DOI https://doi.org/10.30525/978-9934-26-699-7-2

ТЕОРЕТИКО-ПРИКЛАДНІ ЗАСАДИ КРИМІНАЛЬНОГО АНАЛІЗУ ЯК ІНСТРУМЕНТУ ЦИФРОВІЗАЦІЇ СУЧАСНОЇ КРИМІНАЛІСТИКИ

Василова О. В.

ВСТУП

Цифровізація суспільних відносин та стрімке зростання обсягів електронної інформації зумовлюють суттєві трансформації інформаційно-аналітичного забезпечення діяльності правоохоронних органів. У сучасних умовах встановлення обставин кримінального правопорушення дедалі більшою мірою пов'язане з використанням цифрових даних, отриманих із мобільних пристроїв, хмарних сервісів, електронних комунікаційних платформ, цифрових фінансових систем та відкритих джерел інформації (OSINT). Це обумовлює необхідність ефективної інтеграції різнорідних інформаційних масивів, забезпечення їх цілісності, достовірності та належної інтерпретації у межах кримінального провадження. Як зазначають вітчизняні дослідники, щорічне зростання обсягів інформації, що використовується в діяльності правоохоронних органів, зумовлює потребу у формуванні у кримінальних аналітиків спеціалізованих компетентностей у сфері обробки великих даних, використання сучасних аналітичних інструментів і забезпечення належного рівня захисту інформації та дотримання етичних стандартів[1].

У зв'язку з цим, кримінальний аналіз виступає важливим елементом інформаційно-аналітичного забезпечення діяльності правоохоронних органів. У наукових джерелах він визначається як професійна аналітична діяльність, спрямована на збирання, систематизацію, узагальнення та інтерпретацію інформації, отриманої з різних джерел, з метою її трансформації у структуровані знання, необхідні для підтримки оперативно-розшукової та слідчої діяльності. При цьому наголошується, що кримінальний аналіз не підмінює процесуальні функції слідчих чи оперативних підрозділів, а забезпечує їх інформаційно-аналітичну підтримку шляхом застосування алгоритмізованих методів обробки значних обсягів інформації та формування відповідних аналітичних продуктів[2].

[1] Дуфенюк О. М. Невирішені проблеми та нові виклики використання кримінального аналізу оперативними підрозділами Національної поліції. *Аналітично-порівняльне правознавство.* 2025. Вип. 2. С. 995. DOI: https://doi.org/10.24144/2788-6018.2025.02.147.

[2] Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

1. Передумови виникнення та формування теоретико-методологічних засад кримінального аналізу в умовах цифровізації криміналістики

Розвиток кримінального аналізу пов'язаний із впровадженням концепції Intelligence-led policing, яка передбачає використання аналітичної інформації як основи для прийняття управлінських і оперативних рішень у сфері протидії злочинності. У межах даного підходу аналітичні продукти виступають інструментом визначення пріоритетів діяльності правоохоронних органів, оптимізації використання ресурсів і підвищення ефективності протидії кримінальним правопорушенням[3].

Подальший розвиток кримінального аналізу зумовлений процесами цифровізації, які сприяли переходу від аналізу окремих інформаційних фрагментів до комплексної обробки великих масивів даних з метою виявлення закономірностей, взаємозв'язків і тенденцій злочинної діяльності, що передбачає використання сучасних аналітичних методів, спрямованих на встановлення взаємозв'язків між подіями, суб'єктами, об'єктами та іншими елементами кримінально значущої інформації[4].

Водночас наукові дослідження Д. Худенка засвідчують наявність низки системних проблем, пов'язаних із нормативно-правовим, організаційним, технологічним та освітнім забезпеченням кримінального аналізу, а також необхідністю дотримання вимог законності та етичних стандартів під час використання інформації. В умовах подальшої цифровізації ці виклики набувають особливої актуальності, що обумовлює необхідність удосконалення теоретичних і методологічних засад кримінального аналізу як складової інформаційного забезпечення правоохоронної діяльності[5].

Таким чином, трансформація інформаційного середовища та зростання значення цифрових даних у кримінальному провадженні зумовлюють об'єктивну необхідність подальшого розвитку теоретичних і методологічних засад кримінального аналізу як системного інструменту інформаційно-аналітичного забезпечення правоохоронної діяльності в умовах цифровізації. У зв'язку з цим, особливого значення набуває методологічне обґрунтування процесу перетворення цифрових слідів на доказово значущу інформацію, що може бути використана у процесі прийняття процесуальних і управлінських рішень.

З огляду на це методологію кримінального аналізу доцільно розглядати як послідовний процес формування доказово релевантного знання на основі цифрових даних, що включає взаємопов'язані етапи їх отримання, збереження, обробки та інтерпретації. Зокрема, у структурі цифрових розслідувань доцільно виокремлювати послідовні етапи роботи з цифровою інформацією, кожен з яких виконує самостійну функцію у процесі формування доказово

[3] Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

[4] Там само.

[5] Худенко Д. Зміст, принципи і типології методів та інструментів кримінального аналізу. *Реалізація філософії Intelligence-led Policing в системі кримінального аналізу Національної поліції України* : монографія / за заг. ред. О. Є. Користіна. Київ : ВАІТЕ, 2024. С. 220. DOI: https://doi.org/10.36486/978-966-2310-66-5-18.

релевантного знання та забезпечує дотримання вимог процесуальної допустимості результатів.

1) Законний доступ до цифрової інформації та її фіксація. Початковий етап охоплює отримання доступу до цифрових даних на підставі визначених кримінальним процесуальним законодавством повноважень, а також їх первинну фіксацію із забезпеченням цілісності та незмінності інформаційного вмісту. Процесуальна значущість цього етапу полягає у забезпеченні автентичності цифрових даних шляхом створення їх достовірних копій, фіксації джерела походження, технічних параметрів носія та умов отримання інформації. Належна реалізація зазначених процедур забезпечує збереження доказових властивостей цифрової інформації та створює необхідні передумови для її подальшого використання у кримінальному провадженні.

2) Інженерна підготовка цифрових даних до аналітичного дослідження. Цей етап передбачає технічну обробку цифрових масивів з метою забезпечення їх структурної узгодженості, логічної впорядкованості та аналітичної придатності. Його зміст охоплює нормалізацію форматів даних, встановлення відповідностей між інформаційними об'єктами, синхронізацію часових характеристик, а також усунення технічних невідповідностей, які можуть впливати на коректність подальшого аналізу. Зазначені процедури забезпечують формування цілісного інформаційного середовища, придатного для застосування спеціалізованих методів кримінального аналізу.

3) Аналітична обробка цифрової інформації. На даному етапі здійснюється застосування формалізованих методів аналізу, спрямованих на встановлення структурних, функціональних і просторово-часових взаємозв'язків між об'єктами дослідження. Використання методів графового аналізу, просторово-часової кореляції, аналізу текстових масивів і алгоритмічних моделей обробки даних забезпечує можливість виявлення закономірностей, які не можуть бути встановлені шляхом безпосереднього спостереження. У результаті здійснюється трансформація первинних цифрових даних у структуровану аналітичну інформацію, що відображає об'єктивні характеристики досліджуваних процесів.

4) Інтерпретація результатів та формування аналітичного висновку – охоплює змістовне осмислення результатів аналітичної обробки з метою встановлення їх криміналістичного значення. Інтерпретація передбачає встановлення причинно-наслідкових зв'язків, визначення ролі окремих об'єктів у досліджуваних процесах, а також формування аналітичного продукту, який може використовуватися для інформаційно-аналітичного забезпечення кримінального провадження. Сформовані аналітичні висновки повинні характеризуватися логічною узгодженістю, обґрунтованістю та відповідністю вихідним даним.

5) Забезпечення процесуальної відтворюваності результатів. Завершальний етап спрямований на забезпечення можливості перевірки та підтвердження отриманих результатів. Він передбачає документування використаних методів і процедур, фіксацію характеристик інструментальних засобів, а також дотримання вимог щодо збереження цифрових даних і контролю їх цілісності. Забезпечення процесуальної відтворюваності є необхідною умовою використання результатів кримінального аналізу у процесі доказування, оскільки

дозволяє підтвердити їх достовірність, обґрунтованість і відповідність встановленим процесуальним вимогам.

Зазначена послідовність узгоджується з науково обґрунтованими методологічними підходами до проведення цифрових розслідувань, згідно з якими пріоритетним завданням є забезпечення цілісності та незмінності цифрової інформації у її первинному вигляді як необхідної умови подальшого аналітичного дослідження та використання отриманих результатів під час доказування у кримінальному провадженні[6].

Водночас ефективність кримінального аналізу безпосередньо залежить від характеристик цифрових даних, які виступають його інформаційною основою. Цифрові дані, що використовуються у кримінальному провадженні, характеризуються високим рівнем мінливості, залежністю від технічного середовища функціонування та підвищеною вразливістю до несанкціонованого втручання, що обумовлює необхідність забезпечення їх автентичності та незмінності. У наукових дослідженнях А.А. Шишенко підкреслюється, що саме забезпечення достовірності та цілісності цифрових доказів є ключовою передумовою їх процесуальної допустимості та подальшого використання в аналітичній діяльності. У зв'язку з цим аналітичні процедури повинні здійснюватися виключно на основі належним чином збережених, задокументованих і верифікованих даних, що забезпечує їх доказову значущість і можливість подальшої перевірки[7].

У даному контексті фундаментальною технічною передумовою забезпечення достовірності цифрових даних виступає гарантування їх цілісності. Науково-методичні рекомендації з питань збереження цифрових доказів визначають хешування цифрових образів і інших інформаційних об'єктів із використанням стандартизованих криптографічних алгоритмів як базовий механізм підтвердження їх незмінності. При цьому обов'язковою умовою є збереження контрольних хеш-значень окремо від відповідних цифрових файлів, що унеможливлює їх несанкціоновану модифікацію та забезпечує об'єктивний контроль цілісності інформації. У випадках відсутності вбудованих механізмів контролю цілісності у відповідних інформаційних системах, хеш-значення повинні фіксуватися і передаватися незалежно від суб'єкта проведення дослідження, що забезпечує дотримання принципу об'єктивності та прозорості процесу дослідження. Окреслені механізми формують необхідну технологічну та процесуальну основу для подальшого здійснення кримінального аналізу та забезпечення можливості судового контролю достовірності отриманих результатів[8].

---

[6] Lyle J. R., Guttman B., Butler J. M., Sauerwein K., Reed C., Lloyd C. E. Digital investigation techniques: a NIST scientific foundation review. Gaithersburg, MD : National Institute of Standards and Technology, 2022. 84 p. DOI: https://doi.org/10.6028/NIST.IR.8354.

[7] Shyshenko A. A. Digital evidences in criminal proceedings: problems of authenticity and admissibility. Випуск № 05, частина 3. 2025. С. 317. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.46

[8] Snyder J. M., Guttman B., Butler J. M., Farrell S. P., Reed C., Lloyd C. E. Digital evidence preservation and analysis: a NIST scientific foundation review. Gaithersburg, MD : National Institute of Standards and Technology, 2022. 102 p. DOI: https://doi.org/10.6028/NIST.IR.8387.

Цифровізація кримінальних проваджень зумовлює суттєву зміну підходів до збирання доказової інформації, що проявляється у зростанні частки віддалених джерел даних, зокрема кінцевих пристроїв (endpoint), корпоративних мережевих інфраструктур та хмарних сервісів. За таких умов фізичне вилучення матеріальних носіїв інформації часто є технічно неможливим або методологічно нераціональним, що обумовлює необхідність застосування процедур віддаленого збору цифрових даних. У науково-методичних рекомендаціях підкреслюється, що ефективність і процесуальна допустимість такого збору забезпечується за умови дотримання низки обов'язкових вимог, серед яких ключовими є наявність належних правових підстав для доступу до інформації, використання безпечних і відтворюваних методів збору, обов'язкове документування будь-яких змін, що можуть виникати у процесі отримання даних, урахування характеристик волатильних даних, включно з ключами шифрування та журналами системної активності, а також забезпечення контролю цілісності інформації шляхом хешування та ведення повного журналу процесу збору. Водночас, у наукових джерелах представлено різні моделі віддаленого збору цифрових даних, зокрема серверно-орієнтований, клієнтсько-орієнтований та мережево-орієнтований підходи, кожен з яких характеризується специфічними технічними обмеженнями та ризиками, пов'язаними, зокрема, з нестабільністю ідентифікаційних параметрів мережевих вузлів, обмеженнями пропускної здатності каналів зв'язку та особливостями режимів конфіденційності інформації[9].

Подальший розвиток цифрового кримінального аналізу безпосередньо пов'язаний із застосуванням сучасних аналітичних моделей, алгоритмів та технологій штучного інтелекту, що забезпечують можливість обробки значних обсягів різнорідної інформації та виявлення прихованих закономірностей. Одним із ключових напрямів є застосування графової аналітики та аналізу зв'язків, що передбачає формалізоване представлення об'єктів кримінального аналізу у вигляді вузлів (осіб, технічних пристроїв, облікових записів, фінансових інструментів) та зв'язків між ними (комунікацій, транзакцій, спільних подій). Використання графових характеристик, таких як центральність, щільність зв'язків, структурні позиції вузлів і мережеві кластери, дозволяє ідентифікувати організовані злочинні структури, встановлювати посередників та визначати ключові елементи злочинних мереж. Сучасні наукові дослідження підтверджують ефективність інтеграції графових методів із алгоритмами машинного навчання, що забезпечує підвищення точності класифікації об'єктів і виявлення аномальних патернів, зокрема у сфері фінансових правопорушень та злочинів, пов'язаних із використанням корпоративних структур[10].

Разом з цим, важливе значення має застосування методів обробки природної мови (Natural Language Processing, NLP), які забезпечують можливість аналізу значних масивів неструктурованих текстових даних, включно з процесуальними документами, службовими рапортами, електронними повідомленнями та

[9] Scientific Working Group on Digital Evidence. Best practices for remote collection of digital evidence from an endpoint. SWGDE, 2022. 18 p. URL: https://www.swgde.org

[10] Tiwari M., Gepp A., Kumar K. Using data analytics to distinguish legitimate and illegitimate shell companies. *Journal of Economic Criminology.* 2025. Vol. 7. Article 100123. DOI: https://doi.org/10.1016/j.jeconc.2024.100123.

інформацією з відкритих джерел. Результати систематичних наукових оглядів свідчать, що технології машинного навчання та NLP широко застосовуються у сфері правоохоронної діяльності для автоматизації аналітичних процедур, обробки інформаційних масивів, просторового аналізу кримінальної активності та прогнозування криміногенних тенденцій. Водночас наголошується на необхідності врахування ризиків, пов'язаних із можливістю відтворення алгоритмічними моделями структурних упереджень, притаманних вихідним даним, що обумовлює потребу у забезпеченні належного контролю, валідації та нормативного регулювання використання таких технологій у правоохоронній діяльності[11].

Розвиток технологій штучного інтелекту зумовлює розширення можливостей їх застосування у сфері кримінального аналізу, зокрема шляхом використання генеративних моделей і великих мовних моделей (Large Language Models, LLM), які забезпечують нові підходи до обробки та інтерпретації цифрової інформації. Функціональні можливості таких моделей дозволяють здійснювати автоматизований аналіз значних обсягів неструктурованих даних, включаючи текстові документи, електронну кореспонденцію, повідомлення з цифрових комунікаційних платформ та інші інформаційні масиви, що можуть містити криміналістично значущі відомості. Використання зазначених технологій сприяє підвищенню ефективності аналітичної діяльності шляхом автоматизації процесів класифікації інформації, виявлення змістових взаємозв'язків, узагальнення інформаційних масивів і формування аналітичних висновків.

Наукові дослідження зарубіжних учених M. Chernyshev, Z. Baig, N. Syed підтверджують можливість застосування генеративних моделей на різних етапах кримінального аналізу, включаючи первинне дослідження цифрових даних, їх аналітичну обробку та підготовку аналітичних матеріалів. Використання таких технологій дозволяє підвищити швидкість обробки інформації, зменшити навантаження на фахівців і забезпечити більш ефективне виявлення закономірностей у складних інформаційних структурах. Крім того, генеративні моделі можуть застосовуватися для структуризації інформації, узагальнення результатів аналізу та підтримки процесу прийняття аналітичних рішень, що сприяє підвищенню ефективності інформаційно-аналітичного забезпечення кримінального провадження.

Крім того, функціонування генеративних моделей ґрунтується на імовірнісних алгоритмах, що визначає їх обмеження з точки зору забезпечення доказової надійності отриманих результатів. Результати, сформовані такими моделями, є наслідком статистичного узагальнення наявних даних і не можуть розглядатися як самостійне джерело доказової інформації без їх перевірки та підтвердження іншими засобами, що обумовлює необхідність застосування генеративних моделей виключно як допоміжного інструменту аналітичної діяльності, результати якого підлягають обов'язковій перевірці, верифікації та процесуальному документуванню.

[11] Sarzaeim P., Mahmoud Q. H., Azim A., Bauer G., Bowles I. A systematic review of using machine learning and natural language processing in smart policing. *Computers*. 2023. Vol. 12, No. 12. Article 255. DOI: https://doi.org/10.3390/computers12120255.

Використання великих мовних моделей у кримінальному аналізі потребує забезпечення контролю за коректністю їх функціонування, документування умов їх застосування та перевірки достовірності отриманих результатів. Дотримання зазначених вимог забезпечує можливість інтеграції таких технологій у систему кримінального аналізу без порушення процесуальних стандартів доказування та створює передумови для їх ефективного використання як інструменту підвищення якості аналітичної діяльності. Таким чином, генеративні моделі штучного інтелекту можуть розглядатися як перспективний технологічний засіб підтримки кримінального аналізу, за умови забезпечення належного рівня методологічного контролю отриманих результатів[12].

У зв'язку з цим застосування технологій штучного інтелекту у кримінальному аналізі потребує впровадження системного підходу до управління ризиками, що забезпечує належний рівень надійності, безпеки та правомірності їх використання. Міжнародні стандарти визначають, що забезпечення довіреності систем штучного інтелекту повинно здійснюватися на основі комплексного управління ризиками, яке включає оцінювання валідності та надійності моделей, забезпечення їх прозорості, пояснюваності, підзвітності, захисту персональних даних і дотримання принципів справедливості. У процесі кримінального аналізу це передбачає чітке визначення допустимих сценаріїв використання алгоритмічних систем, здійснення постійного моніторингу їх точності та можливих похибок, забезпечення контролю з боку людини та належне документування характеристик моделей, використаних даних і результатів їх застосування, що забезпечує відповідність таких систем вимогам процесуальної допустимості та наукової обґрунтованості[13].

Отже, інтеграція сучасних методів віддаленого збору цифрових даних, алгоритмічних аналітичних інструментів і технологій штучного інтелекту формує нову методологічну основу кримінального аналізу, що забезпечує підвищення ефективності інформаційно-аналітичного забезпечення кримінального провадження за умови дотримання вимог достовірності, відтворюваності та процесуальної допустимості отриманих результатів.

2. Аналіз існуючих методів та формулювання завдання щодо вдосконалення аналітичних інструментів і підходів, що застосовуються у кримінальному аналізі в умовах цифрового середовища

Прикладні інструменти і платформи кримінального аналізу становлять ключовий технологічний компонент сучасного інформаційно-аналітичного забезпечення правоохоронної діяльності. Їх використання забезпечує можливість систематизованої обробки значних обсягів цифрових даних,

[12] Chernyshev M., Baig Z., Syed N., Doss R., Shore M. Large language models in digital forensics: capabilities, challenges and future directions. F*orensic Science International: Digital Investigation.* 2026. Vol. 56. Article 302043. DOI: https://doi.org/10.1016/j.fsidi.2025.302043.

[13] National Institute of Standards and Technology. Artificial intelligence risk management framework (AI RMF 1.0). Gaithersburg, MD : NIST, 2023. 48 p. DOI: https://doi.org/10.6028/NIST.AI.100-1.

встановлення взаємозв'язків між об'єктами кримінального аналізу, виявлення закономірностей злочинної діяльності та формування обґрунтованих аналітичних висновків. У наукових працях вітчизняних вчених зазначено, що ефективність кримінального аналізу безпосередньо залежить від функціональних можливостей інструментальних платформ, рівня їх технологічної інтеграції та відповідності вимогам достовірності, відтворюваності й процесуальної допустимості отриманих результатів[14].

З метою систематизації сучасного інструментарію кримінального аналізу доцільним є проведення їх порівняльного аналізу за функціональними, технологічними та методологічними характеристиками. Узагальнення результатів сучасних українських і міжнародних наукових досліджень, а також практичних рекомендацій у сфері цифрової криміналістики та кримінального аналізу, дозволяє виділити основні методи кримінального аналізу, що застосовуються в умовах цифрового середовища, їх функціональне призначення, інформаційну основу, аналітичні можливості та процесуальне значення (табл. 1).

Таблиця 1

Порівняння методів кримінального аналізу в цифровому середовищі

Метод кримінального аналізу	**Типові вхідні дані**	**Аналітичний продукт (вихід)**	**Методологічні переваги**
Аналіз зв'язків (link analysis, графовий аналіз)	Дані телекомунікацій (CDR), журнали месенджерів, фінансові транзакції, OSINT-дані, державні та корпоративні реєстри	Формалізовані графи зв'язків, визначення ролей суб'єктів, виявлення спільнот, ідентифікація ключових вузлів і посередників	Забезпечує виявлення прихованих структур взаємодії, підтримує розслідування організованої та серійної злочинної діяльності, дозволяє встановлювати ієрархію і функціональні ролі учасників
Просторово-часовий аналіз (spatio-temporal analysis)	Геопросторові дані (GPS, базові станції), часові мітки подій (timestamps), маршрути переміщення, журнали активності	Просторово-часові моделі, карти концентрації подій (hotspots), таймлайни, реконструкція маршрутів і послідовності подій	Забезпечує реконструкцію подій у часовому та просторовому вимірах, підтримує тактичне планування та встановлення закономірностей кримінальної активності

[14] Струков В. М., Узлов Д. Ю., Гнусов Ю. В. Інструментальні інтелектуальні платформи для кримінального аналізу. *Право і безпека.* 2021. № 4 (83). С. 72. DOI: https://doi.org/10.32631/pb.2021.4.07.

Продовження таблиці 1

Обробка природної мови (NLP) для аналізу текстових даних	Процесуальні документи, службові рапорти, електронні повідомлення, текстові масиви месенджерів, OSINT-джерела	Виділення сутностей і тематичних категорій, формування пошукових індексів, аналітичні витяги, встановлення змістових взаємозв'язків	Забезпечує масштабовану обробку неструктурованих текстових масивів, підвищує швидкість первинного аналізу інформації та ідентифікації релевантних даних
Методи машинного навчання (класифікація, виявлення аномалій)	Структуровані (табличні), графові та часові дані, цифрові журнали, транзакційні масиви	Класифікаційні моделі, оцінка ризиків, виявлення аномальних патернів, прогнозні аналітичні моделі	Забезпечує автоматизацію виявлення закономірностей і аномалій, підвищує ефективність пріоритизації об'єктів аналізу
Управління цифровими доказами (hashing, chain of custody)	Цифрові образи носіїв, файли, контейнери даних, журнали системної активності	Контрольні хеш-значення, довірені цифрові копії, задокументований ланцюг зберігання доказів	Забезпечує цілісність, автентичність і процесуальну допустимість цифрових доказів, створює основу для подальшого аналізу
Віддалений збір цифрових даних (endpoint, хмарні та мережеві системи)	Дані кінцевих пристроїв, серверів, хмарних сервісів, мережевих інфраструктур	Контейнери цифрових даних, журнали збору, зафіксовані цифрові образи	Забезпечує доступ до цифрових джерел без фізичного вилучення носіїв, дозволяє оперативно отримувати актуальні дані

Джерело: узагальнено автором на основі сучасних науково-методичних підходів до забезпечення цілісності цифрових доказів і застосування аналітичних методів у правоохоронній діяльності[15]

Представлена у табл. 1 систематизація методів кримінального аналізу в цифровому середовищі відображає методологічну основу обробки та інтерпретації цифрових даних у кримінальному провадженні. Водночас практична реалізація зазначених аналітичних підходів безпосередньо залежить від використання спеціалізованих програмних інструментів, які забезпечують технічну можливість збору, збереження, структуризації, аналізу та візуалізації цифрової інформації. Тобто, відповідні методи кримінального аналізу набувають прикладного значення лише за умови їх реалізації за допомогою

[15] Snyder J. M., Guttman B., Butler J. M., Farrell S. P., Reed C., Lloyd C. E. Digital evidence preservation and analysis: a NIST scientific foundation review. Gaithersburg, MD : National Institute of Standards and Technology, 2022. 102 p. DOI: https://doi.org/10.6028/NIST.IR.8387.

інструментальних платформ, що підтримують обробку великих масивів даних, управління цифровими доказами та формування аналітичних продуктів.

З наукової точки зору між методами кримінального аналізу та програмними засобами їх реалізації існує функціонально-інструментальна взаємозалежність, оскільки кожному аналітичному підходу відповідає певний клас програмного забезпечення, орієнтований на виконання конкретних завдань, зокрема аналіз зв'язків, просторово-часову реконструкцію подій, обробку текстових даних, управління цифровими доказами або проведення віддаленого збору інформації. У зв'язку з цим, програмні засоби виступають технологічним середовищем реалізації методології кримінального аналізу, забезпечуючи формалізацію аналітичних процедур, їх відтворюваність, документування та відповідність вимогам процесуальної допустимості.

Таким чином, після визначення основних методів кримінального аналізу в цифровому середовищі виникає необхідність систематизації інструментальних засобів, які забезпечують їх практичне застосування, що дозволяє встановити відповідність між аналітичними методами та класами програмного забезпечення, визначити їх функціональне призначення та роль у процесі цифрового криміналістичного дослідження.

З метою узагальнення сучасного інструментарію кримінального аналізу та цифрової криміналістики у таблиці 2 наведено порівняльну характеристику основних класів програмних інструментів і прикладів програмного забезпечення, що використовуються для реалізації відповідних аналітичних методів.

Таблиця 2

Порівняння класів інструментів і прикладів ПЗ, релевантних кримінальному аналізу та цифровій криміналістиці

Клас інструментальних засобів	**Типові приклади програмного забезпечення (не вичерпний перелік)**	**Функціональне призначення у кримінальному аналізі**	**Вимоги до забезпечення доказової надійності та контролю якості**
Інструменти графового аналізу зв'язків і OSINT-аналітики	Maltego; i2 Analyst's Notebook	Забезпечують візуалізацію та аналіз взаємозв'язків між об'єктами дослідження, інтеграцію інформації з різних джерел, ідентифікацію ключових суб'єктів, подій і структур взаємодії	Вимагають дотримання процедур документованого імпорту та конвертації даних, ведення журналів аналітичних трансформацій і забезпечення відтворюваності результатів; при роботі з великими масивами даних можливі обмеження масштабованості та необхідність експертної інтерпретації результатів

Продовження таблиці 2

Платформи мобільної криміналістики (витяг і аналіз цифрових даних)	UFED; Oxygen Forensic Detective; XRY; EnCase Mobile Investigator	Забезпечують вилучення цифрових даних з мобільних пристроїв, ідентифікацію та аналіз цифрових артефактів, що можуть використовуватися як джерела доказової інформації	Ключовими вимогами є незалежна валідація інструментів, підтвердження відтворюваності результатів та відповідність стандартизованим процедурам тестування; результати програм тестування (зокрема CFTT) використовуються для підтвердження надійності інструментів
Інформаційні системи управління кримінальними провадженнями (Case Management Systems, CMS)	Системи управління справами (CMS) як функціональний клас	Забезпечують централізоване управління матеріалами кримінальних проваджень, координацію діяльності слідчих і аналітичних підрозділів, управління доказами та аналітичною інформацією	Наукові дослідження підкреслюють необхідність інтеграції CMS із спеціалізованими аналітичними модулями, включно із засобами пошуку, обробки текстових даних і підтримки аналітичної діяльності; важливим є забезпечення цілісності даних і контролю доступу
Системи зберігання та управління цифровими доказами	Системи управління цифровими доказами (Evidence Management Systems); цифрові форензичні контейнери	Забезпечують довгострокове зберігання цифрових доказів, контроль доступу до них, аудит операцій і підтримку ланцюга зберігання доказів	Вимагають застосування криптографічних механізмів контролю цілісності (хешування, цифрового підпису), резервного копіювання, ведення журналів доступу та забезпечення процесуальної відтворюваності
Системи тестування та валідації криміналістичних інструментів	Методології та результати тестування CFTT (Computer Forensic Tool Testing)	Забезпечують оцінювання функціональних можливостей інструментів, визначення їх обмежень і підтвердження їх придатності для використання у криміналістичній практиці	Наявність стандартизованих процедур тестування, відкритих специфікацій і звітів про результати тестування підвищує рівень надійності інструментів і забезпечує доказову обґрунтованість результатів експертних досліджень

Систематизація інструментальних засобів кримінального аналізу та цифрової криміналістики, представлена у таблиці 2, відображає сучасну структуру технологічного забезпечення роботи з цифровою інформацією у кримінальному провадженні та демонструє функціональну диференціацію програмних інструментів відповідно до їх ролі у процесі обробки, аналізу та використання доказово значущих даних. Такий підхід дозволяє розглядати програмні засоби не ізольовано, а як взаємопов'язані компоненти єдиної інформаційно-аналітичної інфраструктури, що забезпечує реалізацію методології кримінального аналізу в умовах цифровізації правоохоронної діяльності.

Аналіз представлених у таблиці класів інструментальних засобів свідчить про те, що їх функціональне призначення охоплює всі ключові етапи роботи з цифровою інформацією, включаючи її отримання, структуризацію, аналітичну обробку, збереження та забезпечення процесуальної перевірюваності результатів. Така функціональна спеціалізація інструментів відповідає загальній логіці цифрового криміналістичного процесу, у межах якого формування доказово релевантної інформації здійснюється шляхом послідовного застосування технологічних процедур, спрямованих на забезпечення достовірності, цілісності та відтворюваності цифрових даних.

Особливого значення набувають інструментальні засоби, що забезпечують аналітичну обробку інформації, оскільки саме на цьому етапі здійснюється встановлення закономірностей, взаємозв'язків і структурних характеристик досліджуваних об'єктів. Використання відповідних програмних інструментів дозволяє здійснювати формалізований аналіз складних інформаційних масивів, інтегрувати дані з різних джерел та формувати обґрунтовані аналітичні висновки, які можуть використовуватися у процесі прийняття процесуальних і управлінських рішень. Водночас ефективність такого аналізу безпосередньо залежить від забезпечення прозорості аналітичних процедур, документування процесу обробки інформації та можливості незалежної перевірки отриманих результатів.

Важливим елементом технологічної інфраструктури кримінального аналізу є також програмні засоби, що забезпечують отримання та первинну обробку цифрових даних, оскільки саме на цьому етапі формується інформаційна основа для подальшої аналітичної діяльності. Надійність результатів кримінального аналізу значною мірою визначається коректністю процедур отримання цифрової інформації, дотриманням встановлених технічних і процесуальних вимог, а також забезпеченням можливості підтвердження автентичності та цілісності отриманих даних.

Окрему функціональну групу становлять інформаційні системи, що забезпечують організацію, управління та збереження цифрової інформації, які виконують роль технологічного середовища, у межах якого здійснюється інтеграція результатів кримінального аналізу у загальну систему кримінального провадження. Використання таких систем забезпечує централізоване управління інформаційними ресурсами, контроль доступу до них, документування операцій із цифровими даними та підтримку безперервності ланцюга їх обробки і використання.

Критично важливим компонентом забезпечення доказової надійності результатів кримінального аналізу є також застосування технологічних

механізмів, спрямованих на забезпечення цілісності цифрової інформації та підтвердження її незмінності. Використання відповідних механізмів дозволяє встановити відповідність досліджуваних даних їх первинному стану та забезпечити можливість підтвердження їх достовірності у процесі кримінального провадження, що створює необхідні передумови для використання результатів кримінального аналізу як доказово значущої інформації.

Водночас аналіз представленої класифікації свідчить про важливість забезпечення науково обґрунтованого використання програмних інструментів шляхом підтвердження їх функціональної придатності, визначення меж застосування та забезпечення відповідності встановленим технічним і методологічним вимогам. Застосування процедур тестування та валідації інструментальних засобів дозволяє мінімізувати ризики отримання недостовірних результатів і забезпечити належний рівень довіри до результатів аналітичної діяльності.

Таким чином, наведена систематизація інструментальних засобів підтверджує, що сучасний кримінальний аналіз у цифровому середовищі ґрунтується на комплексному використанні взаємопов'язаних технологічних рішень, які забезпечують повний цикл роботи з цифровою інформацією – від її отримання до формування аналітичних висновків, придатних для використання у кримінальному провадженні. Їх інтегроване застосування створює необхідні технологічні та процесуальні передумови для забезпечення обґрунтованості, достовірності та процесуальної допустимості результатів кримінального аналізу, що визначає їх ключову роль у сучасній системі інформаційно-аналітичного забезпечення правоохоронної діяльності.

З огляду на зазначене, використання цифрових інструментів кримінального аналізу має здійснюватися у межах визначених нормативно-правових рамок, що забезпечують законність, допустимість і доказову значущість результатів аналітичної діяльності. Відповідно, цифровізація кримінального аналізу повинна реалізовуватися з урахуванням процесуальних вимог кримінального процесуального законодавства, яке регламентує правові підстави, порядок та умови отримання, обробки, збереження і використання інформації у кримінальному провадженні. Дотримання зазначених вимог є необхідною передумовою забезпечення належності, допустимості та достовірності цифрової інформації як джерела доказів, а також гарантією можливості її використання у процесі доказування. Відповідно, особливого значення набуває забезпечення процесуальної форми роботи з цифровими даними, що передбачає належне документування всіх етапів їх отримання та обробки, фіксацію технічних характеристик використаних інструментів, а також створення умов для подальшої перевірки і відтворення отриманих результатів.

Особливого значення зазначені вимоги набувають в умовах правового режиму воєнного стану, який супроводжується внесенням змін до Кримінального процесуального кодексу України, зокрема запровадженням спеціального правового регулювання, передбаченого розділом IX-1 та статтею 615 КПК

України[16]. Окреслені нормативні положення спрямовані на забезпечення безперервності кримінального провадження в умовах підвищених ризиків втрати матеріалів, обмеженого фізичного доступу до документів і доказів, переміщення органів досудового розслідування, а також необхідності забезпечення оперативного реагування на кримінальні правопорушення. У таких умовах особливого значення набуває використання цифрових технологій, які забезпечують можливість дистанційного доступу до матеріалів кримінального провадження, їх збереження у захищених інформаційних системах і підтримання безперервності процесуальної діяльності незалежно від зовнішніх обставин.

Зазначені нормативні зміни обумовлюють необхідність впровадження технологічних рішень, спрямованих на забезпечення цілісності, доступності та захищеності цифрової інформації, що використовується у кримінальному провадженні, що включає використання спеціалізованих інформаційно-аналітичних систем, які забезпечують централізоване збереження даних, контроль доступу до них, фіксацію всіх операцій із цифровою інформацією та можливість відновлення даних у разі їх втрати або пошкодження. Даний підхід дозволяє мінімізувати ризики втрати доказової інформації та забезпечити належний рівень її процесуального захисту.

У зв'язку з цим цифровий кримінальний аналіз набуває особливого значення як інструмент забезпечення належного документування процесуальних дій, збереження цифрових доказів і підтримання безперервності ланцюга зберігання інформації. Його застосування дозволяє забезпечити фіксацію джерел походження цифрових даних, документування процедур їх обробки та збереження, а також створення умов для перевірки їх автентичності та цілісності, що, у свою чергу, забезпечує відповідність результатів кримінального аналізу вимогам кримінального процесуального законодавства та створює необхідні передумови для їх використання у процесі доказування.

Реалізація зазначених завдань обумовлює необхідність впровадження комплексних організаційно-технологічних заходів, зокрема процедур резервного копіювання цифрових даних, застосування механізмів контрольованого доступу до інформаційних ресурсів, використання захищених середовищ зберігання інформації та забезпечення можливості аудиту операцій із цифровими даними. Застосування таких механізмів дозволяє забезпечити належний рівень захисту інформації, її відтворюваність та процесуальну допустимість, що є необхідною умовою ефективного використання цифрового кримінального аналізу у кримінальному провадженні[17].

Важливим компонентом правового регулювання застосування цифрових інструментів кримінального аналізу є забезпечення захисту персональних даних, що обробляються у межах кримінального провадження. Закон України «Про

[16] Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

[17] Про внесення змін до Кримінального процесуального кодексу України щодо удосконалення порядку здійснення кримінального провадження в умовах воєнного стану : Закон України від 14.04.2022 № 2201-IX. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2201-20#Text

захист персональних даних» визначає базові принципи обробки персональної інформації, включно з принципами законності, цільового обмеження, пропорційності, мінімізації обсягу даних і забезпечення їх безпеки. З огляду на те, що кримінальний аналіз передбачає обробку значних масивів персональних даних, у тому числі чутливих категорій інформації, архітектура відповідних інформаційно-аналітичних систем повинна передбачати впровадження механізмів рольового розмежування доступу, ведення журналів доступу до інформації, аудиту операцій обробки даних і контролю передачі інформації між інформаційними системами. Забезпечення зазначених вимог є необхідною умовою правомірного використання цифрових аналітичних інструментів і гарантією дотримання прав і свобод людини у процесі здійснення кримінального провадження[18]. Водночас транснаціональний характер сучасного інформаційного середовища обумовлює необхідність узгодження національних правових механізмів із міжнародними стандартами отримання та використання електронних доказів. У зв'язку з цим особливого значення набуває дотримання міжнародних процедур отримання електронних доказів, які регламентують порядок формування, направлення та виконання відповідних запитів до іноземних суб'єктів і міжнародних провайдерів інформаційних послуг. Практичні рекомендації міжнародних організацій підкреслюють необхідність забезпечення належної процесуальної форми отримання електронних доказів, що включає обґрунтування запиту, визначення його правових підстав і забезпечення можливості подальшої процесуальної перевірки отриманої інформації[19].

Подальший розвиток міжнародно-правового регулювання у зазначеній сфері пов'язаний із прийняттям Другого додаткового протоколу до Конвенції про кіберзлочинність, відкритого для підписання у 2022 році, який спрямований на вдосконалення механізмів міжнародного співробітництва та підвищення ефективності процедур отримання електронних доказів. Приєднання держав до зазначеного протоколу відображає тенденцію до уніфікації процедур доступу до електронних доказів і гармонізації національних правових систем із міжнародними стандартами. Для України це створює необхідність адаптації національних процедур кримінального аналізу до міжнародних вимог, зокрема у частині забезпечення належного документування процесу отримання цифрових даних, дотримання ланцюга зберігання доказів, а також забезпечення пропорційності втручання у сферу приватності при отриманні та використанні електронної інформації[20]. Одним із напрямів реалізації зазначених вимог є використання інформації з відкритих цифрових джерел, яка може набувати значення доказової або орієнтуючої інформації у кримінальному провадженні.

[18] Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

[19] United Nations Office on Drugs and Crime. Electronic evidence. URL: https://www.unodc.org

[20] Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. *Council of Europe,* 2022. URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol

У сучасних умовах цифровізації кримінального провадження відкриті джерела інформації (Open Source Intelligence, OSINT) формують важливу інформаційну основу криміналістичного аналізу, зокрема у процесі розслідування міжнародних злочинів, включаючи воєнні злочини та порушення норм міжнародного гуманітарного права. Це обумовлено тим, що значний обсяг відомостей про події, їх обставини та причетних осіб об'єктивується у цифровому середовищі та фіксується у формі текстових повідомлень, аудіовізуальних матеріалів, геопросторових координат, службових метаданих та інших цифрових артефактів, які можуть бути використані для встановлення фактичних обставин кримінального правопорушення. Доступність таких даних у відкритому інформаційному просторі створює можливість їх оперативного отримання та використання для ідентифікації об'єктів аналізу, реконструкції послідовності подій і перевірки аналітичних та слідчих гіпотез.

Інформаційний потенціал відкритих цифрових ресурсів визначається також їх здатністю відображати події у часовому та просторовому вимірах, що дозволяє здійснювати просторово-часову кореляцію даних, встановлювати закономірності кримінально значущої активності та виявляти взаємозв'язки між окремими інформаційними елементами. Крім того, відкриті цифрові платформи можуть містити унікальні відомості, які не представлені у відомчих інформаційних системах правоохоронних органів, що розширює емпіричну базу кримінального аналізу та підвищує обґрунтованість аналітичних висновків.

Разом з тим використання інформації з відкритих джерел у кримінальному провадженні пов'язане з необхідністю забезпечення її процесуальної придатності, що передбачає належне документування обставин її отримання, фіксацію джерела походження, збереження технічних характеристик цифрових об'єктів та забезпечення можливості подальшої верифікації. Це обумовлено властивостями цифрової інформації, зокрема її мінливістю, залежністю від технічного середовища функціонування та потенційною вразливістю до модифікації або видалення, що може впливати на її доказову цінність.

У цьому аспекті визначального значення набуває застосування науково обґрунтованих методологічних підходів до роботи з відкритими джерелами інформації, які передбачають використання стандартизованих процедур збору, фіксації, збереження та аналітичної обробки цифрових даних. Реалізація зазначених процедур забезпечує відтворюваність аналітичних результатів, можливість їх незалежної перевірки та відповідність вимогам кримінального процесуального законодавства, що створює необхідні передумови для використання інформації з відкритих джерел як складової доказової бази або як аналітичного інструменту підтримки прийняття процесуальних рішень у кримінальному провадженні.

Міжнародні стандарти проведення цифрових розслідувань на основі відкритих джерел підкреслюють, що інформація, отримана із відкритих джерел, може виконувати як орієнтувальну функцію, сприяючи формуванню аналітичних версій, так і виступати самостійним джерелом доказової інформації, за умови дотримання вимог щодо її належного збору, верифікації, документування та збереження. На основі вищезазначеного, визначальним є забезпечення відтворюваності процедур отримання інформації, підтвердження

її походження, а також збереження метаданих і цифрових характеристик, що дозволяють перевірити її автентичність. Berkeley Protocol on Digital Open Source Investigations визначає систему принципів і процедур, спрямованих на забезпечення професіоналізації цифрових розслідувань, наголошуючи, що доказова значущість інформації з відкритих джерел визначається не технічними характеристиками використаних інструментів, а дотриманням уніфікованої методології збору, аналізу та документування інформації, що забезпечує її перевірюваність і процесуальну допустимість[21].

Подальший розвиток підходів до використання цифрових доказів у кримінальному провадженні пов'язаний із формуванням міжнародних стандартів оцінювання їх доказової надійності та допустимості. Зокрема, Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals акцентують увагу на необхідності забезпечення автентичності, достовірності та надійності цифрових даних як ключових умов їх використання у процесі доказування. У зв'язку з цим, результати кримінального аналізу повинні супроводжуватися належним документуванням джерел походження інформації, описом процедур її обробки та трансформації, підтвердженням цілісності даних, а також визначенням обмежень застосованих аналітичних методів, що забезпечує можливість незалежної перевірки отриманих результатів, що є необхідною умовою їх використання у кримінальному провадженні та підтвердження їх доказової значущості[22].

Крім того, розширення використання цифрових технологій у кримінальному аналізі, включаючи застосування систем штучного інтелекту, актуалізує питання забезпечення дотримання прав людини та етичних стандартів обробки інформації. Використання алгоритмічних систем для аналізу цифрових даних пов'язане з обробкою значних масивів персональної інформації, що обумовлює необхідність забезпечення законності, пропорційності та обґрунтованості відповідних процедур. У національних аналітичних документах підкреслюється, що впровадження технологій штучного інтелекту повинно здійснюватися з урахуванням принципів захисту прав людини, забезпечення прозорості функціонування алгоритмічних систем, запобігання необґрунтованому втручанню у приватне життя та забезпечення ефективного контролю за використанням таких технологій. Разом з тим, інформаційно-аналітичні системи, що застосовуються у кримінальному аналізі, повинні проєктуватися з урахуванням вимог захисту прав людини, включаючи механізми контролю доступу, аудиту операцій і оцінювання ризиків для прав і свобод людини, що забезпечує їх відповідність правовим і етичним стандартам сучасного цифрового суспільства[23].

---

[21] Office of the United Nations High Commissioner for Human Rights. The Berkeley protocol on digital open source investigations. New York ; Geneva : United Nations, 2024. 102 p. URL: https://www.ohchr.org

[22] Leiden University ; International Centre for Counter-Terrorism. Leiden guidelines on the use of digitally derived evidence in international criminal courts and tribunals. The Hague ; Leiden, 2022. 54 p. URL: https://leiden-guidelines.com

[23] Уповноважений Верховної Ради України з прав людини. Права людини в епоху штучного інтелекту : аналітична доповідь. Київ, 2023. 84 с. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/ПРАВА%20ЛЮДИНИ%20В%20ЕПОХУ%20ШТУЧНОГО%20ІНТЕЛЕКТУ_compressed.pdf

Міжнародні підходи до впровадження технологій штучного інтелекту у правоохоронній діяльності формують систему принципів, спрямованих на забезпечення їх правомірного, безпечного та відповідального використання. У відповідних настановах визначено ключові засади застосування систем штучного інтелекту, зокрема законність їх використання, мінімізацію потенційної шкоди, забезпечення збереження автономії людини у процесі прийняття рішень, дотримання принципів справедливості, прозорості та належного врядування. Особлива увага приділяється ризикам використання алгоритмічних систем прогнозування кримінальної активності (predictive policing), які можуть призводити до неефективного розподілу ресурсів правоохоронних органів, підвищення соціальної напруги та обмеження можливостей процесуального контролю внаслідок недостатньої прозорості алгоритмічних рішень. У сфері кримінального аналізу зазначені ризики мають принципове значення, оскільки результати аналітичної обробки даних можуть впливати на визначення пріоритетів розслідування, прийняття процесуальних рішень і стратегічне планування правоохоронної діяльності, що обумовлює необхідність забезпечення належного контролю за використанням відповідних технологій.

Важливим орієнтиром у формуванні нормативних засад використання штучного інтелекту у правоохоронній діяльності є правове регулювання Європейського Союзу, зокрема положення Регламенту (ЄС) 2024/1689 (AI Act), який встановлює ризик-орієнтований підхід до класифікації та регулювання систем штучного інтелекту. Зазначений підхід передбачає диференціацію систем залежно від рівня ризику, включаючи категорії неприйнятного ризику, застосування яких заборонено, та високого ризику, що підлягають посиленому регуляторному контролю. Особливого значення для правоохоронної діяльності набувають положення, що регламентують використання систем віддаленої біометричної ідентифікації у публічних просторах, застосування яких у режимі реального часу допускається лише за наявності чітко визначених правових підстав, процедур авторизації, документування та контролю. Крім того, нормативні вимоги передбачають обов'язкове забезпечення людського контролю за функціонуванням таких систем, ведення журналів їх використання та недопущення ухвалення рішень, що мають негативні правові наслідки для особи, виключно на основі автоматизованого аналізу. У цьому контексті положення AI Act можуть розглядатися як нормативно-правовий орієнтир для гармонізації національних підходів до використання штучного інтелекту та формування вимог до інформаційно-аналітичних систем, що застосовуються у кримінальному аналізі, зокрема у частині забезпечення прозорості, підзвітності, аудиту та контролю обмежень алгоритмічних моделей[24].

Разом з тим, з нормативним регулюванням застосування штучного інтелекту важливе значення має забезпечення належного рівня якості криміналістичної діяльності, що поширюється також на цифровий кримінальний аналіз як її складову. Нормативні підходи до регулювання судово-експертної діяльності

[24] European Commission. Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act). Brussels : European Commission, 2025. URL: https://ai-act-service-desk.ec.europa.eu

підкреслюють, що порушення вимог якості може призводити до необхідності перегляду значної кількості експертних висновків і результатів досліджень, що створює ризики для правомірності кримінального провадження. У зв'язку з цим особливого значення набуває впровадження систем управління якістю, які забезпечують стандартизацію процедур, контроль змін, документування процесів і забезпечення відтворюваності результатів. У межах кримінального аналізу це обумовлює необхідність включення аналітичних процедур, зокрема обробки даних, побудови аналітичних моделей та застосування алгоритмічних інструментів, до системи забезпечення якості аналітичної діяльності як складової процесу отримання та використання доказової інформації. Інтеграція аналітичних процедур до зазначеної системи передбачає здійснення контролю версій аналітичних інструментів, належне документування їх функціональних характеристик і змін, а також забезпечення можливості перевірки, відтворення та верифікації результатів аналітичної обробки даних. Реалізація зазначених вимог є необхідною умовою забезпечення процесуальної форми отримання інформації та гарантією її належності, допустимості й достовірності як джерела доказів у кримінальному провадженні. Дотримання цих вимог забезпечує можливість використання результатів кримінального аналізу у процесі доказування відповідно до положень кримінального процесуального законодавства[25].

Таким чином, міжнародні нормативні та методологічні підходи визначають комплекс вимог до впровадження систем штучного інтелекту та цифрових аналітичних інструментів у правоохоронній діяльності, що охоплює забезпечення законності, прозорості, контролю якості та процесуальної допустимості результатів, що є необхідною умовою їх ефективного та правомірного використання у кримінальному аналізі.

З урахуванням викладених теоретико-методологічних засад цифрового кримінального аналізу, а також нормативно-правових і технологічних вимог до роботи з цифровими доказами, подальший розвиток відповідних підходів потребує їх системного впровадження у практику діяльності органів досудового розслідування та судово-експертних установ. Ефективність цифрового кримінального аналізу визначається функціональними можливостями аналітичних інструментів та організаційною структурою взаємодії між суб'єктами кримінального провадження, архітектурою інформаційних систем, стандартизацією процедур обробки даних, а також рівнем інституційної та професійної готовності до їх використання.

У цьому контексті, визначальним напрямом підвищення ефективності цифрового кримінального аналізу є формування інтегрованої організаційної моделі його функціонування, яка забезпечує узгоджену взаємодію між усіма суб'єктами, залученими до процесу обробки, аналізу та використання криміналістично значущої інформації. Реалізація такої моделі передбачає відмову від ізольованого використання аналітичних інструментів у межах окремих структурних підрозділів і перехід до єдиної інформаційно-аналітичної

[25] Forensic Science Regulator. Forensic science activities: statutory code of practice. Version 2. London : Forensic Science Regulator, 2023. URL: https://www.gov.uk/government/publications/forensic-science-activities-statutory-code-of-practice-version-2

системи, що забезпечує централізоване накопичення, обробку та використання даних у межах кримінального провадження. Інтеграція інформаційних ресурсів і аналітичних можливостей створює передумови для забезпечення цілісності аналітичного процесу, підвищення узгодженості дій між підрозділами кримінального аналізу, органами досудового розслідування, кіберпідрозділами та експертними установами, а також підвищення обґрунтованості сформованих аналітичних висновків.

Результати наукових досліджень свідчать, що однією з основних перешкод ефективного використання кримінального аналізу в Україні залишається інституційна фрагментація інформаційних систем і відсутність уніфікованих процедур інформаційної взаємодії між різними суб'єктами правоохоронної діяльності. Така роз'єднаність обмежує можливості комплексного використання наявної інформації, ускладнює встановлення взаємозв'язків між окремими фактами та знижує ефективність аналітичної підтримки кримінального провадження[26]. Відсутність стандартизованих підходів до структурування інформації, ідентифікації об'єктів аналізу та документування результатів аналітичної діяльності ускладнює інтеграцію даних з різних джерел і створює ризики втрати або дублювання інформації.

Вирішення зазначених обмежень потребує впровадження уніфікованих протоколів інформаційної взаємодії, які забезпечують стандартизований обмін даними між інформаційними системами та структурними підрозділами. Стандартизація процедур обробки інформації передбачає встановлення єдиних вимог до формату представлення даних, ідентифікації об'єктів аналізу, структури аналітичних продуктів і порядку їх документування, що забезпечує сумісність інформаційних систем, можливість інтеграції різнорідних інформаційних ресурсів і створює необхідні умови для їх комплексного використання у кримінальному провадженні.

Формалізація структури аналітичних продуктів має принципове значення для забезпечення їх процесуальної придатності та практичного використання у діяльності органів досудового розслідування. Використання стандартизованих форматів аналітичних звітів забезпечує їх однозначність, логічну узгодженість і можливість перевірки обґрунтованості сформованих висновків, що також створює умови для їх інтеграції у матеріали кримінального провадження та використання як складової інформаційно-аналітичного забезпечення процесу доказування.

Запровадження інтегрованої організаційної моделі кримінального аналізу сприяє підвищенню ефективності використання інформаційних ресурсів, забезпечує узгодженість аналітичної діяльності та створює необхідні передумови для формування єдиного інформаційного простору правоохоронної діяльності.

Разом з організаційними аспектами визначальну роль відіграє формування належної технічної архітектури інформаційно-аналітичних систем, що

[26] Дуфенюк О. М. Невирішені проблеми та нові виклики використання кримінального аналізу оперативними підрозділами Національної поліції. *Аналітично-порівняльне правознавство.* 2025. Вип. 2. С. 993–1000. DOI: https://doi.org/10.24144/2788-6018.2025.02.147.

забезпечують підтримку кримінального аналізу. Сучасні вчені зазначають, що у сфері цифрових розслідувань традиційні системи управління кримінальними провадженнями ефективно виконують функції документування процесуальних дій і управління доказами, однак їх функціональні можливості є обмеженими у частині реалізації складних аналітичних процедур, спрямованих на виявлення закономірностей і формування аналітичних висновків. У зв'язку з цим обґрунтованим є застосування модульного підходу до побудови інформаційних систем, який передбачає функціональне розмежування інфраструктурних компонентів, відповідальних за збереження та управління доказовою інформацією, і аналітичних компонентів, призначених для обробки даних, виявлення взаємозв'язків та забезпечення підтримки прийняття процесуальних рішень. Застосування модульної архітектури інформаційних систем забезпечує підвищення гнучкості інформаційної інфраструктури, створює умови для здійснення контролю якості аналітичних процедур, а також сприяє зниженню ризиків технологічної залежності від окремих програмних рішень[27].

Крім того, необхідною умовою забезпечення доказової надійності результатів кримінального аналізу є впровадження стандартизованих процедур роботи з цифровими даними, які регламентують порядок доступу до інформації, її вилучення, збереження, обробки та подальшого використання у кримінальному провадженні. Зазначені процедури повинні передбачати обов'язкове документування правових підстав доступу до інформації, забезпечення цілісності цифрових даних шляхом використання криптографічних методів контролю, ведення журналів обробки даних і документування аналітичних трансформацій. Дотримання таких процедур забезпечує відтворюваність аналітичних результатів і створює необхідні передумови для їх використання як доказово значущої інформації.

Окремого значення набуває обґрунтований вибір програмних інструментів, що використовуються у цифровій криміналістиці та кримінальному аналізі. Аналіз наукових праць, присвячених впровадженню інноваційного програмного забезпечення у правоохоронну діяльність України, свідчить про широке застосування спеціалізованих програмних засобів для вилучення, обробки та аналізу цифрової інформації, що використовується як джерело доказів у кримінальному провадженні та сприяє підвищенню ефективності розслідування кримінальних правопорушень. Водночас у науковій літературі акцентується увага на необхідності забезпечення належної оцінки надійності зазначених програмних засобів, їх відповідності вимогам кримінального процесуального законодавства, а також можливості перевірки та відтворення результатів їх застосування. Дотримання цих вимог є необхідною умовою забезпечення належності, допустимості та достовірності цифрової інформації

[27] Skipanes M., Lorentzen J. P., Yayilgan S. Y. Understanding the role of case management systems in criminal investigations. *International Journal of Law, Crime and Justice.* 2026. Vol. 84. Article 100805. DOI: https://doi.org/10.1016/j.ijlcj.2025.100805.

як джерела доказів, а також гарантією її використання у процесі доказування відповідно до встановленої процесуальної форми[28].

Важливим фактором ефективного впровадження цифрового кримінального аналізу є також формування належного рівня професійної компетентності суб'єктів, які здійснюють відповідну діяльність. О. М. Дуфенюк у своєму дослідженні звертає увагу на наявність системних освітніх обмежень, що ускладнюють повноцінне застосування сучасних аналітичних інструментів у правоохоронній діяльності. Вчений обґрунтовує необхідність впровадження системної професійної підготовки фахівців, яка повинна охоплювати як формування базових компетентностей, пов'язаних із розумінням правової природи цифрових доказів і процесуальних вимог до їх використання, так і розвиток спеціалізованих навичок застосування сучасних аналітичних методів та забезпечення контролю якості аналітичної діяльності, що спрямовано на забезпечення правомірності використання цифрових аналітичних інструментів, а також належності, допустимості та достовірності доказової інформації у кримінальному провадженні[29].

З метою забезпечення належного рівня ефективності цифрового кримінального аналізу необхідним є впровадження формалізованої системи оцінювання його результативності, що ґрунтується на визначенні об'єктивних критеріїв якості аналітичної діяльності. Така система повинна охоплювати як технічні характеристики функціонування аналітичних інструментів, включаючи продуктивність обробки інформації та здатність працювати з великими масивами даних, так і змістовні параметри сформованих аналітичних продуктів, зокрема їх достовірність, повноту, логічну узгодженість і процесуальну придатність. Визначальним показником результативності кримінального аналізу виступає відповідність отриманих результатів вимогам кримінального процесуального законодавства, що регламентує порядок формування, фіксації та використання доказової інформації.

Методологічною основою оцінювання результативності є встановлення зв'язку між вихідними даними, застосованими аналітичними процедурами та отриманими результатами, що дозволяє підтвердити обґрунтованість аналітичних висновків. Необхідною умовою такого оцінювання є забезпечення відтворюваності аналітичних процедур, яка передбачає належне документування джерел інформації, використаних методів обробки та характеристик програмних інструментів. Це забезпечує можливість повторного проведення аналітичних процедур та перевірки коректності отриманих результатів незалежними суб'єктами.

Оцінювання результативності кримінального аналізу також повинно враховувати ступінь доказової значущості сформованих аналітичних продуктів,

[28] Aharkova O., Korosteleva L., Krasnopolskyi V. The use of innovative software packages in digital forensics to combat crime in Ukraine. *Science and Innovation*. 2025. Vol. 21, No. 6. P. 63. DOI: https://doi.org/10.15407/scine21.06.060.

[29] Дуфенюк О. М. Невирішені проблеми та нові виклики використання кримінального аналізу оперативними підрозділами Національної поліції. *Аналітично-порівняльне правознавство.* 2025. Вип. 2. С. 993–1000. DOI: https://doi.org/10.24144/2788-6018.2025.02.147.

яка визначається їх здатністю забезпечувати встановлення фактичних обставин кримінального правопорушення та підтвердження або спростування слідчих версій. Це передбачає перевірку відповідності аналітичних результатів критеріям допустимості, належності та достовірності доказів, а також їх узгодженості з іншими матеріалами кримінального провадження.

Впровадження системи об'єктивного оцінювання результативності цифрового кримінального аналізу забезпечує створення організаційно-методологічного механізму контролю якості аналітичної діяльності, спрямованого на стандартизацію процедур обробки цифрових даних і підвищення обґрунтованості аналітичних висновків. Застосування таких механізмів сприяє підвищенню рівня доказової надійності результатів кримінального аналізу та забезпечує можливість їх використання у кримінальному провадженні відповідно до встановлених процесуальних вимог.

ВИСНОВКИ

Узагальнення результатів дослідження дає підстави констатувати, що кримінальний аналіз у сучасних умовах цифровізації криміналістичної діяльності набуває статусу системоутворювального інструменту обробки, інтерпретації та використання цифрової інформації у кримінальному провадженні. Його сутність полягає у інтеграції процедур управління цифровими доказами, інженерії даних та застосування сучасних аналітичних методів, включаючи графовий аналіз, обробку текстової інформації та алгоритмічні моделі аналізу, що забезпечує формування обґрунтованих аналітичних продуктів, придатних для використання у процесуальній та управлінській діяльності. Встановлено, що кримінальний аналіз виконує не лише допоміжну функцію обробки інформації, але й виступає ключовим механізмом трансформації цифрових даних у доказово релевантні відомості, що можуть бути використані у процесі доказування та прийняття процесуальних рішень.

Водночас встановлено, що ефективність кримінального аналізу у цифровому середовищі безпосередньо залежить від забезпечення стандартизації та відтворюваності процедур роботи з цифровими даними. Доведено, що застосування механізмів контролю цілісності цифрової інформації, ведення журналів аналітичних операцій, а також валідація інструментальних засобів аналізу є необхідними умовами забезпечення доказової надійності отриманих результатів. Це обумовлено тим, що будь-які аналітичні висновки можуть набувати процесуального значення лише за умови забезпечення можливості перевірки їх походження, коректності та відповідності встановленим процедурним вимогам.

Окремо встановлено, що впровадження технологій штучного інтелекту у кримінальний аналіз створює значний потенціал для підвищення ефективності обробки цифрових даних, однак потребує дотримання принципів правомірності, прозорості, підзвітності та людського контролю. Обґрунтовано, що використання алгоритмічних моделей аналізу повинно здійснюватися у межах ризик-орієнтованого підходу, який передбачає оцінювання обмежень відповідних технологій, валідацію результатів їх функціонування та забезпечення процесуальних гарантій їх використання.

З’ясовано, що подальший розвиток кримінального аналізу в Україні потребує системної модернізації організаційних, технологічних і методологічних компонентів відповідної діяльності. Зокрема, визначальними напрямами розвитку є інтеграція аналітичної діяльності у загальну систему кримінального провадження, впровадження модульної архітектури інформаційно-аналітичних систем, стандартизація процедур роботи з цифровими доказами, забезпечення належного рівня професійної підготовки фахівців та впровадження механізмів контролю якості аналітичних процедур.

Таким чином, кримінальний аналіз у цифрову епоху виступає комплексним методологічним і прикладним інструментом цифровізації криміналістичної діяльності, який забезпечує підвищення ефективності кримінального провадження, зміцнення доказової бази та забезпечення відповідності правоохоронної діяльності сучасним технологічним і правовим вимогам.

АНОТАЦІЯ

У статті досліджено теоретико-прикладні засади кримінального аналізу як інструменту цифровізації сучасної криміналістики. Проаналізовано особливості становлення та розвитку кримінального аналізу в умовах трансформації інформаційного середовища та зростання ролі цифрових даних у кримінальному провадженні. Розглянуто концептуальні підходи до використання кримінального аналізу в системі інформаційно-аналітичного забезпечення правоохоронної діяльності, зокрема в контексті реалізації моделі intelligence-led policing. Визначено основні етапи роботи з цифровими даними у процесі кримінального аналізу, що включають отримання, збереження, обробку та інтерпретацію інформації. Охарактеризовано сучасні методи та інструменти кримінального аналізу, зокрема графовий аналіз зв’язків, просторово-часовий аналіз, обробку природної мови, методи машинного навчання та технології штучного інтелекту. Проведено систематизацію сучасних програмних інструментів і платформ, що використовуються для реалізації аналітичних процедур у цифровому середовищі, а також визначено їх функціональне призначення у кримінальному провадженні. Особливу увагу приділено питанням забезпечення цілісності цифрових доказів, процесуальної допустимості результатів кримінального аналізу та дотримання міжнародних стандартів роботи з цифровою інформацією. Обґрунтовано необхідність інтеграції аналітичних інструментів, стандартизації процедур роботи з цифровими даними та розвитку організаційно-технологічної інфраструктури кримінального аналізу. Зроблено висновок про те, що впровадження сучасних цифрових технологій, алгоритмічних моделей та інструментів штучного інтелекту створює передумови для підвищення ефективності інформаційно-аналітичного забезпечення правоохоронної діяльності та формування нових підходів до криміналістичного дослідження цифрових доказів.

Література

1. Дуфенюк О. М. Невирішені проблеми та нові виклики використання кримінального аналізу оперативними підрозділами Національної поліції.

Аналітично-порівняльне правознавство. 2025. Вип. 2. С. 993–1000. DOI: https://doi.org/10.24144/2788-6018.2025.02.147.

2. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 02.03.2026).

3. Про внесення змін до Кримінального процесуального кодексу України щодо удосконалення порядку здійснення кримінального провадження в умовах воєнного стану : Закон України від 14.04.2022 № 2201-IX. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2201-20#Text (дата звернення: 02.03.2026).

4. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 02.03.2026).

5. Струков В. М., Узлов Д. Ю., Гнусов Ю. В. Інструментальні інтелектуальні платформи для кримінального аналізу. *Право і безпека.* 2021. № 4 (83). С. 64–79. DOI: https://doi.org/10.32631/pb.2021.4.07.

6. Уповноважений Верховної Ради України з прав людини. Права людини в епоху штучного інтелекту : аналітична доповідь. Київ, 2023. 84 с. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/ПРАВА%20ЛЮДИНИ%20В%20ЕПОХУ%20ШТУЧНОГО%20ІНТЕЛЕКТУ_compressed.pdf (дата звернення: 02.03.2026).

7. Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

8. Худенко Д. Зміст, принципи і типології методів та інструментів кримінального аналізу. *Реалізація філософії Intelligence-led Policing в системі кримінального аналізу Національної поліції України* : монографія / за заг. ред. О. Є. Користіна. Київ : ВАІТЕ, 2024. С. 215–235. DOI: https://doi.org/10.36486/978-966-2310-66-5-18.

9. Aharkova O., Korosteleva L., Krasnopolskyi V. The use of innovative software packages in digital forensics to combat crime in Ukraine. *Science and Innovation.* 2025. Vol. 21, No. 6. P. 60–67. DOI: https://doi.org/10.15407/scine21.06.060.

10. Chernyshev M., Baig Z., Syed N., Doss R., Shore M. Large language models in digital forensics: capabilities, challenges and future directions. F*orensic Science International: Digital Investigation.* 2026. Vol. 56. Article 302043. DOI: https://doi.org/10.1016/j.fsidi.2025.302043.

11. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. *Council of Europe,* 2022. URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol (дата звернення: 02.03.2026).

12. European Commission. Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act). Brussels : European Commission, 2025. URL: https://ai-act-service-desk.ec.europa.eu (дата звернення: 02.03.2026).

13. Forensic Science Regulator. Forensic science activities: statutory code of practice. Version 2. London : Forensic Science Regulator, 2023. URL:

https://www.gov.uk/government/publications/forensic-science-activities-statutory-code-of-practice-version-2 (дата звернення: 02.03.2026).

14. Leiden University; International Centre for Counter-Terrorism. Leiden guidelines on the use of digitally derived evidence in international criminal courts and tribunals. The Hague ; Leiden, 2022. 54 p. URL: https://leiden-guidelines.com (дата звернення: 02.03.2026).

15. Lyle J. R., Guttman B., Butler J. M., Sauerwein K., Reed C., Lloyd C. E. Digital investigation techniques: a NIST scientific foundation review. Gaithersburg, MD : National Institute of Standards and Technology, 2022. 84 p. DOI: https://doi.org/10.6028/NIST.IR.8354.

16. National Institute of Standards and Technology. Artificial intelligence risk management framework (AI RMF 1.0). Gaithersburg, MD : NIST, 2023. 48 p. DOI: https://doi.org/10.6028/NIST.AI.100-1.

17. Office of the United Nations High Commissioner for Human Rights. The Berkeley protocol on digital open source investigations. New York ; Geneva : United Nations, 2024. 102 p. URL: https://www.ohchr.org (дата звернення: 02.03.2026).

18. Sarzaeim P., Mahmoud Q. H., Azim A., Bauer G., Bowles I. A systematic review of using machine learning and natural language processing in smart policing. *Computers*. 2023. Vol. 12, No. 12. Article 255. DOI: https://doi.org/10.3390/computers12120255.

19. Scientific Working Group on Digital Evidence. Best practices for remote collection of digital evidence from an endpoint. SWGDE, 2022. 18 p. URL: https://www.swgde.org (дата звернення: 02.03.2026).

20. Shyshenko A. A. Digital evidences in criminal proceedings: problems of authenticity and admissibility // Випуск № 05, частина 3. 2025. С. 315–321. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.46

21. Skipanes M., Lorentzen J. P., Yayilgan S. Y. Understanding the role of case management systems in criminal investigations. *International Journal of Law, Crime and Justice*. 2026. Vol. 84. Article 100805. DOI: https://doi.org/10.1016/j.ijlcj.2025.100805.

22. Snyder J. M., Guttman B., Butler J. M., Farrell S. P., Reed C., Lloyd C. E. Digital evidence preservation and analysis: a NIST scientific foundation review. Gaithersburg, MD : National Institute of Standards and Technology, 2022. 102 p. DOI: https://doi.org/10.6028/NIST.IR.8387.

23. Tiwari M., Gepp A., Kumar K. Using data analytics to distinguish legitimate and illegitimate shell companies // Journal of Economic Criminology. 2025. Vol. 7. Article 100123. DOI: https://doi.org/10.1016/j.jeconc.2024.100123.

24. United Nations Office on Drugs and Crime. Electronic evidence. URL: https://www.unodc.org (дата звернення: 02.03.2026).

Information about the author:
Vasylova Oksana Vasylivna,
Candidate of Law Sciences,
Associate Professor at the Department of Criminal Law,
Yuriy Fedkovych Chernivtsi National University
2, Kotsiubynskoho, Chernivtsi, 58012 , Ukraine