УДК 343.9:004.056.55(045)
DOI https://doi.org/10.32782/TNU-2707-0581/2025.4/15

Гнедюк В. Л.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

ЮРИДИЧНИЙ СУПРОВІД У ВИПАДКУ КІБЕРАТАК АБО ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Стаття присвячена комплексному дослідженню проблематики юридичного супроводу кіберінцидентів, зокрема кібератак та витоків конфіденційної інформації, як одного з ключових викликів у сфері сучасної цифрової безпеки. В умовах трансформації інформаційного простору та зростання кіберзалежності критичних функцій держави, бізнесу і суспільства, питання правового реагування на кіберзагрози набуває принципово нового змісту. На основі системного аналізу чинного законодавства України та міжнародних стандартів розглянуто особливості нормативного регулювання у сфері інформаційної безпеки, кваліфікації кіберінцидентів, обігу електронних доказів і процесуального супроводу цифрових правопорушень.

Визначено, що чинна правова система характеризується низьким рівнем узгодженості процедур фіксації та доказування кіберінцидентів, фрагментарністю нормативної бази та обмеженістю процесуальних інструментів для міжвідомчої взаємодії. Обґрунтовано, що ефективний юридичний супровід вимагає поєднання превентивних заходів (аудит, внутрішні політики, договірна модель), реактивних процедур (повідомлення органів, збирання цифрових доказів, представництво в суді) та комунікаційно-репутаційного захисту. Окрему увагу приділено аналізу ролі юриста в умовах кіберінциденту, з урахуванням комплаєнс-вимог, транснаціональної юрисдикції, участі у процесах цифрової експертизи та захисту прав суб'єктів даних.

У межах дослідження також висвітлено актуальні виклики у сфері використання електронних доказів у кримінальному та цивільному процесах, зокрема труднощі з верифікацією, допустимістю та судовою інтерпретацією цифрових слідів. Розкрито механізми міжнародного співробітництва у сфері протидії кіберзлочинності, роль MLATs, а також потенціал взаємодії з організаціями, такими як INTERPOL, ENISA, Europol EC3.

Узагальнення результатів дозволило запропонувати практичні напрями удосконалення правового регулювання юридичного супроводу кіберінцидентів.

Ключові слова: *юридичний супровід, кіберінцидент, кібератака, конфіденційна інформація, електронні докази, комплаєнс, цифрова безпека.*

Постановка проблеми. У добу цифрової трансформації, коли інформація стає ключовим стратегічним ресурсом, захист даних набуває критичного значення для стабільного функціонування держави, бізнесу та суспільства. Зростання масштабів і складності кіберзагроз – зокрема кібератак і витоків конфіденційної інформації – створює нові виклики для правової системи, вимагаючи від неї швидкої адаптації до динамічного технологічного середовища.

Кіберінциденти, що часто мають транскордонний характер і реалізуються за допомогою високотехнологічних засобів, виявляють обмеженість традиційних юридичних інструментів реагування. На цьому тлі посилюється потреба в теоретико-практичному осмисленні юридичного супроводу як комплексної системи превентивних, захисних і процесуальних заходів у сфері кібербезпеки.

Наявні прогалини в нормативному регулюванні, недостатня процесуальна визначеність та слабка міжвідомча координація формують правову вразливість суб'єктів цифрових правовідносин. Тому забезпечення ефективного юридичного супроводу у випадку кібератак або витоку інформації вимагає міждисциплінарного підходу, що поєднує положення інформаційного права, міжнародного та кримінального права, а також практику цифрової криміналістики.

Аналіз останніх досліджень і публікацій. Тематика юридичного супроводу кіберінцидентів дедалі частіше стає об'єктом дослідження у вітчизняній науковій площині. Стаття спирається на праці дослідників, серед яких: О. М. Левченко, У. Ніконенко, О. М. Поляков, С. В. Стендер тощо.

У дослідженні Левченко О. М. [1] проаналізовано проблеми витоку конфіденційної інформації в умовах цифровізації економіки. Ніконенко У. та Халіна О. [2] висвітлюють організаційно-правові засади кібербезпеки в соціально-економічних системах. Поляков О. [3] акцентує увагу на потребі розширення міжнародної правової співпраці у сфері реагування на кіберзагрози. Сироватченко М. [4] порушує питання транснаціональної юрисдикції, допустимості електронних доказів та прогалин у законодавстві. У роботах Стендера С. В. [5] і Шевчука М. О. [6] розглядаються інституційні та договірні механізми цифрового захисту.

Постановка завдання. Метою статті є комплексне дослідження особливостей юридичного супроводу у випадку кібератак або витоку конфіденційної інформації в умовах цифровізації та зростання кіберзагроз, аналіз проблем нормативного регулювання, а також обґрунтування напрямів удосконалення правових механізмів реагування з урахуванням національного законодавства, міжнародних стандартів та практичних потреб інформаційної безпеки.

Для досягнення цієї мети поставлено такі завдання:

– охарактеризувати правову природу та основні складові юридичного супроводу кіберінцидентів;

– визначити основні правові виклики, пов'язані з кваліфікацією, доказовістю та процедурним супроводом кібератак і витоків конфіденційної інформації;

– запропонувати напрями вдосконалення правового механізму супроводу кіберінцидентів.

Виклад основного матеріалу. У сучасних умовах цифровізації суспільних процесів питання правового забезпечення кібербезпеки набуває особливої актуальності як на національному, так і на міжнародному рівнях. Основоположним міжнародним документом у цій сфері є Конвенція про кіберзлочинність (Будапештська конвенція), що визначає стандарти криміналізації комп'ютерних правопорушень та механізми міжнародного співробітництва. У сфері захисту персональних даних вагоме значення має Загальний регламент ЄС щодо захисту даних (GDPR), який впливає й на регуляторні підходи країн за межами ЄС. Директива NIS2 слугує зразком для модернізації політик кіберзахисту, зокрема критичної інфраструктури.

В Україні основи кібербезпеки закладено Законом «Про основні засади забезпечення кібербезпеки України», а також рядом суміжних актів – «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах» та статтями 361–363[1] Кримінального кодексу України. Проте чинне законодавство залишається фрагментарним: не повністю врегульовано статус об'єктів критичної інфраструктури, механізми реагування на кіберінциденти та використання цифрових доказів у процесуальному порядку. Це вказує на необхідність подальшої систематизації та адаптації правових норм відповідно до міжнародних стандартів [9, с. 58].

З огляду на нормативні засади кібербезпеки, важливо також проаналізувати характерні риси, типологію та юридичну природу кібератак і витоків конфіденційної інформації як ключових форм цифрових загроз.

Адже саме правове осмислення змістовних характеристик кіберінцидентів є передумовою для формування дієвих механізмів реагування та притягнення до відповідальності суб'єктів правопорушень у цифровому середовищі.

Під поняттям «кібератака» в юридичній площині доцільно розуміти умисну протиправну дію або сукупність дій, здійснених з використанням інформаційно-телекомунікаційних технологій з метою порушення конфіденційності, цілісності або доступності інформації, інформаційних систем чи інфраструктурних об'єктів. З огляду на особливості реалізації та цільову спрямованість, у науковій та прикладній літературі виокремлюють різні типи кібератак:

– DoS / DDoS-атаки, спрямовані на виведення з ладу сервісів шляхом перевантаження каналів зв'язку чи ресурсів системи;

– ransomware, які передбачають шифрування даних з подальшою вимогою викупу;

– фішинг – метод соціальної інженерії, що має на меті обманним шляхом отримати доступ до облікових даних;

– APT (Advanced Persistent Threats) – складні, тривалі та приховані атаки з елементами шпигунства або саботажу.

У свою чергу, витоки конфіденційної інформації можуть бути класифіковані за джерелом загрози на внутрішні (інсайдерські дії персоналу, службова недбалість, неналежне адміністрування системи безпеки) та зовнішні (несанкціоноване проникнення, експлуатація вразливостей, дії третіх осіб). Кожен із цих випадків має власну юридичну специфіку, що обумовлює необхідність диференціації правових наслідків та форм відповідальності.

Юридична кваліфікація кіберінцидентів може набувати кримінально-правового змісту (зокрема, відповідно до ст. 361–363[1] КК України), адміністративного (наприклад, за порушення правил

зберігання або захисту персональних даних) або цивільно-правового (відшкодування шкоди, завданої внаслідок витоку інформації чи порушення договірних зобов'язань щодо її захисту). Вибір кваліфікаційної моделі залежить від характеру діяння, обсягу завданих збитків, правового статусу сторін та наявності умислу [4, с. 315].

Встановлення юридичних ознак кіберінцидентів та їх належна правова кваліфікація є лише первинною складовою ширшого процесу реагування на цифрові загрози, який передбачає системне й поетапне залучення правових механізмів. У цьому контексті набуває особливої ваги поняття *юридичного супроводу кіберінцидентів* як комплексної системи взаємопов'язаних дій, що здійснюються з метою мінімізації правових, фінансових та репутаційних наслідків кібератак або витоків інформації.

Юридичний супровід, як феномен правозастосовної практики, охоплює *превентивну, реактивну та репутаційно-стабілізаційну складові,* що функціонують у взаємодії із внутрішніми політиками організації та зовнішніми регуляторними вимогами. *Превентивний рівень* включає аудит інформаційної безпеки на предмет відповідності чинному законодавству та галузевим стандартам, розробку та імплементацію внутрішніх нормативних актів (політик захисту персональних даних, процедур доступу, інструкцій з реагування), а також укладення юридично обґрунтованих договорів із контрагентами – зокрема, договорів про нерозголошення (NDA), угод про обробку даних (DPA), положень про відповідальність за порушення кібербезпеки.

У випадку настання інциденту актуалізується *реактивний вектор,* що передбачає правомірне інформування уповноважених державних органів (зокрема Кіберполіції, CERT-UA, НКЦК), документування факту порушення (лог-файли, технічні звіти, цифрові докази), а також ініціювання процесуальних дій у межах кримінального чи цивільного провадження. Окремої уваги заслуговує *репутаційний компонент*, який проявляється у формуванні комунікаційної стратегії щодо інциденту, публічних заявах, інформуванні постраждалих сторін та захисті бренду в умовах інформаційного тиску [7, с. 32–33].

Слід зазначити, що комплексність та багатовекторність юридичного супроводу кіберінцидентів зумовлює потребу в чіткому функціональному розмежуванні ролей учасників процесу реагування, серед яких ключове місце посідає фахівець із правового забезпечення – адвокат або юрисконсульт. У межах правової доктрини його діяльність розглядається не лише як процесуальне представництво, але як інтегральний компонент управління кіберризиками, що охоплює консультативну, аналітичну, комунікаційну та комплаєнс-функції.

Саме на етапі реагування на інцидент роль юриста виходить за межі традиційної правозастосовної практики і набуває мультидисциплінарного характеру. Йдеться, зокрема, про проведення *юридичного аудиту* події з метою верифікації фактів порушення, виявлення прогалин у внутрішній нормативній документації, а також оцінки потенційної відповідальності компанії відповідно до чинного законодавства чи договірних зобов'язань. У разі атак типу ransomware, юрист виступає медіатором між технічними фахівцями, менеджментом та зовнішніми суб'єктами, оцінюючи допустимість переговорів з кіберзлочинцями з погляду кримінального права, міжнародних санкцій та етичних стандартів.

Крім того, до сфери компетенції юриста належить процесуальне представництво інтересів постраждалої сторони у правоохоронних органах, судах, а також перед державними регуляторами у разі необхідності подання звітів про інцидент. Не менш важливою є функція забезпечення відповідності (комплаєнс) – перевірка дотримання компанією вимог законодавства про захист персональних даних, кібербезпеку, договірні умови з контрагентами, а також міжнародних норм (зокрема, GDPR, NIS2 тощо) [8, с. 283].

У межах супроводу кіберінцидентів важливою складовою ефективного правового реагування є належне формування та процесуалізація доказової бази, що у випадках інформаційних правопорушень має переважно нематеріальний, цифровий характер. Саме тому питання електронних доказів виходить на передній план, оскільки від коректності їх збору, збереження та легітимізації залежить не лише успішність розслідування, але й допустимість матеріалів у судовому провадженні.

Цифрові сліди – файли логів, метадані, пакети мережевого трафіку, листування, хеш-коди, дані з резервних копій тощо – потребують особливої процедури обігу, яка має відповідати принципам незмінності, автентичності, цілісності та відтворюваності. Відхилення від цих вимог здатне поставити під сумнів доказову силу інформації, що ускладнює як притягнення винних до відповідальності, так і реалізацію захисту порушених прав потерпілих осіб.

Окремого значення набуває визнання електронних доказів у межах кримінального та цивільного процесу, що на практиці супроводжується

методологічними та процедурними труднощами. Хоча процесуальні кодекси України формально закріплюють допустимість електронних доказів, відсутність усталеної судової практики та недосконаліть інструментів їх автентифікації залишають простір для правової невизначеності. Відтак ключову роль у верифікації таких матеріалів відіграють судові експертизи у сфері комп'ютерно-технічного аналізу, які покликані забезпечити фахове тлумачення цифрового контексту, підтвердження фактів втручання, способів доступу чи модифікації інформації.

Таким чином, ефективне використання електронних доказів в юридичному супроводі кіберінцидентів вимагає чіткого дотримання процесуальних стандартів, міждисциплінарної координації між правниками, ІТ-фахівцями та експертами, а також подальшого нормативного розвитку у сфері цифрової криміналістики [5].

Також, значною складовою юридичного супроводу кіберінцидентів є питання, пов'язані з порушенням режиму обробки персональних даних, оскільки витоки таких даних тягнуть за собою низку правових наслідків. Зокрема, порушення вимог щодо захисту персональної інформації активізує відповідальність контролерів і операторів даних за невиконання обов'язків зі збереження конфіденційності та безпеки. У цьому контексті застосовуються різні форми санкцій – від адміністративних штрафів до суттєвих фінансових збитків і репутаційних втрат, що можуть мати довготривалий вплив на діяльність суб'єкта господарювання [1, с. 26].

З огляду на транскордонний характер більшості кіберінцидентів, національні механізми правового реагування часто виявляються недостатніми для ефективного переслідування правопорушників та нейтралізації наслідків кіберзлочинів. Це зумовлює потребу в розширенні практики міжнародно-правового співробітництва, яке дедалі більше розглядається не як факультативний інструмент, а як невід'ємний елемент системи глобальної кібербезпеки.

Міжнародне співробітництво у цій сфері реалізується через комплекс інституційних, договірних та оперативно-практичних механізмів. Одним із ключових напрямів є екстрадиція та транснаціональне переслідування кіберзлочинців, що ускладнюється проблемами юрисдикції, різницею в кримінально-правовій кваліфікації діянь, а також політичними чинниками. Практика показує, що у разі виявлення суб'єкта, який діяв за межами держави-реєстратора інциденту, успішне притягнення до відповідальності можливе лише за умови наявності двосторонніх або багатосторонніх угод про правову допомогу, а також за сприяння компетентних органів інших країн.

У цьому контексті вагомого значення набуває координація з міжнародними структурами:

– Europol (Європейське поліцейське управління) – через Європейський центр боротьби з кіберзлочинністю (EC3), який виконує роль хаба для аналітичної, експертної та оперативної взаємодії;

– ENISA (Агентство ЄС з кібербезпеки) – у частині вироблення політик, проведення навчань та формування нормативної рамки кіберзахисту;

– INTERPOL – через підрозділ кіберзлочинності, що забезпечує глобальне спостереження, спільні операції та обмін інформацією про загрози.

Окрему роль відіграють механізми міжнародної правової допомоги, зокрема MLATs (Mutual Legal Assistance Treaties), що забезпечують процесуальне оформлення запитів про отримання цифрових доказів, тимчасовий арешт активів, виклик свідків тощо.

Таким чином, формування ефективної моделі реагування на кіберінциденти неможливе без активного залучення до міжнародних форматів співпраці, гармонізації національного законодавства з міжнародними стандартами та розвитку каналів оперативної транснаціональної взаємодії [3, с. 135–136].

Враховуючи зростання складності кіберзагроз та посилення ролі цифрового середовища в житті держави й суспільства, особливої актуальності набуває необхідність комплексного вдосконалення правового регулювання у сфері кібербезпеки. Право більше не може відігравати суто реактивну роль – натомість воно має випереджати технологічні трансформації, створюючи адаптивні механізми, здатні функціонувати в умовах високотехнологічної невизначеності. Традиційні нормативні підходи дедалі більше втрачають ефективність у ситуаціях, що пов'язані з транснаціональними кіберзлочинами, стрімким розвитком штучного інтелекту, Інтернету речей і децентралізованих цифрових систем. Одним із найбільш суттєвих викликів залишається проблема доказовості та юрисдикції в кіберпросторі, оскільки анонімність дій і відсутність чітких територіальних меж зумовлюють потребу в оновленні підходів до юрисдикційного підпорядкування, міжнародної взаємодії (зокрема через MLATs), а також гармонізації процесуальних норм щодо електронних доказів [6, с. 183].

Актуальні тенденції правового регулювання кібербезпеки формуються під впливом цифрової трансформації та технологічних інновацій. Нагальною є адаптація нормативної бази до особливостей функціонування AI, IoT і blockchain, що передбачає формування чітких правових дефініцій, визначення меж відповідальності автономних алгоритмів, а також перегляд стандартів захисту даних. Одночасно постає завдання забезпечити баланс між публічною безпекою та правами на приватність – з урахуванням ризиків, пов'язаних із масовим моніторингом, збиранням даних і профілюванням. Це зумовлює потребу в правовій легітимації таких практик і запровадженні незалежного контролю (наприклад, через інститути кіберетики). Окремою проблемою залишається правова невизначеність: відсутність чітких критеріїв допустимості електронних доказів, суперечливість норм і спроби застосування загальних правових конструкцій до високоспецифічних цифрових явищ, що загрожує як правовим вакуумом, так і надмірною формалізацією [2, с. 110–111].

Пропозиції щодо вдосконалення:

1. Розробити універсальну нормативну рамку для цифрових доказів, яка передбачатиме стандарти збору, верифікації та зберігання слідів у мережі.

2. Інтегрувати принципи «технологічної нейтральності» в законодавство, щоб уникнути його надмірної прив'язки до конкретних технічних рішень.

3. Запровадити адаптивні механізми нормативного прогнозування, зокрема через створення міждисциплінарних експертних груп при органах законодавчої влади.

4. Гармонізувати українське законодавство з ключовими європейськими актами, як-от NIS2, GDPR, DORA, для забезпечення сумісності правових режимів [7, с. 37].

Висновки. Отже, юридичний супровід кіберінцидентів є багатокомпонентним і міждисциплінарним інструментом, що охоплює не лише процесуальне реагування на кібератаки та витоки конфіденційної інформації, але й превентивні заходи, побудову внутрішньої комплаєнс-системи, а також забезпечення належного обігу електронних доказів. Його ефективність залежить від здатності правника діяти на перетині технологічних, правових і організаційних сфер у тісній взаємодії з державними та міжнародними інституціями.

Незважаючи на поступову еволюцію національного підходу до кібербезпеки, чинне нормативне поле залишається фрагментарним і потребує гармонізації з міжнародними стандартами, зокрема у сфері доказовості, юрисдикції та відповідальності цифрових агентів. Перспективи подальших досліджень вбачаються у розробці моделей правового реагування із залученням штучного інтелекту, формалізації процедур цифрової криміналістики та визначенні правових меж приватності в умовах гібридних кіберконфліктів.

Список літератури:

1. Левченко О. М., Левченко А. О., Немченко Т. А. Захист конфіденційної таємниці в контексті стратегічного управління економічною безпекою організації в умовах цифровізації економіки. *Центральноукраїнський науковий вісник. Економічні науки.* Вип. 6 (39). 2021. С. 20–30. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/1582418 (дата звернення: 10.07.2025). DOI: https://doi.org/10.32515/2663–1636.2021.7(40). 20–30

2. Ніконенко У., Халіна О. Організаційно-правовий механізм забезпечення кібербезпеки соціально-економічних систем в умовах викликів сучасності. *Економічний простір*. 2024. №190. С. 108–113. DOI: https://doi.org/10.32782/2224–6282/190–20

3. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право.* 2021. № 2 (37). С. 129–138. DOI: https://doi.org/10.37750/2616–6798.2021.2(37).238348

4. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка». Сер.: Юридичні науки.* 2024. Т. 11. №1 (41). С. 314–320. DOI: DOI: https://doi.org/10.23939/law2024.41.314

5. Стендер С. В., Фротер О. С., Снітко Ю. М. Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії. *Академічні візії*. 2023. №26. URL: https://academy-vision.org/index.php/av/article/view/799 (дата звернення: 09.07.2025). DOI: http://dx.doi.org/10.5281/zenodo.10389831

6. Шевчук М. О. Основні аспекти механізму забезпечення інформаційної безпеки підприємницької діяльності. *Науковий вісник Ужгородського національного університету. Сер.: Право.* 2024. Вип. 85 (3). С. 181–186.

7. Kravchuk M., Kravchuk V., Hrubinko A. Cyber security in Ukraine: Theoretical view and legal regulation. *Law, Policy & Security.* 2024. №2 (2). P. 28–38. doi: https://doi.org/10.62566/lps/2.2024.28

8. Semenchenko A. I., Pleskach V. L., Zaiarnyi O. A., Pleskach M. V. Organizational and legal mechanisms of cybersecurity and cyber defense in Ukraine: essentiality, conditions and development prospects. *Problems in Programming.* 2021. №2–3. 278–286. DOI: https://doi.org/10.15407/pp2020.02–03.278

9. Tkachov A., Korolov R., Rahimova I. and etc. Cybersecurity challenges and solutions for critical infrastructure protection. *Ukrainian Scientific Journal of Information Security.* 2024. Vol. 30. Issue 1. P. 58–66. DOI: https://doi.org/10.18372/2225–5036.30.18604

Gnediuk V. L. LEGAL SUPPORT IN CASE OF CYBERATTACKS OR CONFIDENTIAL INFORMATION LEAKAGE

The article presents a comprehensive study of the legal support of cyber incidents, particularly cyberattacks and confidential information leaks, as one of the key challenges in the field of modern digital security. In the context of the transformation of the information space and the growing cyber-dependence of critical functions of the state, business, and society, the issue of legal response to cyber threats is acquiring fundamentally new dimensions. Based on a systematic analysis of current Ukrainian legislation and international standards, the article examines the specific features of legal regulation in the field of information security, qualification of cyber incidents, circulation of electronic evidence, and procedural support of digital offenses.

It has been established that the existing legal system is characterized by a low level of procedural consistency in the documentation and proof of cyber incidents, fragmentation of the regulatory framework, and limited procedural tools for interagency coordination. It is substantiated that effective legal support requires a combination of preventive measures (security audits, internal policies, contractual frameworks), reactive procedures (notification of authorities, collection of digital evidence, legal representation), and communication-based reputation protection. Particular attention is given to the role of the legal professional in the context of a cyber incident, taking into account compliance requirements, transnational jurisdiction, involvement in digital forensics, and protection of data subjects' rights.

The study also highlights current challenges in the use of electronic evidence in criminal and civil proceedings, including issues related to verification, admissibility, and judicial interpretation of digital traces. Mechanisms of international cooperation in combating cybercrime are disclosed, including the role of MLATs and the potential of cooperation with organizations such as INTERPOL, ENISA, and Europol EC3.

The generalization of the findings has allowed the authors to propose practical directions for improving the legal regulation of legal support in response to cyber incidents.

Key words: *legal support, cyber incident, cyberattack, confidential information, electronic evidence, compliance, digital security.*

Дата надходження статті: 31.08.2025
Дата прийняття статті: 01.10.2025
Опубліковано: 15.12.2025