національних інтересів України: монографія. Тернопіль: Новий колір. 2016. 812 с.

4. Гур'єв В.І., Мехед Д.Б. та ін. Інформаційна безпека держави. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея». 2018. 166 с.

5. Шатун В.Т., Гладун О.В. Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці. Державне управління*. 2016. Вип. 255, том 267, С. 174-180

6. Носок С.О., Коломицев М.В., Стьопочкіна І.В. Управління інформаційною безпекою. Київ: КПІ ім. Ігоря Сікорського. 2025, 88 с.

УДК 343.9

Василова О. В.
к.ю.н., асистент кафедри кримінального права,
Чернівецький національний університет
імені Юрія Федьковича

АНАЛІТИЧНІ ІНСТРУМЕНТИ КРИМІНАЛЬНОГО АНАЛІЗУ

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, 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 [1].

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
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	Цифрові образи носіїв, файли,	Контрольні хеш-значення, довірені	Забезпечує цілісність, автентичність і

доказами (hashing, chain of custody)	контейнери даних, журнали системної активності	цифрові копії, задокументований ланцюг зберігання доказів	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 [2].

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 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.

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.

ЛІТЕРАТУРА:

1. 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.
2. 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.
3. 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.
4. Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.
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. 215–235. DOI: https://doi.org/10.36486/978-966-2310-66-5-18.

УДК 340.1

Антюк І.П.
викладач кафедри кримінального права та процесу
Західноукраїнського національного університету

ДЕЯКІ ПИТАННЯ ОЗНАЙОМЛЕННЯ СТОРОНИ ЗАХИСТУ ІЗ МАТЕРІАЛАМИ ДОСУДОВОГО РОЗСЛІДУВАННЯ

Частиною 1 ст.290 КПК України передбачено, що визнавши зібрані під час досудового розслідування докази достатніми для складання обвинувального акта, клопотання про застосування примусових заходів медичного або виховного характеру прокурор або слідчий за його дорученням зобов'язаний повідомити підозрюваному, його захиснику, законному представнику та захиснику особи, стосовно якої передбачається застосування примусових заходів медичного чи виховного характеру, про завершення досудового розслідування та надання доступу до матеріалів досудового розслідування [1].

Відповідно до ч.ч.2, 3 ст. 290 КПК України прокурор або слідчий за його дорученням зобов'язаний надати доступ до матеріалів досудового розслідування, які є в його розпорядженні. Прокурор або слідчий за його дорученням зобов'язаний надати доступ та можливість скопіювати або відобразити відповідним чином будь-які речові докази або їх частини, документи або копії з них, а також надати доступ до приміщення або місця,