Київ : Дакор, 2023. 238 с. URL: https://rep.dnuvs.ukr.education/server/api/core/bitstreams/ad8f13d9-9b33-4a3f-beb1-17489cb8884e/content

4. Білоус Р. В., Василинчук В. І., Таран О. В. Використання методів кримінального аналізу під час оперативного провадження та досудового розслідування. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 1 (118). С. 131–137. DOI: https://doi.org/10.33270/01211181.131

5. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України : монографія / О. Користін, Д. Швець, Б. Бутко, Б. Денисенко та ін., за заг. ред. О. Є. Користіна. Київ : ВАЙТ, 2024. 450 с. URL: https://vaite.kiev.ua/biblio/euam/240322_1830_INTELLIGENCE-LED_POLICING.pdf

6. Марко С.І., Богатирчук О. М. Використання можливостей кримінального аналізу у протидії організованій екологічній злочинності. *Українська поліцеїстика: теорія, законодавство, практика.* № 1 (9). 2024. С. 8–10. DOI: https://doi.org/10.32782/2709-9261-2024-1-9-3

Салманов Олексій Валерійович,
заступник директора інституту
з освітньої та науково-дослідної діяльності
ННІ № 1 Харківського національного
університету внутрішніх справ, кандидат
юридичних наук, доцент;
Лисюк Артьом Миколайович,
курсант Харківського національного
університету внутрішніх справ

ПРОЦЕСУАЛЬНІ АСПЕКТИ ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ КРИМІНАЛЬНОГО АНАЛІЗУ ЗА ДОПОМОГОЮ ШІ В ДОКАЗУВАННІ

Впровадження технологій штучного інтелекту (далі – ШІ) у сферу кримінального судочинства є однією з найбільш обговорюваних тенденцій сучасної юридичної науки та правозастосовної практики. Кримінальний аналіз, як зазначив В. А. Бурангулов традиційно базувався на аналітичних здібностях правоохоронних органів, сьогодні отримує потужний інструмент у вигляді алгоритмів машинного навчання, здатних

обробляти колосальні масиви великих даних [1, с. 17]. Штучний інтелект дозволяє виявляти приховані закономірності, прогнозувати кримінальні ризики, зіставляти спосіб вчинення злочинів, аналізувати трафік мобільного зв'язку, фінансові потоки та зв'язки між фігурантами з точністю й швидкістю, недоступними для людини. Проте автоматизація аналітичної функції породжує складну систему процесуальних викликів, пов'язаних із трансформацією результатів такого аналізу в належні та допустимі докази у кримінальному провадженні.

Аналізуючи нормативну базу, слід підкреслити, що чинний Кримінальний процесуальний кодекс України [2] (далі – КПК України) не містить дефініцій «штучний інтелект» чи «кримінальний аналіз за допомогою ШІ». Водночас процесуальна основа для використання таких технологій закладена у загальних положеннях про збирання та оцінку доказів. Відповідно до ч. 1 ст. 84 КПК України [2], доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому КПК України [2] порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Самі по собі аналітичні звіти, генеровані ШІ, є продуктом інтелектуальної та програмної обробки наборів даних з різних джерел, включаючи попередні звіти про інциденти, журнали безпеки та патерни мережевого трафіку [3, с. 357].

Тому ключове процесуальне питання полягає у визначенні правової природи та процесуального статусу кінцевого документа кримінального аналізу. Залежно від способу залучення технології, такий документ може процесуально оформлюватися або як висновок аналітика, або як частина висновку експерта, якщо проводилася судова експертиза з використанням автоматизованих систем штучного інтелекту відповідно до Закону України «Про судову експертизу» [4].

Важливим елементом процесуального доказування є дотримання вимог належності та допустимості. Згідно ст. 85 КПК України [2], належними є докази, які прямо чи непрямо підтверджують обставини, що підлягають доказуванню у кримінальному провадженні, та інші обставини, які мають значення для кримінального провадження, а також достовірність чи недостовірність інших доказів. ШІ допомагає встановити

належність, пов'язуючи між собою, наприклад, геолокація цифрових слідів різних осіб у певний проміжок часу. Набагато складнішою є проблема допустимості, яка регулюється ст. 86 КПК України [2]. Доказ визнається допустимим, якщо він отриманий у порядку, встановленому цим КПК України [2]. Оскільки алгоритми ШІ працюють за принципом «чорної скриньки», коли внутрішня логіка прийняття рішення програмою може діяти творчо та непередбачувано, що порушує право на справедливий суд [5, с. 79]. Сторона захисту, керуючись ст. 22 КПК України [2] щодо змагальності сторін, має повне право оскаржувати достовірність висновків ШІ. Для забезпечення допустимості обвинувачення повинно мати можливість продемонструвати суду валідність програмного забезпечення, відсутність системних помилок та алгоритмічного упередження.

Процес використання результатів ШІ-аналізу у доказуванні має чітко розмежовувати тактико-криміналістичне значення та безпосередньо процесуальне. На етапі досудового розслідування аналітичні системи ШІ використовуються переважно як орієнтовна інформація для висування слідчих версій, планування розслідування або визначення напрямів обшуку. Така інформація не є доказом у розумінні ст. 84 КПК України [2], а виступає криміналістичним орієнтиром. Щоб набути процесуального статусу, результати аналізу мають пройти процедуру легалізації. Процесуальний алгоритм легалізації включає: по-перше, вилучення первинних цифрових даних із дотриманням вимог ст. 168 КПК України [2] щодо порядку тимчасового вилучення майна, по-друге, призначення технічної або комп'ютерно-технічної експертизи із залученням ШІ як інструменту дослідження, де експерт несе кримінальну відповідальність за ст. 384 Кримінального кодексу України [6] за завідомо неправдивий висновок. Саме експерт, а не алгоритм, верифікує результати роботи ШІ та підписує висновок, інтегруючи автоматизовані розрахунки у процесуальну площину.

Серйозною процесуальною перепоною є забезпечення права на захист та доступу до матеріалів розслідування. Відповідно до ч. 1 ст. 290 КПК України [2], визнавши зібрані під час досудового розслідування докази достатніми для складання обвинувального акта, прокурор або слідчий за його дорученням зобов'язаний відкрити матеріали кримінального провадження стороні захисту. Якщо аналітичний звіт або висновок експерта

прямо посилається на розрахунки автоматизованої системи, захист має право знати, за якими критеріями та алгоритмами ці дані було оброблено. Обмеження доступу до технологічної суті ШІ-аналізу під приводом охорони інтелектуальної власності порушує рівність прав сторін. Захист позбавляється можливості перевірити, чи не було у вихідних даних помилок, які викривили кінцевий результат.

Отже, на основі проведеного аналізу можна зробити висновок, що використання результатів кримінального аналізу за допомогою ШІ у доказуванні є перспективним, але процесуально складним інститутом, який потребує негайної адаптації національного законодавства. Результати роботи ШІ самі по собі не є автономними доказами, вони набувають процесуального значення лише через їх належне оформлення як документів або через висновки судових експертиз, де ШІ виступає як метод дослідження. Ключовою умовою їх допустимості є дотримання стандартів прозорості, можливості верифікації алгоритмів стороною захисту та повне виключення принципу «чорної скриньки» під час судового розгляду. Перспективи подальших досліджень полягають у розробці детальних криміналістичних методик і внесенні змін до КПК України [2], які б чітко регламентували порядок використання цифрових аналітичних платформ штучного інтелекту, забезпечуючи баланс між технологічним прогресом у розслідуванні злочинів та дотриманням фундаментальних прав і свобод людини.

Список використаних джерел

1. Бурангулов В. А. Сутність кримінального аналізу. *Протидія злочинності: проблеми практики та науково-методичне забезпечення.* 2023. № 4. С. 14–17. URL: https://sulj.oduvs.od.ua/archive/2023/4/4_2023.pdf#page=14.

2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

3. Форос Г. В., Калугін В. Ю., Грезіна О. М. Методологія кримінального аналізу в умовах зростання кіберзагроз. *Юридичний науковий електронний журнал.* 2025. № 11. С. 356–359. URL: https://dspace.oduvs.edu.ua/server/api/core/bitstreams/cf9a9d25-92d3-4199-b2b5-483875755ff9/content.

4. Про судову експертизу: Закон України від 25.02.1994 № 4038-XII. URL: https://zakon.rada.gov.ua/go/4038-12.

6. Кожухар О. Принцип прозорості в контексті правового регулювання систем штучного інтелекту. *Наукові записки НаУКМА*. 2025. № 15. С. 78–85. URL: https://nrplaw.ukma.edu.ua /article/view/324736/325537.

7. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-IIIURL: https://zakon.rada.gov.ua/go/2341-14.

Спиридонов Олексій Володимирович,
начальник Управління кримінального
аналізу Головного управління
Національної поліції
в Миколаївській області

ПІДГОТОВКА АНАЛІТИКІВ В УМОВАХ ВОЄННОГО СТАНУ

Стабільний розвиток та захист суверенітету Української держави в умовах збройної агресії вимагають побудови гнучкої, стійкої та багатофункціональної системи національної безпеки. Еволюція людської цивілізації та глобальна цифровізація сприяють виникненню нових форматів суспільних відносин, які потребують чіткого врегулювання. Цей процес неминуче супроводжується трансформацією характеру злочинності, її засобами, умовами та способами вчинення, формуючи потребу у постійному вдосконаленні та готовності до нових викликів з боку працівників правоохоронних органів. Національна поліція України як центральний орган виконавчої влади стала ключовою ланкою, що забезпечує стабільність внутрішнього безпекового середовища. В умовах повномасштабного вторгнення характер протиправної діяльності зазнав докорінних змін, спричинених веденням гібридної війни, що створює необхідність у підготовці кваліфікованих кадрів, здатних на збір, аналіз та узагальнення оперативно значущої інформації.

Впровадження моделі поліцейської діяльності, керованої аналітичною розвідкою (Intelligence-Led Policing, ILP) стало поштовхом для переходу правоохоронної системи від традиційної моделі роботи до діяльності, спрямованої запобігання злочинності. В умовах воєнного стану, коли ресурси правоохоронних органів є обмеженими, модель ILP забезпечує їх максимально вигідне та раціональне використання, надаючи