УДК 343.9:004.056:004.9
DOI https://doi.org/10.32782/TNU-2707-0581/2026.1/16

Гнедюк В. Л.
https://orcid.org/0009-0007-8025-0876
Український наково-дослідний інститут Спеціальної техніки
та судових експертиз Служби безпеки України

КІБЕРЗЛОЧИНИ, ЦИФРОВІ РОЗСЛІДУВАННЯ ТА ЕКСПЕРТИЗИ

У статті здійснено комплексний аналітично-статистичний аналіз сучасного стану кіберзлочинності, цифрових розслідувань та судових комп'ютерно-технічних експертиз в умовах цифрової трансформації суспільства. Розкрито теоретико-концептуальні засади дослідження кіберзлочинності як багатовимірного криміногенного явища, що реалізується у кіберпросторі або з використанням інформаційно-комунікаційних технологій. Обґрунтовано відмежування понять «кіберзлочинність» і «комп'ютерні правопорушення», визначено роль цифрових доказів у структурі кримінального провадження та значення цифрової криміналістики як міждисциплінарної методологічної основи їх дослідження.

На підставі узагальнення статистичних даних за 2022–2025 роки встановлено зростання структурної ваги кіберзлочинів у загальному масиві кримінальних правопорушень, домінування фінансово орієнтованих форм протиправної діяльності, а також наявність кількісного розриву між офіційною кримінальною статистикою та даними інцидентного обліку, що свідчить про високий рівень латентності. Доведено, що результативність протидії кіберзлочинності безпосередньо залежить від ефективності цифрових розслідувань, своєчасності проведення судових експертиз і дотримання процесуальних стандартів роботи з електронними доказами.

Окрему увагу приділено проблемам допустимості цифрових доказів, навантаженню на експертні установи, транснаціональному характеру кіберзагроз та ролі міжнародного співробітництва у сфері отримання цифрової інформації. Обґрунтовано необхідність підвищення інституційної спроможності системи цифрових розслідувань шляхом технічної модернізації, оптимізації строків експертиз і впровадження автоматизованих інструментів аналізу даних.

Практична значущість результатів дослідження полягає у можливості їх використання для підвищення ефективності цифрових розслідувань і судових комп'ютерно-технічних експертиз, оптимізації строків їх проведення та вдосконалення роботи з цифровими доказами. Отримані висновки можуть бути застосовані в діяльності правоохоронних органів, експертних установ і в освітньому процесі.

Ключові слова: *кіберзлочинність, цифрові розслідування, цифрові докази, комп'ютерно-технічна експертиза, латентність, онлайн-шахрайство.*

Постановка проблеми. Стрімка цифровізація соціально-економічних процесів зумовила формування кіберпростору як самостійного криміногенного середовища, у межах якого спостерігається інтенсивне зростання кількості та ускладнення способів вчинення правопорушень. Кіберзлочинність характеризується транснаціональністю, високим рівнем латентності та значним економічним і соціальним впливом. За оцінками міжнародних інституцій, зокрема Інтерполу та Європолу, цей вид злочинності належить до найбільш динамічних сегментів глобальної кримінальної активності, що зумовлює необхідність удосконалення механізмів протидії.

Ускладнення технічних засобів вчинення кіберзлочинів (анонімізуючі мережі, криптовалюти, хмарні технології, розподілені системи зберігання даних) істотно підвищує вимоги до процесу збирання, фіксації та аналізу цифрових доказів. Ефективність кримінального провадження дедалі більше залежить від якості цифрових розслідувань та результатів судових комп'ютерно-технічних експертиз, що повинні відповідати процесуальним стандартам допустимості й наукової обґрунтованості. Водночас спостерігаються проблеми методичної уніфікації, кадрового забезпечення та забезпе-

чення цілісності ланцюга збереження доказової інформації.

Попри імплементацію міжнародних стандартів, закріплених у Будапештській конвенції про кіберзлочинність, зберігається дисбаланс між темпами розвитку кіберзлочинності та інституційними можливостями її ефективного розслідування й експертного забезпечення. Зазначена суперечність актуалізує необхідність комплексного аналітично-статистичного дослідження сучасного стану кіберзлочинів, практики цифрових розслідувань і судових експертиз з метою визначення напрямів їх системного вдосконалення.

Аналіз останніх досліджень і публікацій. Проблематика кіберзлочинності, цифрових розслідувань та використання електронних доказів активно досліджується у сучасній кримінально-правовій і криміналістичній науці. І. В. Гора, В. А. Колесник та І. І. Попович [1] обґрунтовують місце цифрової криміналістики у системі криміналістичних знань і її значення для забезпечення допустимості цифрових доказів. О. Джафарова та Д. Зінченко [2] аналізують процесуальні особливості дослідження електронної інформації під час розслідування кіберзлочинів. Організаційні та експертні аспекти розслідування кіберзлочинів висвітлює М. О. Ларченко [6], акцентуючи на ролі спеціальних знань у сфері ІТ та навантаженні на експертні установи. Економічний вимір кіберзлочинності досліджує О. Корчинська [5], а інституційні механізми протидії сучасним кіберзагрозам аналізують Б. Макаліш, О. Мойко та В. Лучик [7]. Разом із тим комплексна аналітично-статистична оцінка динаміки кіберзлочинності у взаємозв'язку з ефективністю цифрових розслідувань і судових експертиз залишається недостатньо узагальненою, що зумовлює актуальність даного дослідження.

Постановка завдання. Метою статті є аналітично-статистична оцінка сучасного стану кіберзлочинності та результативності цифрових розслідувань і судових комп'ютерно-технічних експертиз.

Для досягнення цієї мети поставлено такі завдання:

– визначити теоретико-концептуальні підходи до визначення кіберзлочинності та цифрових доказів;

– проаналізувати динаміку й структуру кіберзлочинів за 2022–2025 роки та оцінити рівень їх латентності;

– дослідити вплив цифрових розслідувань і судових експертиз на результативність кримінального провадження.

Виклад основного матеріалу. Формування інформаційного суспільства та інтенсивна інтеграція цифрових технологій у всі сфери соціально-економічного життя зумовили трансформацію традиційних форм злочинності й появу якісно нових криміногенних ризиків. У науковому дискурсі кіберзлочинність розглядається як сукупність суспільно небезпечних діянь, що вчиняються у кіберпросторі або з використанням інформаційно-комунікаційних технологій і посягають на інформаційні відносини, майнові інтереси, безпеку функціонування державних і приватних систем. Такий підхід відображає подвійний характер зазначеного явища: з одного боку, інформаційні системи можуть бути безпосереднім об'єктом посягання, з іншого – виступати інструментом реалізації протиправної поведінки.

Більш вузькою категорією є комп'ютерні правопорушення, які охоплюють діяння, пов'язані з несанкціонованим доступом до автоматизованих систем, втручанням у їх функціонування, незаконним копіюванням, модифікацією або знищенням даних. Відмежування цих понять має принципове значення для формування кримінально-правової кваліфікації та статистичного обліку, оскільки не всі кіберзлочини зводяться до технічного втручання в комп'ютерні системи; частина з них реалізується через використання цифрових каналів комунікації для вчинення традиційних складів злочинів [1, с. 88].

Особливого значення у структурі сучасного кримінального провадження набувають цифрові докази, під якими розуміється інформація в електронній формі, здатна підтвердити або спростувати обставини, що підлягають доказуванню. Їх специфіка полягає у нематеріальній природі, залежності від технічного середовища відтворення, потенційній змінюваності та можливості точного копіювання без втрати змісту. З огляду на це, забезпечення автентичності, цілісності та безперервності ланцюга збереження є ключовими умовами процесуальної допустимості таких доказів.

Методологічну основу роботи з цифровими доказами становить цифрова криміналістика, яка сформувалася як міждисциплінарна галузь на стику права, інформатики та криміналістичної техніки. Її предмет охоплює розроблення та застосування науково обґрунтованих методів виявлення, фіксації, вилучення, аналізу й інтерпретації електронної інформації з дотриманням принципів відтворюваності процедур і мінімізації впливу на первинні носії даних. Розвиток цифро-

вої криміналістики відбувається в контексті міжнародної уніфікації підходів до протидії кіберзлочинності, зокрема відповідно до положень Будапештська конвенція про кіберзлочинність, що закріплює основні стандарти криміналізації та співпраці держав у цій сфері [6, с. 72–73].

Кіберпростір у сучасних дослідженнях трактується як складна багаторівнева система інформаційних ресурсів, телекомунікаційних мереж і цифрових сервісів, у межах якої відбувається обіг даних та реалізація соціальних і економічних процесів. Відсутність чітких територіальних меж, високий рівень анонімності суб'єктів, швидкість трансакцій і технічна складність інфраструктури зумовлюють специфіку кіберпростору як середовища злочину та об'єктивно ускладнюють процес встановлення юрисдикції й атрибуції протиправних дій [2, с. 85].

Класифікація кіберзлочинів ґрунтується на функціонально-об'єктному підході, що дозволяє систематизувати їх залежно від характеру посягання та спрямованості протиправної діяльності. У межах цього підходу доцільно виокремити такі базові групи:

– злочини проти конфіденційності, цілісності та доступності даних і систем, які безпосередньо спрямовані на порушення інформаційної безпеки шляхом несанкціонованого доступу, втручання у функціонування інформаційних систем, модифікації або знищення даних;

– фінансові кіберзлочини, що поєднують традиційні майнові посягання з використанням цифрових технологій, зокрема електронних платіжних інструментів, онлайн-банкінгу, криптовалютних платформ та дистанційних каналів комунікації;

– кібертероризм, спрямований на дестабілізацію діяльності органів державної влади, об'єктів критичної інфраструктури або суспільно значущих інформаційних систем із метою досягнення політичного чи ідеологічного ефекту;

– створення та розповсюдження шкідливого програмного забезпечення, яке використовується для несанкціонованого отримання доступу до інформації, блокування систем, викрадення даних або порушення їх функціонування;

– соціальна інженерія, у межах якої основним інструментом виступає психологічний вплив на користувачів з метою отримання конфіденційної інформації чи спонукання до здійснення фінансових або організаційних дій.

Зазначена типологія відображає багатовимірність кіберзлочинності та створює аналітичну основу для подальшого статистичного дослідження її структури, динаміки та взаємозв'язку з ефективністю цифрових розслідувань і судових експертиз [5; 6].

Зазначена типологія визначає логіку подальшого емпіричного аналізу кіберзлочинності. Кількісна оцінка її динаміки у 2022–2025 роках ґрунтується на аналізі обсягів зареєстрованих правопорушень у сфері високих інформаційних технологій, їх питомої ваги у загальній структурі злочинності та показників розкриття як індикатора ефективності цифрових розслідувань. Результати відповідного аналізу наведено у таблиці 1.

Отримані дані свідчать про суттєві коливання інтенсивності кіберзлочинності протягом досліджуваного періоду. Пік 2023 року характеризується різким зростанням питомої ваги правопорушень у сфері ВІТ у структурі загальної злочинності. Водночас відносний показник розкриття демонструє зниження у порівнянні з попереднім роком, що може свідчити про дисбаланс між зростанням обсягів кіберзлочинів та процесуальними можливостями їх ефективного розслідування. У 2024 році спостерігається певна стабілізація, однак кіберкомпонент зберігає структурну вагомість у загальному кримінальному масиві.

Поряд із показниками офіційної кримінальної статистики доцільно залучити дані інцидентного обліку, що відображають фактичну інтенсивність кіберзагроз та доповнюють формалізовану картину зареєстрованих правопорушень (таблиця 2).

Динаміка кіберінцидентів демонструє стале зростання, особливо у 2024–2025 роках, що підтверджує підвищення інтенсивності атак на

Таблиця 1

Динаміка кіберзлочинів у структурі загальної злочинності (2022–2025 рр.)

Рік	Зареєстровано кримінальних правопорушень (усього), тис.	Кіберзлочини / ІТ, тис.	Частка кіберзлочинів, %	Розкрито, тис.	Орієнтовний рівень розкриття, %
2022	259,7	14,9	5,74	7,3	48,99
2023	374,2	61,4	16,41	13,9	22,64
2024	357,2	50,2	14,05	14,0	27,89
2025	н/д	26,9	н/д	н/д	н/д

Таблиця 2

Кількість кіберінцидентів, опрацьованих CERT-UA (2022–2025 рр.)

Рік	Кількість кіберінцидентів
2022	2194
2023	2541
2024	4315
2025	5927

інформаційні ресурси держави. Концентрація інцидентів у сферах державного управління, критичної інфраструктури, енергетики та телекомунікацій свідчить про стратегічний характер кіберзагроз і їх спрямованість на системно значущі об'єкти [3; 4; 8; 9].

Структурний аналіз дозволяє визначити, які саме види кіберзлочинів формують основний масив кримінальної статистики (таблиця 3).

Таблиця 3

Структура правопорушень у сфері ВІТ (2022–2024 рр.)

Рік	Усього ВІТ, тис.	Онлайн-шахрайства, тис.	Частка онлайн-шахрайств, %
2022	14,9	7,9	53,0
2023	61,4	45,7	74,4
2024	50,2	~35,0	~69,7

Структурна домінанта онлайн-шахрайств підтверджує фінансову орієнтованість сучасної кіберзлочинності. Питома вага таких правопорушень перевищує половину загального масиву, а в окремі роки наближається до трьох чвертей. Це зумовлює необхідність посилення інструментів цифрового фінансового аналізу, транзакційного моніторингу та міжвідомчої координації.

Порівняння кримінальної статистики з кількістю зафіксованих кіберінцидентів дає підстави для оцінки рівня латентності (Таблиця 4).

Таблиця 4

Співвідношення кримінальних правопорушень та кіберінцидентів (2022–2025 рр.)

Рік	Кіберзлочини (ВІТ), тис.	Кіберінциденти, од.
2022	14,9	2194
2023	61,4	2541
2024	50,2	4315
2025	26,9	5927

Наявність кількісного розриву між кримінальною статистикою та даними інцидентного обліку підтверджує складність безпосереднього зіставлення різних систем вимірювання та вказує на високий рівень латентності кіберзлочинності. Це актуалізує потребу в удосконаленні механізмів виявлення, фіксації та процесуальної трансформації кіберподій у кримінальні провадження [3; 4; 8; 9].

Сукупність наведених статистичних показників засвідчує зростання структурної ваги кіберзлочинності, домінування фінансово орієнтованих правопорушень, нестабільність показників результативності їх розслідування та наявність істотного розриву між кримінальною статистикою і фактичним масивом кіберінцидентів, що підтверджує високий рівень латентності й актуалізує необхідність підвищення ефективності цифрових розслідувань.

У практичному вимірі це проявляється у зростанні ролі цифрових доказів та судових комп'ютерно-технічних експертиз у структурі кримінальних проваджень. Методологія цифрового розслідування зводиться до забезпечення збереження електронної інформації, її аналітичного дослідження та процесуальної трансформації результатів у доказову форму. Порушення процедур фіксації або безперервності зберігання може призвести до втрати доказового значення матеріалів [7, с. 318].

Збільшення масиву правопорушень у сфері ІТ супроводжується зростанням кількості призначених експертиз, що формує додаткове навантаження на експертні установи. Строки їх проведення стають одним із визначальних чинників тривалості досудового розслідування та опосередковано впливають на показники розкриття.

Кількісними індикаторами ефективності експертного забезпечення доцільно вважати співвідношення фактично виконаних судових комп'ютерно-технічних експертиз до кількості призначених у відповідному звітному періоді, а також середній строк їх проведення. Зменшення частки невиконаних експертиз і скорочення середнього строку дослідження свідчить про підвищення інституційної спроможності експертної системи та позитивно корелює з рівнем процесуального завершення кримінальних проваджень.

Транснаціональний характер кіберзлочинності ускладнює отримання цифрових доказів, оскільки значна частина даних розміщується поза межами національної юрисдикції. У цьому контексті важливу роль відіграють механізми міжнародної співпраці, передбачені Будапештською конвенцією про кіберзлочинність, а також взаємодія з Європолом та Інтерполом, однак строки

міжнародної правової допомоги часто не відповідають оперативним потребам розслідування [5, с. 12–13].

Таким чином, результативність цифрових розслідувань визначається не лише масштабами кіберзлочинності, а й рівнем ресурсного забезпечення, кадрової спроможності та технічної модернізації експертних підрозділів. Оптимізація строків експертиз і впровадження автоматизованих інструментів аналізу даних виступають ключовими напрямами підвищення ефективності протидії кіберзлочинності.

Висновки. Отже, проведене дослідження підтвердило тенденцію до посилення ролі кіберзлочинності у структурі кримінальних правопорушень та її фінансову домінанту, що відображається у високій частці онлайн-шахрайств. Виявлений розрив між показниками кримінальної статистики та даними інцидентного обліку свідчить про системну латентність кіберзлочинів і потребу вдосконалення механізмів їх виявлення та процесуальної фіксації. Зростання обсягів правопорушень у сфері ІТ обумовлює підвищене навантаження на систему цифрових розслідувань та експертного забезпечення, а строки проведення судових комп'ютерно-технічних експертиз виступають одним із чинників, що впливають на результативність кримінального провадження. Транснаціональність кіберзагроз посилює значення міжнародної координації та уніфікації процедур отримання цифрових доказів.

Перспективними напрямами подальших досліджень є розроблення інтегральних показників оцінки ефективності цифрових розслідувань, удосконалення стандартів роботи з електронними доказами, оптимізація строків проведення експертиз та впровадження автоматизованих інструментів аналізу великих масивів даних, зокрема технологій штучного інтелекту й методів blockchain forensic. Комплексне поєднання статистичного, криміналістичного та технологічного підходів створює підґрунтя для підвищення результативності системи протидії кіберзлочинності в умовах цифрової трансформації суспільства.

Список літератури:

1. Гора І. В., Колесник В. А., Попович І. І. До питання про цифрову криміналістику в системі криміналістичних знань. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2024. № 68. С. 86–91. DOI: https://doi.org/10.32782/2307-1745.2024.68.18.

2. Джафарова О., Зінченко Д. Роль цифрової криміналістики в розслідуванні кіберзлочинів. *Актуальні питання судової експертизи і криміналістики*: зб. матеріалівлів міжнар. наук.-практ. конф. з нагоди 100-річчя від дня народження М. С. Романова. Харків : ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», 2024. С. 85–86.

3. Єдиний звіт про кримінальні правопорушення за 2025 рік. URL: https://data.gov.ua/ (дата звернення: 19.02.2026).

4. Єдиний звіт про кримінальні правопорушення за 2023 рік. URL: https://data.gov.ua/ (дата звернення: 19.02.2026).

5. Корчинська О. Кіберзлочинність як загроза економічній безпеці: світовий досвід та ситуація в україні. *Економічний дискурс*. 2025. №1-2. С. 7–16. DOI: https://doi.org/10.36742/2410-0919-2025-1-1

6. Ларченко М. О. Деякі особливості розслідування кіберзлочинів. *Науковий вісник Львівського державного університету внутрішніх справ. Сер.: Юридична.* 2024. №3. С. 70–77. DOI: https://doi.org/10.32782/2311-8040/2024-3-9

7. Макаліш Б., Мойко О., Лучик В. Сучасні виклики кіберзлочинності та роль національної поліції україни у їх подоланні. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2025. №3(31). С. 309–322. DOI: https://doi.org/10.28925/2663-4023.2025.31.983

8. Понад 80% кібератак РФ у першій половині 2025р. припадала на цивільну інфраструктуру України – Держспецзв'язку. URL: https://interfax.com.ua/news/general/1118261.html (дата звернення: 18.02.2026).

9. У 2024 році кількість кібератак на Україну зросла на 70%. URL: https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931 (дата звернення: 18.02.2026).

Hnediuk V. L. CYBERCRIME, DIGITAL INVESTIGATIONS AND FORENSIC ANALYSIS

The article presents a comprehensive analytical and statistical study of the current state of cybercrime, digital investigations, and forensic computer examinations in the context of the ongoing digital transformation of society. The theoretical and conceptual foundations of cybercrime are examined as a multidimensional criminogenic phenomenon manifested in cyberspace or through the use of information and communication technologies. The distinction between the concepts of "cybercrime" and "computer-related offenses" is

substantiated, and the role of digital evidence within criminal proceedings is defined, along with the significance of digital forensics as an interdisciplinary methodological framework for its examination.

Based on the generalization of statistical data for the period 2022–2025, the study identifies an increase in the structural share of cybercrime within the overall crime structure, the dominance of financially motivated offenses, and a quantitative gap between official criminal statistics and incident reporting data, indicating a high level of latency. It is demonstrated that the effectiveness of countering cybercrime directly depends on the efficiency of digital investigations, the timeliness of forensic examinations, and compliance with procedural standards governing electronic evidence.

Special attention is paid to the admissibility of digital evidence, the growing workload of forensic institutions, the transnational nature of cyber threats, and the role of international cooperation in obtaining digital information. The necessity of strengthening the institutional capacity of digital investigation systems through technical modernization, optimization of forensic timeframes, and the implementation of automated data analysis tools is substantiated.

Practical significance of the research results lies in the possibility of their application to enhance the effectiveness of digital investigations and forensic computer examinations, optimize the timeframes for their conduct, and improve procedures for handling digital evidence; the findings may be used in the activities of law enforcement agencies, forensic institutions, and within the educational process.

Keywords: *cybercrime, digital investigations, digital evidence, forensic computer examination, latency, online fraud.*

Дата першого надходження статті до видання: 24.02.2026
Дата прийняття статті до друку після рецензування: 20.03.2026
Дата публікації (оприлюднення) статті: 04.05.2026