. *M.N. (EncroChat)*, Case C-670/22, Judgment of 30 April 2024, ECLI:EU:C:2024:372.

15. European Court of Human Rights. *Yüksel Yalçınkaya v. Türkiye* [GC], Application no. 15669/20, Judgment of 26 September 2023. HUDOC No. 001-227636.

Рижков Едуард Володимирович,
професор кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, професор

ШІ-АГЕНТИ ЯК ІНСТРУМЕНТ АВТОМАТИЗАЦІЇ КРИМІНАЛЬНОГО АНАЛІЗУ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Фундаментальною перешкодою для оперативного розкриття та всебічного розслідування злочинів у цифрову епоху є біологічні та психологічні обмеження людського аналітичного апарату. Концепт «інформаційного перевантаження», вперше введений у науковий обіг соціологом Бертрамом Гроссом, описує стан системи, за якого вхідний потік даних суттєво перевищує обчислювальні та пропускні можливості системи щодо їх обробки та засвоєння [1, с. 23]. У контексті індивідуальної роботи кримінального аналітика, слідчого або оперативника цей феномен трансформується у когнітивне перевантаження – стан, коли вимоги до обробки інформації виснажують доступні когнітивні ресурси та ємність робочої пам'яті людини [2, с. 1178]. На сьогодні можливості генерації та збору цифрових слідів багаторазово перевищують фізичні можливості людського мозку щодо їх обробки.

На сучасному етапі понад 80 % інформації, що становить оперативний інтерес, існує у неструктурованому вигляді. Тому в умовах перманентної цифрової багатозадачності когнітивне перевантаження безпосередньо впливає на спроможність співробітника приймати обґрунтовані рішення. Перевищення ємності робочої пам'яті погіршує якість аналітики, подовжує час реакції на оперативну обстановку та знижує стійкість до маніпуляцій [2, с. 1180]. Управлінським наслідком цього явища є феномен «паралічу прийняття рішень», за якого наявність величезного обсягу інформації не призводить до розкриття злочину, а навпаки, унеможливлює своєчасне формування стратегії розслідування [3, с. 99].

З позиції пошуку максимальної ефективності використання сучасних ІТ-інструментів важливою є потенційна інтеграція штучного інтелекту у правоохоронну діяльність взагалі та кримінальний аналіз зокрема [4, с. 248].

Технологічна еволюція інструментарію кримінального аналізу характеризується переходом від систем, заснованих на жорстко детермінованих правилах пошуку та реактивних чат-ботах, до епохи штучного інтелекту агентного типу. Це зсув парадигми реалізації кримінального аналізу в інтересах слідства та оперативно-розшукової діяльності, де поліцейський перетворюється з оператора баз даних на стратегічного керівника цифрового аналітичного штабу.

У цьому контексті автономні ШІ-агенти розглядаються нами як програмні сутності, здатні сприймати цифрове середовище, ухвалювати рішення та виконувати багатокрокові дії для досягнення цілей, визначених користувачем, з мінімальним зовнішнім втручанням. Фундаментальною архітектурою для таких агентів є великі мовні моделі (LLM), які забезпечують не просто семантичний розбір тексту, а виконують функцію когнітивного рушія.

Можливості автономних агентів базуються на трьох основних стовпах: міркування, планування, контекстна пам'ять. Перший демонструє здатність аналізувати неповні або зашумлені дані, використовувати дедуктивні та індуктивні методи для виявлення неочевидних патернів, кореляцій та формування логічних висновків з урахуванням складного правового контексту. Другий – розкладання глобальної мети розслідування на послідовність атомарних завдань. Такий агент здатний

ідентифікувати необхідні кроки (наприклад, оцінити достовірність джерела, витягнути геолокацію, перевірити особу за базами розшуку), оцінити альтернативні варіанти дій та динамічно адаптувати план при виявленні нової інформації. Третій – утримання в пам'яті хронології операцій, збереження проміжних результатів (persistent memory) та здатність звертатися до попереднього досвіду аналізу в рамках поточного або пов'язаних кримінальних проваджень [5].

Найвищим рівнем реалізації агентного підходу у правоохоронній діяльності є мультиагентні системи, де складні аналітичні процеси декомпозуються та розподіляються між вузькоспеціалізованими віртуальними експертами. Архітектурно це нагадує концепцію розподіленого вирішення проблем:

– агент доступу до реєстрів, який відповідає виключно за легітимне опитування державних баз даних (наприклад, ЄІС МВС) з дотриманням протоколів доступу;

– агент розвідки відкритих джерел, який займається картуванням цифрових слідів, аналізом соціальних зв'язків і виявленням прихованих контактів у мережі Інтернет;

– агент аналізу свідчень, який фокусується на NLP-аналізі текстів, виявляючи семантичні суперечності у показаннях фігурантів, маркери обману або невідповідності хронології;

– агент предиктивної аналітики, який застосовує методи ймовірнісного моделювання для прогнозування еволюції злочинної діяльності або ймовірних локацій переховування.

Такий структурований поділ обов'язків гарантує, що операції зі спостереження, вилучення даних та їх кореляції логічно ізольовані, що відповідає вимогам інформаційної безпеки та мінімізує ризики перевищення повноважень [6].

Проте слід зазначити, що великі мовні моделі здатні до складного синтезу текстів, проте вони не володіють істинним розумінням реальності. Фундаментальною проблемою є так звані «галюцинації» – феномен, коли модель впевнено генерує синтаксично зв'язний, але фактично хибний контент (притаманно у 15–30 % випадків) [7]. У криміналістичному контексті це створює загрозу генерування хибних слідів.

Прецеденти генерування фальшивих даних вже зафіксовані в українському судочинстві. В Ухвалі Верховного Суду від 15 січня 2026 року (справа № 240/14153/24) було виявлено, що учасник справи подав касаційну скаргу, аргументовану посиланнями на постанови Великої Палати Верховного Суду,

яких в реальності ніколи не існувало. Суд констатував, що скаржник використав інструменти ШІ, отримав результат у формі «галюцинацій» і вдався до недобросовісного користування процесуальними правами [8]. Це безапеляційно доводить, що будь-який результат ШІ потребує фахової верифікації людиною.

Чинний Кримінальний процесуальний кодекс України наразі не містить спеціальних норм, які б детально регулювали допустимість доказів, отриманих за допомогою обробки ШІ або результатів автоматизованого розпізнавання біометричних даних [9, с. 277]. Ключовою доктринальною перешкодою є проблема так званої «чорної скриньки» – непрозорості внутрішньої логіки та архітектури прийняття рішень моделлю штучного інтелекту. Якщо сторона захисту не може перевірити, за якими саме критеріями алгоритм розпізнав обличчя підозрюваного або встановив кореляцію у білінгах, такий доказ з високою ймовірністю буде визнано судом недопустимим через сумніви у його достовірності [9, с. 278].

На шляху до європейської інтеграції імплементація ШІ у Нацполіції має корелюватися з положеннями Закону ЄС про штучний інтелект. Документ жорстко класифікує ШІ-системи за рівнем ризику. Практично всі сфери застосування ШІ в правоохоронній діяльності – зокрема оцінка надійності доказів, профілювання ризиків вчинення злочинів, поліграфи – віднесені до категорії «Високого ризику» [10].

З огляду на суворі вимоги до безпеки та критичну чутливість слідчої та оперативно-розшукової інформації (персональні дані громадян, матеріали НСРД, державна таємниця), використання публічних комерційних LLM-платформ (таких як хмарні версії ChatGPT, Claude, Gemini) у роботі Національної поліції є категорично неприпустимим.

Комерційні хмарні моделі створюють безпрецедентні загрози компрометації даних. Завантаження матеріалів кримінальних проваджень на сервери третіх осіб автоматично виводить їх за периметр контролю правоохоронного органу [11].

Єдино можливим вектором технологічного розвитку є створення суверенних локальних поліцейських ШІ-систем, які функціонують у повністю ізольованих комп'ютерних мережах [12]. У такій архітектурі всі обчислювальні потужності фізично розміщені у захищених центрах обробки даних Національної поліції або інших уповноважених структур сектору безпеки та не мають жодного, навіть опосередкованого, з'єднання з мережею Інтернет.

Процес імплементації ШІ в правоохоронні органи є глобальним трендом, який активно підтримується і в Україні. Успішні кейси розгортання доводять критичну необхідність переходу від теоретичних досліджень до оперативної інтеграції. Національна поліція України послідовно розбудовує цифрову інфраструктуру, ключовим елементом якої є Єдина інформаційна система МВС (ЄІС МВС). Ця система забезпечує технологічний фундамент для інтеграції, об'єднуючи Інформаційний портал НПУ, бази біометричної ідентифікації та інші спеціалізовані реєстри в єдиний простір, управління доступом до якого координують Департамент інформаційно-аналітичної підтримки (ДІАП) та Департамент кримінального аналізу [13, с. 144].

Сьогодні правоохоронні органи стикаються з викликами, які неможливо подолати виключно за рахунок збільшення людського ресурсу; натомість потрібна фундаментальна зміна парадигми аналізу даних [14, с. 172].

У контексті зазначеного фахівці пропонують на інституційному рівні створення міжвідомчих криміналістичних центрів штучного інтелекту [15, с. 413]. Своєю чергою ми стверджуємо, що пріоритетним напрямком є створення єдиного, інституційного локального ШІ для кримінального аналізу (можливо, для усієї вітчизняної правоохоронної системи), який об'єднає розрізнені ініціативи в стандартизований мультиагентний комплекс із дотриманням усіх гарантій захисту персональних даних та інтеграцією стандартів транскордонної еквівалентності збору даних.

Отже, трансформація операційної діяльності підрозділів кримінального аналізу Національної поліції України за рахунок імплементації ШІ-агентів є не просто технологічним оновленням програмного фонду, а радикальним зсувом парадигми протидії злочинності. Застосування автономних алгоритмів дозволяє ефективно розв'язати кризу когнітивного перевантаження аналітиків, спричинену експоненційним зростанням масивів неструктурованих даних. Автоматизація рутинних операцій звільняє висококваліфіковані кадри для безпосередньої роботи з розкриття та розслідування злочинів. Створення надійної архітектури з автоматичним логуванням та глибоким аудитом дій агентів забезпечить відповідність українського правоохоронного інструментарію загальноєвропейському контуру збору та оцінки доказів.

Список використаних джерел

1. Грабовська С. Л., Мусаковська О. М. Інформаційне перевантаження: психологічний ракурс. *Psychological journal*. Vol. 6 Is. 7. Інст-т психол-ї ім. Г. С. Костюка НАПН України. 2020. С. 18–27.
2. Жук В. В. Когнітивне перевантаження як проблема сучасної психології. *Наукові інновації та передові технології.* 2025. № 7 (47). С. 1173–1182. URL: https://perspectives.pp.ua /index.php/nauka/article/download/26479/26449/35129.
3. Іванова С., Анпілогов А. Meaning як механізм координації: філософсько-когнітивна модель стратегічної діяльності. *Грані*. Науково-теоретичний альманах. 2026. 29 (2). С. 97–103. https://doi.org/10.15421/172691.
4. Рижков Е. В. Перспективи комплексного використання автоматизованих систем (фреймворків) та моделей штучного інтелекту в процесі OSINT. *Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України, наук.-практ. конфер. :* матер. Всеукр. науково-практ. конф. (м. Львів, 26 грудн. 2025 р.) / упор. : Т. В. Магеровська. Львів : Львівськ. держ. ун-т внутр. справ, 2026. С. 245–251.
5. What are AI agents? Definition, examples, and types. *Google Cloud. 04/02/2026.* URL: https://cloud.google.com/ discover/what-are-ai-agents.
6. Niranjan M. M. Medini Narasimha Bailkeri Law Enforcement Framework for Multi-Agent AI Systems. *Technical Disclosure Commons.* 04 May 2026. 20 с. URL: https://www.tdcommons.org/cgi/viewcontent.cgi?article=11295&context=dpubs_series
7. Large Language Models in Public Health: Theory and Practice. URL: https://publichealthaihandbook.com/future/llm-theory-practice.html.
8. Берназюк Я. О. Штучний інтелект крізь призму судової практики: реалії, помилки та перспективи. *Верховний Суд.* 2026. URL: https://court.gov.ua/storage/portal/supreme/ prezent2026/167_AI_through_Case_Law_Lens_bernaziuk.pdf.
9. Машталяр О. М. Штучний інтелект і біометричні дані в кримінальному процесі України: допустимість, ризики, судовий контроль. *Науковий вісник УжНУ. Серія «Право».* 2026. Вип. 39–42. С. 276–283. URL: https://visnyk-juris-uzhnu.com/wp-content/ uploads/2026/01/39-2.pdf.

10. High-Risk AI - EU AI Act Guide // Orrick AI Resource Center. URL: https://ai-law-center.orrick.com/eu-ai-act/high-risk-ai/.

11. Manish Gupta Secure LLM for Government: Why Public Sector AI Needs a Different Playbook // Innefu Labs. March 10, 2026. URL: https://innefu.com/secure-llm-for-government-why-public-sector-ai-needs-a-different-playbook/.

12. Jamil Alshaer Mitigating Data Leakage in High-Compliance Environments: A Governance Framework for Local TechRxiv. 10 January 2026. DOI: 10.36227/techrxiv.176800912. 24304866/v1. URL:

13. Моца В. В. Теоретико-методологічні засади використання кримінального аналізу оперативними підрозділами правоохоронних органів України. *Науков. вісник Ужгород. Нац. унів-ту. Серія «Право».* Вип. 73: ч. 2. 2022. С. 141–147.

14. Рижков Е. В. Прикладні аспекти впровадження штучного інтелекту в системи біометричної ідентифікації та відеоаналітики в діяльності підрозділів Національної поліції України. *Роль OSINT-досліджень у підвищенні рівня національної безпеки України :* матер. Всеукр. наук. конф. (м. Львів, 07 травня 2026 р.). / укладачі : О. І. Пацула, І. О. Ревак. Львів : ЛьвДУВС, 2026. С. 172–175. DOI https://doi.org/10.5281/zenodo.20718088.

15. Погорецький М. А. Штучний інтелект у доказуванні в досудовому та судовому провадженнях. *Науковий вісник УжНУ. Серія «Право».* 2025. Вип. 58. Ч. 4. С. 398–417. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/12/58.pdf

Русиник Андрій Михайлович,
начальник Управління кримінального
аналізу Головного управління
Національної поліції в Донецькій області

СПЕЦИФІКА РОБОТИ ПІДРОЗДІЛІВ КРИМІНАЛЬНОГО АНАЛІЗУ В УМОВАХ ВОЄННОГО СТАНУ

Кримінальний аналіз – це професія та процес, у яких використовується комплекс кількісних і якісних методів для аналізу даних, що мають цінність для правоохоронних структур та їхніх громад. Він охоплює аналіз злочинів і злочинців, жертв злочинів, порушень громадського порядку, проблем якості життя, проблем дорожнього руху та внутрішніх операцій поліції,