ISSN 2524-0374

УДК 343.98:004.056:004.8
DOI https://doi.org/10.32782/2524-0374/2025-11/74

МЕТОДОЛОГІЯ КРИМІНАЛЬНОГО АНАЛІЗУ В УМОВАХ ЗРОСТАННЯ КІБЕРЗАГРОЗ

METHODOLOGY OF CRIMINAL ANALYSIS IN THE CONTEXT OF INCREASING CYBER THREATS

Форос Г.В., к.ю.н., доцент,
завідувачка кафедри кримінального аналізу та інформаційних технологій
Одеський державний університет внутрішніх справ
orcid.org/0000-0002-9504-3681

Калугін В.Ю., к.ю.н., доцент,
професор кафедри кримінального аналізу та інформаційних технологій
Одеський державний університет внутрішніх справ
orcid.org/0000-0002-2950-2763

Грезіна О.М., доктор філософії,
доцент кафедри кримінального аналізу та інформаційних технологій
Одеський державний університет внутрішніх справ
orcid.org/0000-0002-2491-6529

У статті розглянуто трансформацію методології кримінального аналізу в умовах зростання кіберзагроз, зумовлену цифровізацією суспільства, ескалацією кіберзлочинності та активним використанням злочинцями сучасних інформаційних технологій, зокрема штучного інтелекту та машинного навчання. Проаналізовано динаміку кіберзлочинів у світі та в Україні, з акцентом на виклики, що виникають у період повномасштабної збройної агресії та зростання кількості атак на об'єкти критичної інфраструктури.

Обґрунтовано обмеженість традиційних реактивних підходів до кримінального аналізу та необхідність переходу до проактивних і прогностичних моделей. Значну увагу приділено ролі цифрової криміналістики як ключового елемента сучасного кримінального аналізу, зокрема комп'ютерної, мобільної та мережевої криміналістики, а також особливостям роботи з великими обсягами цифрових доказів, шифруванням і технологіями анти-криміналістики. Розглянуто технічні, правові та етичні виклики, пов'язані з транскордонним характером кіберзлочинності та застосуванням автоматизованих аналітичних інструментів.

Проаналізовано можливості інтеграції штучного інтелекту, машинного навчання та генеративних моделей у процеси виявлення, аналізу та прогнозування кіберзагроз, зокрема у сфері боротьби з фішингом, вторгненнями в мережі та автоматизованими атаками. На основі міжнародного й національного досвіду сформульовано рекомендації щодо вдосконалення методології кримінального аналізу, розвитку міжвідомчої та міжнародної співпраці, а також підвищення професійної підготовки фахівців правоохоронних органів.

Ключові слова: кримінальний аналіз, кіберзагрози, кіберзлочинність, цифрова криміналістика, штучний інтелект, машинне навчання, прогностична аналітика, кібербезпека.

The article examines the transformation of criminal analysis methodology under conditions of increasing cyber threats driven by the digitalization of society, the escalation of cybercrime, and the active use of modern information technologies by offenders, particularly artificial intelligence and machine learning. The dynamics of cybercrime at the global level and in Ukraine are analyzed, with a focus on the challenges arising during the period of full-scale armed aggression and the growing number of attacks on critical infrastructure facilities.

The limitations of traditional reactive approaches to criminal analysis are substantiated, along with the need to transition to proactive and predictive models. Particular attention is paid to the role of digital forensics as a key component of modern criminal analysis, including computer, mobile, and network forensics, as well as the specifics of handling large volumes of digital evidence, encryption, and anti-forensic technologies. Technical, legal, and ethical challenges associated with the transnational nature of cybercrime and the use of automated analytical tools are also considered.

The possibilities of integrating artificial intelligence, machine learning, and generative models into the processes of detecting, analyzing, and forecasting cyber threats are analyzed, particularly in combating phishing, network intrusions, and automated attacks. Based on international and national experience, recommendations are formulated to improve criminal analysis methodology, enhance interagency and international cooperation, and increase the professional training of law enforcement specialists.

Key words: criminal analysis, cyber threats, cybercrime, digital forensics, artificial intelligence, machine learning, predictive analytics, cybersecurity.

Постановка проблеми. Постановка проблеми. Суспільні процеси на нинішньому етапі розвитку відзначаються інтенсивною цифровізацією та ескалацією кіберзлочинних проявів. За даними дослідження, опублікованого у 2023 році, глобальні збитки від кіберзлочинності можуть досягти 10,5 трильйонів доларів США на рік до 2025 року, що значно перевищує показник у 3 трильйони доларів у 2015 році. В Україні ситуація особливо загострилася в умовах повномасштабної війни, коли у першому кварталі 2025 року зафіксовано 341 підтверджений кіберінцидент та близько 6 тисяч критичних подій у сфері кібербезпеки [1]. За даними Держспецзв'язку України, у 2023 році кількість кібератак зросла на 15,9% порівняно з 2022 роком, досягнувши 2543 інцидентів [13]. Традиційні методи кримінального аналізу, які базувалися на реактивному підході та мануальному опрацюванні доказів, виявилися неефективними у боротьбі з сучасними кіберзагрозами. Зростання обсягів цифрових даних, швидкість поширення кібератак, транснаціональний характер злочинів та використання злочинцями передових технологій, включаючи штучний інтелект, вимагають кардинального перегляду методології кримінального аналізу. Особливої актуальності ця проблема набуває в контексті того, що кіберзлочинці все частіше застосовують методи

машинного навчання для створення складних фішингових схем, дипфейків та автоматизованих атак.

Мета дослідження. Метою статті є аналіз сучасних методів та інструментів кримінального аналізу в умовах зростання кіберзагроз, дослідження інноваційних підходів до виявлення, розслідування та запобігання кіберзлочинам, а також формулювання рекомендацій щодо вдосконалення методології кримінального аналізу з урахуванням викликів цифрової епохи.

Аналіз останніх публікацій. Проблематика кримінального аналізу в контексті кіберзагроз активно досліджується як вітчизняними, так і зарубіжними науковцями. У 2022 році Департамент оперативно-розшукової діяльності опублікував фундаментальне видання, присвячене теоретичним та практичним аспектам здійснення кримінального аналізу, де описано основні алгоритми роботи кримінального аналітика в оперативних підрозділах, а також методики роботи із сучасним програмним забезпеченням та інформаційними ресурсами [2]. Дослідження 2023 року, опубліковане в журналі Sensors, присвячене застосуванню штучного інтелекту в кібербезпеці, демонструє, що ШІ-системи здатні аналізувати великі обсяги даних у реальному часі, виявляючи підозрілі патерни та шкідливе програмне забезпечення, що значно підвищує ефективність кримінального аналізу [3]. У 2024 році вчені з Університету Оксфорда та Університету Нового Південного Уельсу оприлюднили перший Світовий індекс кіберзлочинності, згідно з яким Україна посіла друге місце після Росії, що підкреслює масштабність проблеми для нашої держави [7]. Важливий внесок у розвиток методології цифрової криміналістики зробили дослідники, які у 2025 році опублікували комплексний аналіз ролі штучного інтелекту та машинного навчання в сучасній цифровій криміналістиці [4]. Їхнє дослідження показало, що автоматизація процесів збору та аналізу доказів значно підвищує швидкість та точність розслідувань [4]. У роботі 2024 року, присвяченій цифровій криміналістиці як інструменту боротьби з сучасними кіберзлочинами, наголошується на необхідності інтеграції блокчейн-криміналістики, інструментів автоматизації та квантово-стійких методів для підвищення ефективності розслідувань [19]. Українські науковці також активно досліджують цю проблематику. У 2024 році в журналі UNIVERSUM опубліковано статтю, присвячену методам кримінального аналізу, де автори розглядають теоретичні та практичні аспекти збору та аналізу доказів, профілювання злочинів, використання технічних засобів та сучасних технологій [6]. Дослідження 2025 року, представлене на міжнародній науково-практичній конференції в Кам'янець-Подільському, висвітлює роль сучасних інформаційних технологій у діяльності поліції, включаючи ГІС та аналіз злочинності [14].

Виклад основного матеріалу. Кримінальний аналіз традиційно визначається як інтелектуально-логічна діяльність працівників правоохоронних органів, що полягає у пошуку, перевірці й оцінці інформації, яка має значення для розкриття злочинів та їхньої профілактики [2]. Однак цифрова трансформація суспільства докорінно змінила природу злочинності та вимоги до методології її аналізу.

За міжнародними стандартами, кримінальний аналіз – це застосування формальних аналітичних та статистичних методів, а також методології до вивчення злочинності [10]. Сучасний кримінальний аналіз у сфері кіберзагроз повинен охоплювати не лише традиційні методи, але й інноваційні підходи, що базуються на цифрових технологіях. Кіберзагрози визначаються як протиправні карні дії суб'єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства та держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [9]. Основними видами загроз є шкідливе програмне забезпечення, програми-вимагачі, фішинг, внутрішні загрози та DDoS-атаки [9].

Цифрова криміналістика стала ключовим елементом методології кримінального аналізу кіберзлочинів. Згідно з дослідженням 2025 року, процес цифрової криміналістики включає кілька етапів: ідентифікацію потенційних джерел цифрових доказів (комп'ютери, смартфони, планшети, сервери), збереження даних без їх зміни, аналіз зібраної інформації та презентацію результатів у форматі, придатному для судового розгляду [12].

Сучасна методологія цифрової криміналістики охоплює декілька спеціалізованих напрямків. Комп'ютерна криміналістика зосереджена на аналізі дискових накопичувачів та метаданих для відстеження активності користувачів, відновлення видалених даних та виявлення несанкціонованого доступу [12]. Мобільна криміналістика стикається з особливими викликами через різноманітність пристроїв, операційних систем та можливості віддаленого видалення даних [12]. Мережева криміналістика передбачає запис та аналіз пакетів даних для виявлення вторгнень та підозрілої активності [12].

У дослідженні Soni N. 2025 року виділяється три основні категорії викликів у цифровій криміналістиці: технічні виклики (управління великими обсягами даних, шифрування та обфускація, нові технології IoT та блокчейн), юридичні виклики (транскордонні розслідування, прийнятність доказів, проблеми конфіденційності) та етичні виклики (упередженість ШІ-інструментів, баланс між розслідуванням та правами особи) [12].

Інтеграція штучного інтелекту та машинного навчання революціонізувала методологію кримінального аналізу кіберзлочинів. У дослідженні A. Djenna, E. Barka, A. Benchikh, K. Khadir ШІ-системи здатні аналізувати дані в реальному часі на масштабах, недосяжних для людини, швидко ідентифікуючи підозрілі тенденції та шкідливе програмне забезпечення [3].

Прогностична аналітика на основі ШІ дозволяє передбачати потенційні загрози на підставі історичних тенденцій. Моделі машинного навчання аналізують великі набори даних з різних джерел, включаючи попередні звіти про інциденти, журнали безпеки та патерни мережевого трафіку, виявляючи тренди та закономірності [16]. Системи можуть використовувати ці тренди для прогнозування того, коли та як відбудуться майбутні загрози, встановлюючи автоматизацію як превентивний захід ще до матеріалізації загрози [16].

У дослідженні Nachaat Mohamed 2025 року демонструється ефективність конволюційних нейронних мереж у виявленні вторгнень та підвищенні безпеки мережі [20]. ШІ-інструменти автоматично визначають, чи є спроба входу в систему справжньою, допомагаючи запобігати таким тактикам кіберзлочинності, як атаки грубої сили та підміна облікових даних [20]. У сфері захисту електронної пошти ШІ аналізує контент та контекст повідомлень для швидкого виявлення ознак фішингу, таких як підроблення електронної пошти та неправильно написані доменні імена [17].

Генеративний ШІ виступає потужним союзником у боротьбі з кіберзагрозами, створюючи реалістичні симуляції, прогнозуючи сценарії атак та покращуючи виявлення загроз [18]. Він може генерувати синтетичні дані, що імітують реальні патерни атак, розширюючи навчальні дані для моделей машинного навчання та покращуючи їхню здатність ідентифікувати навіть тонкі або нові загрози [18].

Незважаючи на значний прогрес, методологія кримінального аналізу кіберзлочинів стикається з численними викликами. У статті Kevin Poireault зазначається, що кіберзлочинці швидко адаптуються до нових захисних технологій, використовуючи власні ШІ-інструменти для створення більш складних атак [4]. За даними звіту

SlashNext State of Phishing Report 2023, кількість шкідливих фішингових електронних листів зросла на 1265% з четвертого кварталу 2022 року, значною мірою через використання ШІ-інструментів [17].

Важливою проблемою залишається транснаціональний характер кіберзлочинності. Кіберзлочинці можуть діяти з будь-якої точки світу, а жертви можуть перебувати в іншій країні, що створює юрисдикційні конфлікти та ускладнює розслідування [7]. В українських реаліях доступ до документів та речей підозрюваних здійснюється відповідно до статті 159 Кримінального процесуального кодексу України, що може не завжди відповідати швидкості, необхідній для розслідування кіберзлочинів [5].

У своєму дослідженні Sarker та співавтори виявляють проблему роботи з величезними обсягами цифрових доказів, шифруванням, що ускладнює аналіз, та технологіями анти-криміналістики, які використовують злочинці для приховування слідів [11]. Середня вартість витоку даних у 2023 році становила 4,45 мільйона доларів США, що на 15% перевищує показники останніх трьох років, що свідчить про зростаючу складність та вартість кіберінцидентів.

Для підвищення ефективності кримінального аналізу в умовах зростання кіберзагроз необхідна інтеграція декількох інноваційних підходів. У дослідженні The Role of Artificial Intelligence and Machine Learning in Enhancing Cybersecurity against Cybercrime рекомендується використання прогностичного аналізу на основі ШІ для попередження злочинів, впровадження систем раннього попередження про нові кіберзагрози та застосування поведінкової аналітики для виявлення підозрілої поведінки [16].

Важливим напрямком є розвиток міжвідомчої та міжнародної співпраці. Проєкт CyberUA Ради Європи, який діє в Україні з 2025 року, спрямований на покращення обробки електронних доказів для використання в кримінальних провадженнях, пов'язаних з воєнними злочинами та грубими порушеннями прав людини в контексті російської агресії проти України [15]. Проєкт зміцнює можливості кримінального правосуддя українських правоохоронних органів, прокурорів та судової системи щодо роботи з електронними доказами [15].

Тактичний кримінальний аналіз повинен включати аналіз криміногенної ситуації на конкретній території за невеликий проміжок часу, встановлення тенденцій злочинності, визначення місць концентрації вчинення злочинів та профілювання підозрюваних [8]. Стратегічний кримінальний аналіз спрямований на виявлення тенденцій, закономірностей та прогнозування розвитку ситуації за великий період часу, що дозволяє приймати стратегічні управлінські рішення щодо розподілу сил та засобів [8].

У першому кварталі 2025 року Система виявлення вразливостей України здійснила аналіз понад 2,7 мільйонів подій [1]. Найпоширенішими типами атак були сканування мереж, спроби експлуатації вразливостей, з'єднання зі шкідливими ресурсами та зараження шкідливим програмним забезпеченням [1]. Частина атак була здійснена організованими проросійськими хакерськими угрупованнями, такими як UAC-0010, UAC-0202, UAC-0006, основною метою яких залишаються державні установи та об'єкти критичної інфраструктури [1].

Львівська обласна військова адміністрація у межах реалізації державної політики кібербезпеки запровадила комплексний підхід до захисту інформаційних систем [1]. Інтеграція в Системою виявлення вразливостей дозволила запровадити проактивну модель кіберзахисту, коли загрози виявляються до того, як вони призводять до інцидентів [1]. Регулярний аналіз подій, аудит вразливостей та тісна співпраця з фахівцями Державного центру кіберзахисту стали частиною щоденної роботи [1]. Згідно з дослідженням 2023 року, Департамент кіберполіції Національної поліції України відповідає за реалізацію державної політики у боротьбі з кіберзлочинністю та організовує й проводить оперативно-розшукову діяльність [13]. Департамент також відповідає за підготовку висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах, здатних застосовувати найновіші технології на високому професійному рівні [13].

Міжнародний досвід демонструє ефективність картографування злочинності як методу кримінального аналізу [14]. Динаміка злочинності розраховується на підставі показників безробіття, зміни співвідношення міського та сільського населення та інших демографічних і просторових факторів, що сприяє розробці ефективних стратегій протидії [14].

Висновки. Методологія кримінального аналізу в умовах зростання кіберзагроз потребує комплексної трансформації, що базується на інтеграції традиційних криміналістичних підходів з інноваційними технологіями штучного інтелекту, машинного навчання та великих даних. Ефективна протидія сучасній кіберзлочинності можлива лише за умови системного впровадження нових методів аналізу, які дозволяють працювати з величезними обсягами цифрових даних, виявляти складні патерни злочинної діяльності та прогнозувати майбутні загрози. Ключовими напрямками вдосконалення методології є: впровадження ШІ-систем для автоматизації виявлення та аналізу кіберзагроз; розвиток цифрової криміналістики з акцентом на мобільну, мережеву та хмарну криміналістику; створення систем прогностичної аналітики на основі машинного навчання; зміцнення міжвідомчої та міжнародної співпраці в розслідуванні транснаціональних кіберзлочинів; підвищення кваліфікації фахівців правоохоронних органів у сфері сучасних інформаційних технологій. Досвід України, зокрема функціонування системи виявлення вразливостей та проактивний підхід до кіберзахисту, демонструє можливість ефективного впровадження сучасних методів кримінального аналізу навіть в умовах збройної агресії. Однак залишаються виклики, пов'язані з швидким розвитком технологій, які використовують кіберзлочинці, юрисдикційними конфліктами в транскордонних розслідуваннях та необхідністю постійного оновлення технічної бази та методологічних підходів.

Перспективами подальших досліджень є вивчення можливостей застосування квантових технологій у кримінальному аналізі, розробка методів протидії ШІ-генерованим кіберзагрозам, включаючи дипфейки та автоматизовані фішингові атаки, а також удосконалення правових механізмів роботи з цифровими доказами на міжнародному рівні. Інтеграція блокчейн-технологій для забезпечення цілісності ланцюга доказів та розвиток методів Explainable AI для підвищення прозорості та довіри до ШІ-систем у судових процесах також є важливими напрямками майбутніх наукових розробок.

ЛІТЕРАТУРА

1. Державний центр кіберзахисту при Держспецзв'язку. Кіберзагрози у цифрах: аналіз інцидентів та вразливостей за І квартал 2025 року URL:https://loda.gov.ua/news/134478
2. Департамент оперативно-розшукової діяльності. Основи кримінального аналізу: навч. посібник. Нац. акад. Держ. прикордон. служби України, 2022. URL:https://dspace.nadpsu.edu.ua/bitstream/123456789/3241/1/osnovy_kryminaljnogo_analizu.pdf
3. Djenna, A., Barka, E., Benchikh, A., Khadir, K. Unmasking Cybercrime with Artificial-Intelligence-Driven Cybersecurity Analytics. Sensors. 2023. Vol. 23, no. 14. Art. 6302. DOI: 10.3390/s23146302
4. Dunsin, D., Ghanem, M. C., Ouazzane, K., Vassilev, V. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Science International: Digital Investigation. 2024. Vol. 48. Art. 301675. URL: https://www.sciencedirect.com/science/article/pii/S2666281723001944

5. Kozlovskyi, S. et al. Legal Regulation of Cyberattacks and Cybercrime. Baltic Journal of Economic Studies. 2024. Vol. 10, no. 5. P. 50–60. URL: https://www.cribfb.com/journal/index.php/BJMSR/article/download/2651/1507/3886

6. Крутоголов, А., Базаренко, І., Кисельов, А. Методи кримінального аналізу. UNIVERSUM. 2024. No. 9. URL: https://archive.liga.science/index.php/universum/article/view/1096

7. Lusthaus, J. et al. Mapping the Global Geography of Cybercrime with the World Cybercrime Index. PLOS ONE. 2024. URL: https://www.infosecurity-magazine.com/news/russia-ukraine-world-cybercrime/

8. Національна академія внутрішніх справ. Використання тактичного кримінального аналізу в діяльності аналітичних підрозділів Національної поліції України: матеріали конференції. URL: https://www.navs.edu.ua/files/naukova-diyalnist/naukovi-zaxodi/konferencii/2022/11_08/materialy_konf_110822.pdf

9. Сироватченко, М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник* Національного університету Львівська політехніка. Серія: *Юридичні науки*. 2024. № 1 (41). С. 314–322. DOI: http://doi.org/10.23939/law2024.41.314.

10. Rogers, M. Digital Forensics in Cybercrime Investigation. International Journal of Applied Information Systems. 2022. Vol. 12, no. 47. P. 25–31. URL: https://www.ijais.org/archives/volume12/number47/digital-forensic-tools-for-cybercrime-investigation-a-comparative-analysis/

11. Sarker, I. H. et al. Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: methods, taxonomy, challenges and prospects. ICT Express. 2024. Vol. 10, no. 3. P. 123–137. URL: https://www.sciencedirect.com/science/article/pii/S2405959524000572

12. Soni, N. Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges. Journal of Forensic Legal & Investigative Sciences. 2025. Vol. 11. P. 105–115. URL: https://www.heraldopenaccess.us/openaccess/digital-forensics-confronting-modern-cyber-crimes-technological-advancements-and-future-challenges

13. The system of cybersecurity bodies in Ukraine. Revista de Ciencias Humanas y Sociales. 2023. Vol. 7, no. 3. URL: https://www.redalyc.org/journal/4762/476273700003/html/

14. Калякін, С. В., Міхтєєв, Д. Д. Сучасні інформаційні технології в діяльності поліції: ГІС, аналіз злочинності та predictive policing. Безпека у кіберсфері: Матеріали міжнар. конф. Харків, 2025. С. 147–149. URL: https://dspace.univd.edu.ua/items/a8b419be-6f87-4819-971f-1fb19995b6a7

15. Council of Europe. CyberUA: Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine. 2025. URL: https://www.coe.int/en/web/kyiv/cyberua

16. EC-Council. The Role of Artificial Intelligence and Machine Learning in Enhancing Cybersecurity against Cybercrime. 2025. URL: https://www.eccouncil.org/cybersecurity-exchange/network-security/role-of-ai-ml-in-enhancing-cybersecurity-against-threats/

17. CLTC UC Berkeley. Beyond Phishing: Exploring the Rise of AI-enabled Cybercrime. 2025. URL: https://cltc.berkeley.edu/2025/01/16/beyond-phishing-exploring-the-rise-of-ai-enabled-cybercrime/

18. Akamai. AI in Cybersecurity: How AI Is Impacting the Fight Against Cybercrime. 2025. URL: https://www.akamai.com/blog/security/ai-cybersecurity-how-impacting-fight-against-cybercrime

19. Шепітько, В. Ю. (ред.) Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі: монографія. Київ, 2024. НДІ вивчення проблем злочинності ім. акад. В. В. Сташиса НАПрН України. URL: https://ivpz.kh.ua/wp-content/uploads/2025/01/Монографія-Криміналістів-2024.pdf

20. Cutting-edge advances in AI and ML for cybersecurity: a comprehensive review of emerging trends and future directions. Cogent Business & Management. 2025. Vol. 12. URL: https://www.tandfonline.com/doi/full/10.1080/23311975.2025.2518496

Дата першого надходження рукопису до видання: 22.11.2025
Дата прийнятого до друку рукопису після рецензування: 15.12.2025
Дата публікації: 30.12.2025