УДК 004.056.5
DOI 10.33244/2617-4154.3(20).2025.28-36

А. В. Гарбінська-Руденко,
кандидат юридичних наук, доцент,
Державний податковий університет
email: prokyror.irpin@i.ua
ORCID 0000-0002-0971-1234;
М. О. Кучко,
здобувачка вищої освіти,
Державний податковий університет
email: mariiakuchko@gmail.com
ORCID 0009-0004-5639-6152

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРАВООХОРОННИМИ ОРГАНАМИ УКРАЇНИ

Стаття присвячена комплексному дослідженню проблем забезпечення інформаційної безпеки правоохоронними органами України в умовах воєнного стану. У роботі розглянуто різні наукові підходи до визначення категорії «інформаційна безпека», акцентовано увагу на відсутності єдиного законодавчого визначення цього поняття й проблемах термінологічної розмитості, що створюють труднощі в правозастосовній практиці. Проведено аналіз нормативно-правової бази, зокрема положень Конституції України, законів України «Про інформацію», «Про захист персональних даних», «Про основні засади забезпечення кібербезпеки України», а також статей Кримінального кодексу України, які встановлюють відповідальність за кіберзлочини.

Особливу увагу приділено аналізу статистики кіберзлочинності за 2020–2024 рр. Установлено, що в цей період відбувалися суттєві коливання в кількості зареєстрованих правопорушень і результативності досудових розслідувань. Найбільше падіння ефективності спостерігалося 2023 р., що пояснюється перевантаженням правоохоронної системи через зростання масштабів кібератак, кадровим дефіцитом і складністю отримання цифрових доказів у транскордонних справах. Поряд з цим 2024 р. зафіксовано певне покращення показників завдяки посиленню спроможностей кіберполіції та адаптації методик документування злочинів.

У дослідженні визначено основні проблеми практичної діяльності правоохоронних органів: асиметрію між центральними й регіональними підрозділами, нестачу технічних засобів цифрової криміналістики, проблеми уніфікації процедур інцидент-менеджменту, відсутність швидких механізмів транскордонної співпраці та високий рівень латентності кібершахрайств. Зазначено, що більшість злочинів у кіберсфері залишається нерозкритою через слабкість механізмів блокування активів і затримки у взаємодії з міжнародними провайдерами.

Сформовано висновок, що ефективне забезпечення інформаційної безпеки правоохоронними органами України можливе лише за умови комплексного підходу, який поєднує оновлення правового регулювання, розвиток кадрового потенціалу, технологічне переоснащення та міжнародну кооперацію.

Ключові слова: *інформаційна безпека, кіберзлочинність, кібершахрайство, правоохоронні органи, кібербезпека, інформація, персональні дані.*

Постановка проблеми. Розвиток цифрових технологій в Україні супроводжується зростанням ризиків у сфері інформаційної безпеки. Кібератаки на державні ресурси, втручання в роботу критичної інфраструктури, витоки персональних даних і поширення дезінформації посилюють вразливість держави й суспільства. В умовах воєнного стану інформаційний простір фактично перетворився на інструмент гібридної війни, де протистояння відбувається не лише на полі бою, а й у мережі. Правоохоронні органи України змушені реагувати на нові виклики: від протидії кіберзлочинам до виявлення інформаційно-психологічних операцій. Проте ефективність їхньої діяльності знижують нестача сучасних технічних засобів, кадрові проблеми та повільна адаптація правової бази до швидких технологічних змін.

Аналіз останніх досліджень і публікацій. У наукових працях О. Ільченка та К. Корощенка інформаційна безпека розглядається крізь призму діяльності правоохоронних органів як ключових суб'єктів кіберзахисту [8], тоді як С. Лихова та В. Сисоєва акцентують увагу на її адміністративно-правовій природі [9]. Н. Моргун, О. Шевчук та С. Марчевський визначають багаторівневий характер інформаційної безпеки в діяльності Національної поліції [11], а К. Батрак підкреслює її екзистенційне значення в умовах воєнного стану [6]. Водночас відсутні комплексні роботи, що поєднували б теоретичні визначення із практичним аналізом кіберзлочинності та діяльності правоохоронців, що й зумовлює актуальність цієї статті.

Метою статті є здійснення комплексного аналізу категорії інформаційної безпеки та виявлення можливих напрямів її підвищення правоохоронними органами.

Виклад основного матеріалу. У науковій літературі категорія «інформаційна безпека» розглядається з різних теоретико-правових позицій, що свідчить про відсутність усталеного підходу до її змісту. О. Ільченко та К. Корощенко трактують її як «невід'ємну складову кібербезпеки, що реалізується через діяльність системи суб'єктів – від Служби безпеки України та Державної служби спеціального зв'язку і захисту інформації до підрозділів Національної поліції України» [8, с. 199].

На відміну від цього бачення С. Лихова та В. Сисоєва підкреслюють адміністративно-правову природу інформаційної безпеки, розглядаючи її не лише як систему технічних засобів захисту, а й як комплекс організаційних і правових механізмів, що визначають доступ до інформації, порядок її використання та межі втручання держави у сферу інформаційних прав громадян [9, с. 100]. Така позиція дає змогу підкреслити роль держави як гаранта прав і свобод, але водночас звужує дискурс до адміністративно-правових інструментів, не враховуючи вплив глобальних цифрових трансформацій.

Н. Моргун, О. Шевчук та С. Марчевський пропонують більш багатовимірне трактування, розглядаючи інформаційну безпеку в діяльності Національної поліції як систему, що функціонує на трьох рівнях: внутрішньо-відомчому (захист службових баз даних і комунікацій), державному (протидія загрозам інформаційного суверенітету) та міжнародному (взаємодія з Інтерполом, Європолом, ЄС) [11, с. 117]. Особливу увагу приділяє досліджуваній категорії К. Батрак, який у контексті воєнного стану визначає її як екзистенційну умову збереження не лише правоохоронної, а й оборонної спроможності держави. Автор наголошує на відсутності єдиного законодавчого визначення поняття «інформаційна безпека», що породжує термінологічну розмитість та ускладнює правозастосування [6, с. 200].

Вважаємо, що для правоохоронної діяльності доцільно інтегрувати ці позиції в комплексне розуміння. Інформаційна безпека в цій сфері має визначатися як врегульований нормами публічного права стан захищеності інформаційних ресурсів, систем і комунікацій, який дає змогу правоохоронним органам ефективно виконувати завдання із запобігання, виявлення та розслідування правопорушень, водночас забезпечуючи дотримання прав і свобод людини в інформаційній сфері.

Нормативно-правове забезпечення інформаційної безпеки в Україні ґрунтується на положеннях Конституції України та спеціальних законів. Основний Закон України визначає державну безпеку пріоритетом діяльності держави та гарантує захист приватного життя й персональних даних громадян [1]. Закон України «Про основні засади забезпечення кібербезпеки України» закріплює правові та організаційні механізми функціонування національної системи кібербезпеки й визначає компетенцію правоохоронних органів [4]. Закони України «Про інформацію» та «Про захист персональних даних» регламентують принципи відкритості інформаційних відносин, порядок обробки й охорони персональних даних [2; 3]. Важливе значення мають і положення Кримінального кодексу України (ст. 361–363[1]), що встановлюють відповідальність за кіберзлочини [5]. Україна також орієнтується на європейські та міжнародні стандарти, інтегруючи їх у національну практику кібер- та інформаційної безпеки.

Аналіз динаміки кіберзлочинів у 2020–2024 рр. свідчить про нестабільність криміногенної ситуації у сфері використання комп’ютерних систем і мереж (табл. 1). У 2020–2021 рр. простежується поступове зростання кількості зареєстрованих правопорушень: з 2 217 до 2 790 випадків. Показник ефективності досудового розслідування також зростав – 2021 р. підозри було вручено понад 72 % осіб, а до суду направлено більше 63 % справ, що свідчить про підвищення результативності роботи кіберполіції та оптимізацію процесів документування злочинів.

Виявлена динаміка вказує на чутливість інформаційної сфери до зовнішньополітичних і внутрішніх чинників, а також на зростання складності способів вчинення правопорушень. Попри окремі позитивні зміни в показниках ефективності правоохоронців, зберігаються серйозні проблеми, пов’язані з латентністю кіберзлочинів, нестачею ресурсів і труднощами в доведенні справ до суду.

Таблиця 1 – Динаміка кримінальних правопорушень у сфері використання комп'ютерних систем, мереж і засобів електрозв'язку

Рік	Обліковано кримінальних правопорушень у звітному періоді, од.	Кримінальні правопорушення, у яких особам вручено повідомлення про підозру, од.	%	Кримінальні правопорушення, за якими провадження направлені до суду, од.	%
2020	2 217	1 515	68,34	1 139	51,38
2021	2 790	2 034	72,90	1 759	63,05
2022	3 102	2 393	77,14	1 458	47,00
2023	2 437	1 193	48,95	886	36,36
2024	3 945	3 061	77,59	2 328	59,01

Джерело: [10, с. 492].

Так, масштаб вхідних звернень і подій створює «довгу чергу інцидентів». Упродовж 2023 р. кіберполіція отримала десятки тисяч повідомлень громадян переважно щодо соціальної інженерії, фішингу та фінансових шахрайств, що потребує ресурсомісткої фільтрації й систематизації та, відповідно, розтягує час реагування на найкритичніші кейси. У річних підсумках фіксується також зростання організованих схем – від багаторівневих фішингових «ферм» до транскордонних фінансових злочинів, – подолання яких можливе лише за умови узгоджених дій із банками, платіжними сервісами, провайдерами хмарної інфраструктури та іноземними юрисдикціями [7].

Тактики зловмисників швидко еволюціонують. Аналітичні огляди фіксують масові кампанії через месенджери із «маскуванням» під знайомих, військову тематику вкладень і постійне оновлення доменно-акаунтної інфраструктури. Вразливість кінцевого користувача залишається ключовим тригером інцидентів, а превентивна комунікація держави та сервісів не завжди встигає за темпами появи нових сценаріїв обману. Попри стратегічні рамки, уніфіковані SOP для первинного огляду IT-середовища, вилучення та консервації даних, роботи з хмарними середовищами, CDN і криптоактивами впроваджені неоднаково [7]. Через це частина інцидентів із критичними сервісами фіксується постфактум, коли відновити ланцюг збереження цифрових доказів складно або неможливо.

Регіональний рівень демонструє об'єктивну асиметрію спроможностей. Складні транскордонні кейси зазвичай концентруються в центральних підрозділах і спеціалізованих слідчих групах, тоді як територіальні органи здебільшого виконують функції первинної фіксації й передають матеріали «вгору». Така конфігурація обумовлена як технічною базою (доступ до сучасних засобів цифрової форензіки, аналізу трафіку), так і кадровим чинником: дефіцит підготовлених фахівців та їх відтік у приватний сектор прямо позначаються на якості досудового розслідування [14, с. 19].

Доведення технічно складних проваджень до суду ускладнюють юрисдикційні й процесуальні бар'єри. Стандарти допустимості цифрових доказів не завжди однаково застосовуються щодо логів у розподілених системах, артефактів із хмарних платформ або криптоактивів, а отримання критичних даних від іноземних провайдерів часто потребує тривалих процедур, несумісних із «леткістю» артефактів.

Нарешті, масовий сегмент кібершахрайств перетворюється на «чорну діру» безпеки громадян. Найпоширеніші схеми – інвестиційні «дзеркала», фішингові «допомоги», псевдопродажі / доставки – швидко мутують і ротифікують інфраструктуру доменів, акаунтів і бот-мереж [14, с. 22]. Ефективна протидія залежить від «гарячих» механізмів блокування / замороження активів і сталих каналів обміну даними між правоохоронцями, банківськими установами, платіжними сервісами та регуляторами; будь-яка затримка на ділянці ланцюга прямо конвертується в збитки.

Отже, основними вузлами залишаються: операційна координація та стандартизація інцидент-менеджменту; вирівнювання кадрово-технічної спроможності «на краю мережі»; прискорення та уніфікація транскордонних процедур доступу до цифрових даних. Зважаючи на вищезазначене, існує потреба в розробленні комплексної програми вдосконалення діяльності правоохоронних органів України в системі забезпечення інформаційної безпеки.

Насамперед важливим завданням є формування єдиного правового підходу до категорії «інформаційна безпека». Розпорошеність дефініцій у чинних актах знижує ефективність застосування права та породжує міжвідомчі суперечності. Удосконалення законодавчої бази має ґрунтуватися на системній гармонізації з європейськими стандартами, насамперед Директивою NIS2, яка визначає правила захисту критичних інформаційних інфраструктур, та практикою GDPR у сфері обробки персональних даних [12]. Створення уніфікованої термінології та закріплення її в базових законах дасть змогу сформувати стабільне підґрунтя для подальшої практики правоохоронців.

Особливої уваги потребує питання розвитку кадрового потенціалу. В умовах постійного відтоку висококваліфікованих спеціалістів у приватний сектор правоохоронні органи мають зосередитись на створенні умов для довготривалого утримання експертів. Йдеться не лише про підвищення рівня матеріального забезпечення, але й про впровадження системи безперервного професійного навчання. У зарубіжній практиці, зокрема в країнах НАТО, ефективно функціонують моделі спільних тренінгових центрів, де навчання відбувається в симуляційних кіберполігонах. Запровадження схожих підходів в Україні сприятиме формуванню сталої системи підготовки кадрів, здатних ефективно реагувати на новітні загрози [13, с. 447].

У воєнний час набуває особливої ваги розвиток технологічних спроможностей. Правоохоронні органи потребують інноваційних інструментів цифрової криміналістики, автоматизованих систем моніторингу й аналізу трафіку, технологій прогнозної аналітики на основі штучного інтелекту. Застосування таких рішень дасть змогу скоротити час на виявлення та документування правопорушень, що особливо важливо в умовах масованих атак і високої латентності кіберзлочинності. Вдалим прикладом, який можна адаптувати до українських умов, є досвід Європейського центру з кіберзлочинності, що активно використовує алгоритми машинного навчання для виявлення транскордонних шахрайських схем.

Важливою складовою програми вдосконалення є налагодження сталої міжнародної кооперації. Враховуючи транскордонний характер більшості кіберзлочинів, правоохоронна система України має інтегруватися до оперативних механізмів обміну даними з

партнерами ЄС, НАТО та Інтерполу. Укладення двосторонніх угод щодо прискорених процедур доступу до даних глобальних провайдерів дасть змогу уникати ситуацій, коли цифрові артефакти втрачаються через тривалість формальних процедур. Досвід Естонії, яка стала прикладом побудови національної системи кіберзахисту в тісній співпраці з ЄС, може бути використаний як модель для розвитку українських практик.

Не менш актуальним є превентивний аспект. Більшість злочинів у цифровому середовищі стають можливими завдяки вразливості користувачів, які стають жертвами фішингу, соціальної інженерії чи шахрайських схем. Розбудова системи інформаційних кампаній, спрямованих на підвищення рівня цифрової грамотності населення, має стати складовою національної безпекової політики. Поширення матеріалів з кібергігієни, інтеграція навчальних курсів у програми закладів освіти та співпраця із засобами масової інформації забезпечать довготривалий ефект зниження латентності кіберзлочинів.

Висновки. Проблема забезпечення інформаційної безпеки правоохоронними органами в Україні вже давно вийшла за межі суто технічної проблеми та стала системним викликом національній безпеці. Коливання в показниках розслідувань у 2020–2024 рр. чітко продемонстрували залежність результативності правоохоронної діяльності від зовнішньополітичних чинників, кадрового потенціалу та можливостей міжнародної співпраці. Водночас відсутність єдиного законодавчого підходу до категорії «інформаційна безпека» створює додаткові бар'єри для координації між відомствами. Подальше вдосконалення можливе лише за умови поєднання трьох вимірів: уніфікації нормативної бази відповідно до європейських стандартів, технологічного оновлення інструментів цифрової криміналістики та посилення міжнародної взаємодії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України від 28 червня 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

2. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-XII. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650.

3. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI. *Відомості Верховної Ради України.* 2010. № 34. Ст. 481.

4. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

5. Кримінальний кодекс України від 5 квітня 2001 р. № 2341-III. *Відомості Верховної Ради України.* 2001. № 25–26. Ст. 131.

6. Батрак К. М. Інформаційне забезпечення правоохоронної діяльності в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2024. № 9. С. 198–203.

7. Звіти про результати роботи Департаменту кіберполіції Національної поліції України / Кібеполіція України. URL : https://surl.li/vkiibc (дата звернення: 16.09.2025).

8. Ільченко О. В., Корощенко К. Р. Правоохоронні органи як суб'єкти забезпечення кібербезпеки в Україні. *Юридичний науковий електронний журнал*. 2022. № 9. С. 198–202.

9. Лихова С. Я., Сисоєва В. П. Діяльність правоохоронних органів у сфері забезпечення інформаційної безпеки. *Науковий вісник публічного та приватного права*. 2021. Вип. 6, т. 2. С. 98–103.

10. Миненко С., Кочнєва В., Бабич Я. Оцінка рівня кібербезпеки України в умовах війни. *Європейський науковий журнал економічних та фінансових інновацій*. 2024. № 2 (14). С. 487–500.

11. Моргун Н. С., Шевчук О. О., Марчевський С. В. Поняття та зміст інформаційної безпеки в діяльності Національної поліції України. *Науковий вісник публічного та приватного права*. 2020. Вип. 5, т. 2. С. 115–120.

12. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) № 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). *Official Journal of the European Union*. 27.12.2022. L 333. P. 80–152.

13. Kulchytskyi T., Rezvorovych K., Povalena M., Dutchak S., Kramar R. Legal regulation of cybersecurity in the context of the digital transformation of ukrainian society. *Lex Humana*. 2024. № 1. P. 443–460.

14. National Cybersecurity Situation Centre. Year in review 2024. Київ, 2025. 64 с. / Рада національної безпеки і оборони України. URL : https://surl.li/tyqbre (дата звернення: 18.09.2025).

REFERENCES

1. Konstytutsiia Ukrainy vid 28 chervnia 1996 r. № 254k/96-VR. *Vidomosti Verkhovnoi Rady Ukrainy.* 1996. № 30. St. 141.

2. Pro informatsiiu : Zakon Ukrainy vid 2 zhovtnia 1992 r. № 2657-XII. *Vidomosti Verkhovnoi Rady Ukrainy.* 1992. № 48. St. 650.

3. Pro zakhyst personalnykh danykh : Zakon Ukrainy vid 1 chervnia 2010 r. № 2297-VI. *Vidomosti Verkhovnoi Rady Ukrainy.* 2010. № 34. St. 481.

4. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 5 zhovtnia 2017 r. № 2163-VIII. *Vidomosti Verkhovnoi Rady Ukrainy.* 2017. № 45. St. 403.

5. Kryminalnyi kodeks Ukrainy vid 5 kvitnia 2001 r. № 2341-III. *Vidomosti Verkhovnoi Rady Ukrainy.* 2001. № 25–26. St. 131.

6. Batrak K. M. Informatsiine zabezpechennia pravookhoronnoi diialnosti v umovakh voiennoho stanu. *Yurydychnyi naukovyi elektronnyi zhurnal.* 2024. № 9. S. 198–203.

7. Zvity pro rezultaty roboty Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy / Kibepolitsiia Ukrainy. URL : https://surl.li/vkiibc (data zvernennia: 16.09.2025).

8. Ilchenko O. V., Koroshchenko K. R. Pravookhoronni orhany yak subiekty zabezpechennia kiberbezpeky v Ukraini. *Yurydychnyi naukovyi elektronnyi zhurnal.* 2022. № 9. S. 198–202.

9. Lykhova S. Ya., Sysoieva V. P. Diialnist pravookhoronnykh orhaniv u sferi zabezpechennia informatsiinoi bezpeky. *Naukovyi visnyk publichnoho ta pryvatnoho prava.* 2021. Vyp. 6, t. 2. S. 98–103.

10. Mynenko S., Kochnieva V., Babych Ya. Otsinka rivnia kiberbezpeky Ukrainy v umovakh viiny. *Yevropeiskyi naukovyi zhurnal ekonomichnykh ta finansovykh innovatsii.* 2024. № 2 (14). S. 487–500.

11. Morhun N. S., Shevchuk O. O., Marchevskyi S. V. Poniattia ta zmist informatsiinoi bezpeky v diialnosti Natsionalnoi politsii Ukrainy. *Naukovyi visnyk publichnoho ta pryvatnoho prava.* 2020. Vyp. 5, т. 2. S. 115–120.

12. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) № 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). *Official Journal of the European Union.* 27.12.2022. L 333. P. 80–152.

13. Kulchytskyi T., Rezvorovych K., Povalena M., Dutchak S., Kramar R. Legal regulation of cybersecurity in the context of the digital transformation of ukrainian society. *Lex Humana*. 2024. № 1. R. 443–460

14. National Cybersecurity Situation Centre. Year in review 2024. Kyiv, 2025. 64 c. / Rada natsionalnoi bezpeky i oborony Ukrainy. URL : https://surl.li/tyqbre (data zvernennia: 18.09.2025).

A. V. Harbinska-Rudenko, M. O. Kuchko. ENSURING INFORMATION SECURITY BY LAW ENFORCEMENT AGENCIES OF UKRAINE

The article is devoted to a comprehensive study of the problems of ensuring information security by law enforcement agencies of Ukraine under martial law. The paper analyzes various scholarly approaches to defining the concept of «information security» and emphasizes the lack of a unified legal definition, which creates terminological ambiguity and complicates law enforcement practice. The analysis of the legal framework includes the provisions of the Constitution of Ukraine, the Laws «On Information», «On Personal Data Protection», «On the Basic Principles of Ensuring Cybersecurity in Ukraine», as well as relevant articles of the Criminal Code that establish liability for cybercrime.

Particular attention is paid to the analysis of cybercrime statistics for 2020–2024. The study reveals significant fluctuations in the number of registered offenses and the effectiveness of pre-trial investigations. The sharpest decline was observed in 2023, which is explained by the overload of law enforcement agencies due to the large-scale increase in cyberattacks, shortage of qualified personnel, and difficulties in obtaining digital evidence in cross-border cases. At the same time, 2024 showed certain improvements, primarily due to the strengthening of the Cyber Police's operational capacities and the adaptation of investigative methodologies.

The research highlights key challenges in the practical activities of law enforcement agencies: asymmetry between central and regional units, shortage of technical digital forensics tools, lack of unified incident management procedures, delays in international cooperation, and the high latency of cyber fraud cases. It is noted that the majority of cybercrimes remain unresolved due to the weakness of asset blocking mechanisms and procedural delays in cooperation with international service providers.

The article concludes that the effective provision of information security by Ukrainian law enforcement agencies is possible only through a comprehensive approach that combines legislative harmonization, personnel development, technological modernization, and sustainable international cooperation.

Keywords: *information security, cybercrime, cyberfraud, law enforcement agencies, cybersecurity, information, personal data.*

Стаття надійшла до редколегії 7 жовтня 2025 року