НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ІТ-ПРАВО ПІД ЧАС ГІБРИДНОЇ ВІЙНИ: ВІД ПОШУКУ ПАРАДИГМИ ДО ПРАГМАТИЧНИХ РІШЕНЬ

Колективна монографія

За редакцією
Є. Харитонова, О. Харитонової, І. Давидової

Одеса
Фенікс
2025

УДК 340:004:327:355
І-87

Рекомендовано рішенням вченої ради
Національного університету «Одеська юридична академія»
(протокол № 9 від 30 червня 2025 р.)

Рецензенти:

Майданик Р. А. – академік НАПрН України, доктор юридичних наук, професор, професор кафедри цивільного процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка;

Соколов А. В. – доктор технічних наук, професор, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»;

Маковій В. П. – кандидат юридичних наук, професор, завідувач кафедри цивільно-правових дисциплін Одеського державного університету внутрішніх справ.

І-87 **ІТ-право під час гібридної війни: від пошуку парадигми до прагматичних рішень** : кол. монографія / за заг. ред. проф.: Є. Харитонова, О. Харитонової, І. Давидової. – Одеса : Фенікс, 2025. – 588 с.
ISBN 978-617-8430-70-2

Монографія є продовженням циклу праць колективу кафедри цивільного права Національного університету «Одеська юридична академія», присвячених результатам досліджень цивілістичних шкіл університету від часу їхнього формування до гібридної війни, що триває нині. У третьому томі аналізуються в контексті гібридної війни: проблеми визначення концепту «ІТ-право», особливості правового регулювання відносин, що виникають у зв'язку з використанням інформаційних технологій, особливості механізму цивільно-правового регулювання у сфері ІТ, чинник симулякру, значення та роль інформаційного середовища як стратегічного ресурсу, правові рамки для цифрових активів і перспективи цифрової власності, ІТ-правочини, порушення прав інтелектуальної власності в Інтернет, протидія кіберзагрозам у гібридній кібервійні, загрози вербування неповнолітніх через соцмережі та месенджери та юридичні заходи запобігання таким загрозам, правове регулювання стартапів, е-кредитування, цивільно-правова відповідальність за шкоду, завдану кібератаками, забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні та ін.

Авторський колектив концентрував увагу на обґрунтуванні необхідності комплексного вирішення практичних питань впорядкування інформаційно-технологічні відносини в умовах гібридної російсько-української війни. Автори прагнули розкрити особливості правового регулювання цих відносин і запропонувати власне бачення шляхів вирішення проблем, що виникають у цій сфері. Усвідомлюючи спірність низки висновків і пропозицій, автори розраховують на продовження плідних дискусій з проблем правового регулювання інформаційних технологій, зокрема в умовах гібридної війни.

Монографія може бути цікавою науковцям, практикуючим юристам, викладачам, аспірантам, здобувачам вищої освіти, а також широкому загалу небайдужих українців, які цікавляться проблемами правового регулювання у сфері ІТ, зокрема під час гібридної війни.

УДК 340:004:327:355

ISBN 978-617-8430-70-2

ЗМІСТ

Авторський колектив

Харитонов Євген (ORCID ID: 0000-0001-5521-0839), доктор юридичних наук, професор, член-кореспондент НАПрН України, зав. кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з О. Харитоновою, І. Давидовою); розділ 2 (у співав. з О. Харитоновою); розділ 3 (у співав. з О. Харитоновою); розділ 4 (у співав. з О. Харитоновою); розділ 5 (у співав. з О. Харитоновою); розділ 11 (у співав. з О. Харитоновою); розділ 14 (у співав. з О. Харитоновою);

Харитонова Олена (ORCID ID: 0000-0002-9681-9605), докторка юридичних наук, професорка, членкиня-кореспондент НАПрН України, зав. кафедри права інтелектуальної власності і патентної юстиції НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, І. Давидовою); розділ 2 (у співав. з Є. Харитоновим); розділ 3 (у співав. з Є. Харитоновим); розділ 4 (у співав. з Є. Харитоновим); розділ 5 (у співав. з Є. Харитоновим); розділ 11 (у співав. з Є. Харитоновим); розділ 14 (у співав. з Є. Харитоновим);

Давидова Ірина (ORCID ID: 0000-0001-5622-671X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, О. Харитоновою); розділ 9;

Некіт Катерина (ORCID ID: 0000-0002-3540-350X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 7;

Сафончик Оксана (ORCID ID: 0000-0001-6781-8219), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 19;

Бааджи Наталія (ORCID ID: 0000-0002-9889-4879), кандидатка юридичних наук, доцента, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 10;

Берназ-Лукавецька Олена (ORCID ID: 0000-0002-2133-1672), кандидатка юридичних наук, доцента, доцентка кафедри цивільного права НУ «ОЮА»: розділ 17;

Галупова Лариса (ORCID ID: 0000-0001-6263-2773), кандидатка юридичних наук, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з А. Кирилюк);

Дрогозюк Крістіна (ORCID ID: 0000-0001-9254-9575), кандидатка юридичних наук, доцента, доцентка кафедри цивільного, нотаріального та виконавчого процесу НУ «ОЮА»: розділ 20;

Калітенко Оксана (ORCID ID: 0000-0003-1001-3561)**,** кандидатка юридичних наук, доцентка, професорка кафедри цивільного права НУ «ОЮА»: розділ 6;

Кирилюк Алла (ORCID ID: 0000-0002-3051-6599), кандидатка юридичних наук, доцентка, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з Л. Галуповою);

Омельчук Олександр (ORCID ID: 0000-0002-0082-3619), кандидат юридичних наук, доцент, доцент кафедри цивільного права НУ «ОЮА»: розділ 12;

Ткалич Максим (ORCID ID: 0000-0003-4224-7231), кандидат юридичних наук, доцент, доцент кафедри цивільного права Запорізького національного університету: розділ 21 (у співав. з Ю. Толмачевською);

Токарева Віра (ORCID ID: 0000-0002-8409-1477), кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права НУ «ОЮА»: розділ 13;

Толмачевська Юлія (ORCID ID: 0000-0002-7964-8875), докторка філософії (081 право): розділ 21 (у співав. з О. Ткаличем);

Фасій Богдан (ORCID ID: 0000-0002-8715-930X), кандидат юридичних наук, доцент, декан факультету судового та міжнародного права НУ «ОЮА»: розділ 18;

Розумейко Дмитро (ORCID ID: 0000-0001-8206-1031)**,** аспірант кафедри цивільного права НУ «ОЮА»: розділ 16;

Рябченко Вікторія (ORCID ID: 0009-0007-1542-6492)**,** аспірантка кафедри цивільного права НУ «ОЮА»: розділ 15.

Розділ 18

ЦИВІЛЬНО-ПРАВОВА ВІДПОВІДАЛЬНІСТЬ ЗА ШКОДУ, ЗАВДАНУ КІБЕРАТАКАМИ

DOI

Богдан Фасій
кандидат юридичних наук, доцент

У сучасному інформаційному суспільстві, яке характеризується стрімким розвитком цифрових технологій та їх глибокою інтеграцією у усі сфери суспільного життя, питання цивільно-правової відповідальності за шкоду, завдану кібератаками набуває особливої актуальності. Масштабність та складність кіберзагроз, які охоплюють як фізичних особі, так і юридичних осіб та державні інституції, зумовлюють необхідність вироблення ефективних механізмів притягнення до відповідальності, здатних забезпечити належний рівень правового захисту та мінімізувати негативні наслідки для правопорядку.

Кібератаки можуть завдавати значної матеріальної та моральної шкоди, що зумовлює потребу у встановленні чітких правових критеріїв щодо відшкодування збитків та визначення суб'єктного складу відповідальних осіб. Особливості вчинення правопорушення у кіберпросторі, зокрема складність ідентифікації правопорушника, транскордонний характер кіберзлочинності, а також використання новітніх технологій для приховування слідів злочину, створюють значні виклики для правозастосування практики.

Проблематика цивільно-правової відповідальності за шкоду, завдану кібератаками, займає важливе місце в сучасному правовому полі, оскільки цифровізація суспільних відносин створює нові загрози правам та законним інтересам фізичних та юридичних осіб. Наукова доктрина пропонує низку концептуальних підходів до визначення правової природи та механізмів реалізації відповідальності в умовах кіберпростору, однак єдиного узгодженого підходу в межах цивільного права наразі не вироблено, що обумовлює необхідність подальшого наукового дискурсу[1].

[1] Підопригора О. А. Цивільно-правова відповідальність: теорія та практика. Київ: Юрінком Інтер, 2020. С. 15.

Одним із домінантних підходів у цивілістиці є концепція деліктної відповідальності, що ґрунтується на традиційних юридичних конструкціях, які передбачають наявність шкоди, протиправні діяння, причинно-наслідковий зв'язок та вину правопорушника[1]. Однак у випадку кібератак застосування загальних положень деліктного права стикається з труднощами, зокрема у зв'язку з анонімністю суб'єкта правопорушень, складністю ідентифікації джерела кібератаки та встановлення причинного зв'язку між конкретними діями порушника та заподіяною шкодою[2]. Додатковою проблемою є питання про можливість притягнення до відповідальності суб'єктів, які не є безпосереднім ініціаторами атаки, але створили передумови для її реалізації, зокрема власників вразливих інформаційних систем чи операторів цифрових платформ, які не забезпечують належний рівень кібербезпеки.

Альтернативний науковий підхід до цієї проблематики передбачає застосування концепції об'єктивної відповідальності у випадках, коли шкода є наслідком недотримання стандартів інформаційної безпеки[3]. Така модель відповідальності є поширеною в правових системах, що ґрунтуються на ризик-орієнтованому регулюванні, і передбачає, що суб'єкти господарювання, які здійснюють обробку великих масивів персональних даних або забезпечують функціонування критичної цифрової інфраструктури, несуть відповідальність незалежно від їхньої вини у разі порушення безпеки, якщо не доведуть, що вжили всіх необхідних заходів для запобігання настання шкоди[4]. Вказаний підхід є характерним для правового регулювання ЄС, де відповідальність за витік даних чи порушення кібербезпеки покладається на контролерів та операторів інформаційних систем навіть у разі, якщо зловмисники діяли автономно.

Наукова дискусія також охоплює питання про можливість застосування договірних механізмів відповідальності у випадку, коли

---

1 Штефан М. Й. Деліктне право України: сучасний стан та перспективи розвитку. Харків: Право, 2019. С. 92

2 Хом'як В. В. Інформаційна безпека та правові аспекти її забезпечення. Львів: Галицький інститут, 2021. С. 47.

3 Вдовиченко П. А. Цивільно-правові аспекти відповідальності у сфері цифрових технологій. Одеса: Фенікс, 2022. С. 61.

4 European Union Agency for Cybersecurity (ENISA). *Cybersecurity Act and its implications.* Luxembourg: Publications Office of the European Union. 2020. P.73.

правовідносини між потерпілим та потенційним відповідачем мають контрактний характер[1]. В умовах цифрової економіки значна частина кібератак завдає шкоди суб'єктам, які перебувають у договірних відносинах із операторами цифрових послуг, фінансових платформ чи хмарних сервісів, що ускладнює кваліфікацію відповідних правопорушень виключно як деліктів[2]. Деякі науковці обґрунтовують необхідність закріплення презумпції договірної відповідальності у випадках порушення безпеки даних або неналежного виконання зобов'язань щодо захисту інформації, що уможливлює застосування жорсткіших санкцій до постачальників цифрових послуг, які не забезпечили належний рівень кіберзахисту.

Важливим аспектом проблематики є транскордонний характер кібератак, що зумовлює необхідність міжнародно-правової координації механізмів цивільно-правової відповідальності. Відсутність єдиних міжнародних стандартів щодо юрисдикції, застосовного права та механізмів правового захисту потерпілих створює ситуацію правової невизначеності, що перешкоджає ефективному притягненню до відповідальності осіб, які здійснюють кібератаки[3]. У зв'язку з цим у доктрині висловлюється необхідність розроблення спеціальних міжнародних угод, які б передавали єдині підходи до визначення юрисдикції у справах, пов'язаних із кібератаками, а також процедурні механізми співпраці між державами у сфері судового захисту прав потерпілих.

Окремого розгляду в науковій літературі заслуговує концепція орієнтованого регулювання кібербезпеки, яка передбачає впровадження превентивних заходів для мінімізації ризиків правопорушень у кіберпросторі. Відповідно до цього підходу, цивільно-правова відповідальність має заповнюватись механізмами кіберстрахування, корпоративного комплаєнсу та аудиту інформаційної безпеки, що дозволяє мінімізувати ймовірність завдання шкоди та покласти частину фінансових ризиків на спеціалізовані інститути страхування кіберзагроз.

---

1 Kuner C. Data Protection Law and International Jurisdiction on the Internet. *International Journal of Law and Information Technology*. 2018. Vol. 26. №. 2. P. 1-20.

2 Koops B. J. The Trouble with European Data Protection Law. *International Data Privacy Law*. 2019. Vol. 9. №. 1. P. 5-12.

3 Hartzog W. Privacy's Blueprint: The Battle to Control the Design of New Technologies. Harvard University Press, 2018. 312 p.

Кіберстрахування є порівняно, новим явищем у правовому просторі, тому потребує ґрунтовного дослідження питання використання його як механізму захисту від ризиків, що виникають (можуть виникнути) внаслідок кібератак.

Кіберстрахування – це спеціалізований вид страхування, спрямований на захист організацій та фізичних осіб від фінансових втрат, пов'язаних з інцидентами в кіберпросторі, такими як кібератаки, витоки даних або збої в інформаційних системах. Це інструмент управління ризиками, який дозволяє передати фінансову відповідальності за можливі кіберінциденти страховій компанії, забезпечуючи тим самим фінансову стабільність та безпеку суб'єктів господарювання[1].

Кіберстрахування є новим явищем не лише для України, а й для всього світу. За даними Munich Re за 2018 рік, такий вид захисту надається лише 60 страховими компаніями у різних країнах, причому охоплення кіберризиків поки що залишається обмеженим – застраховано лише 5% таких ризиків[2]. Однак стрімке зростання кіберзагроз, викликаних діяльністю хакерів, сприяє активному розвитку цього сектора. За оцінками страхової групи Allianz, ринок кіберстрахування щорічно демонструє приріст на 25-50%[3].

США по праву можна вважати лідером у сфері кіберстрахування завдяки розвиненій IT-інфраструктурі, першому виявленню серйозних кіберзагроз для бізнесу та жорсткому законодавчому регулюванню захисту персональних електронних даних. Кіберстрахування є одним із найдинамічніших сегментів глобального ринку страхових послуг і розглядається як ефективний інструмент управління ризиками та захисту бізнесу від загроз, що супроводжують електронну комерцію.

До ключових ризиків, які покривають кіберстрахування, належать:

- викрадення конфіденційної інформації співробітниками компанії;
- викрадення відомостей щодо кредитних карт;
- незаконне виведення коштів із рахунків;
- втрата носіїв інформації;

---

[1] Нагайчук Н. Страхування в системі управління кібер-ризиками підприємства в умовах цифрової економіки. URL: https://www.academia.edu/116320960/Страхування_в_системі_управління_кібер_ризиками_підприємства_в_умовах_цифрової_економіки

[2] Підсумки 2018. URL: https://cyberpolice.gov.ua/results/2018/

[3] Селіверстова Л. С., Трухан Д. А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. *Економіка та держава.* 2020. № 1. С. 23-26.

- фішинг-атаки;
- кібервимагання;
- збої в роботі комп'ютерних мереж через хакерські атаки.

Основною метою кіберстрахування залишається захист від масштабних хакерських атак, здатних завдати значної фінансової та репутаційної шкоди.

Популярність цього виду страхування у розвинених країнах пояснюється розумінням того, що навіть за умови впровадження передових технологій кібербезпеки та регулярного навчання персоналу завжди залишається мінімальний ризик компрометації системи, який складно передбачити чи оцінити[1].

Основними механізми кіберстрахування є процеси андеррайтингу, оцінки ризиків, встановлення страхових премій та врегулювання претензій. Андеррайтинг включає в себе оцінку кіберизиків конкретної організації, аналіз її інформаційної безпеки та визначення відповідних умов страхування[2]. Цей процес є важливим, оскільки правильна оцінка ризиків дозволяє страховикам встановлювати адекватні страхові премії та умови покриття. Встановлення страхових премій базується на аналізі ймовірності настання кіберінцидентів та потенційних збитків. Страхові компанії використовують статистичні дані, моделі ризиків та інформацію про попередні інциденти для визначення розміру премій. Це дозволяє забезпечити фінансову стійкість страховика та адекватне покриття страховика.

Врегулювання претензій є ключовим етапом у механізмі кіберстрахування. Після настання кіберінциденту страхувальник подає претензію до страхової компанії, яка проводить розслідування, оцінює збитки та здійснює відповідні виплати. Цей процес вимагає тісної співпраці між страховиком та страхувальником для забезпечення швидкого відновлення бізнес-процесів та мінімізації негативних наслідків інциденту[3].

---

[1] Shaun S. Wang. Integrated Framework for Information Security. Investment and Cyber Insurance. Wang, Shaun, Integrated Framework for Information Security Investment and Cyber Insurance (September 15, 2017). URL: https://ssrn.com/abstract=2918674

[2] Jason R. C. Nurse. The Data that Drives Cyber Insurance: *A Study into the Underwriting and Claims Processes* / Jason R. C. Nurse, Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, Sadie Creese. URL: https://arxiv.org/pdf/2008.04713

[3] Ruperto P. Majuca. The Evolution of Cyberinsurance / Ruperto P. Majuca, William Yurcik, Jay P. Kesan. URL: https://arxiv.org/pdf/cs/0601020

Важливим аспектом кіберстрахування є управління моральним ризиком та проблеми асиметрії інформації. Страхові компанії розробляють спеціальні умови та вимоги до страхувальників, такі як впровадження політик кібербезпеки, регулярні аудити та навчання персоналу, щоб знизити ймовірність настання інцидентів та забезпечити прозорість у відносинах зі страхувальником[1].

Кіберстрахування також стимулює організації до підвищення рівня кібербезпеки. Наявність страхового покриття спонукає компанії впроваджувати кращі практики та стандарти захисту інформації, оскільки це впливає на умови страхування та розмір премій. Таким чином кіберстрахування відіграє важливу роль у загальному підвищенні кіберстійкості суб'єктів господарювання та суспільства в цілому.

Розвиток кіберстрахування в Україні знаходиться на початковому етапі. На нашу думку, основними перешкодами для впровадження кіберстрахування є низька обізнаність бізнесу про кіберризики, відсутність статистичних даних та недостатній рівень кібербезпеки в організаціях. Однак, з огляду на зростання кількості кіберінцидентів та цифровізацією економіки, потреба в кіберстрахуванні стає все більш актуальною.

Для стимулювання розвитку кіберстрахування в Україні необхідно розробити нормативно-правову базу, що регулює цей вид страхування, а також підвищувати обізнаність бізнесу про важливість кібербезпеки та можливості страхового захисту. Крім того, необхідним є співпраця між страховими компаніями, державними органами та експертними організаціями у сфері кібербезпеки може стати ефективним механізмом успішного впровадження кіберстрахування[2].

Таким чином, кіберстрахування є важливим елементом сучасної системи управління ризиками, який забезпечує фінансовий захист від кіберзагроз. Розвиток цього інструменту в Україні вимагає комплексного підходу, включаючи вдосконалення законодавства, підвищення рівня кібербезпеки та обізнаності бізнесу про переваги кіберстрахування. Це сприятиме підвищенню стійкості національної економіки до кіберзагроз та забезпечить захист інтересів як юридичних, так і фізичних осіб у цифровому середовищі.

[1] Галатюк К. О., Лозова В. О. Явище інформаційної асиметрії на ринку страхування. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/11/259.pdf

[2] Приказюк Н. В., Гуменюк Л. С. Дорожня карта впровадження кібер-страхування в Україні. *Innovation and Sustainability.* 2021. № 1. С. 68.

На сьогоднішній день, підходи до питань цивільно-правової відповідальності за шкоду завдану кібератаками засвідчують відсутність єдиного підходу до визначеної проблематики. Очевидно, що традиційні конструкції цивільного права потребують адаптації до нових технологічних реалій, що передбачає формування гібридних правових механізмів, які поєднують елементи деліктної, договірної та об'єктивної відповідальності, а також забезпечують ефективні механізми міжнародного співробітництва у сфері захисту прав осіб, які постраждали внаслідок кібератак.

Для ґрунтовного дослідження питань відповідальності за шкоду завдану кібератаками, необхідно визначити правову природу поняття «кібератаки». У міжнародному праві термін «кібератака» немає єдиного загальноприйнятого визначення, що пов'язано з різними концептуальними підходами держав та міжнародних організацій до кваліфікації протиправних дій у кіберпросторі. Одним із перших міжнародних документів, що визначає основи регулювання кіберзагроз, є Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція, 2001 р.)[1]. Вона не містить безпосереднього визначення поняття «кібератака», однак описує категорію комп'ютерних злочинів, зокрема несанкціонований доступ до комп'ютерних систем, втручання в дані та систему, а також комп'ютерне шахрайство та підробку[2].

Іншим ключовим документом є Талліннський посібник із застосування міжнародного права до кібероперацій (Tallinn Manual 2.0, 2017), який визначає кібератаку як «дію або серію пов'язаних дій, спрямованих на цілеспрямоване порушення конфіденційності, цілісності або доступності інформації, інформаційних систем і мереж»[3]. При цьому, у рамках міжнародного гуманітарного права кібератаки можуть кваліфікуватися як «напади» відповідно до ст. 49 Додаткового протоколу I до Женевських конвенцій, якщо вони завдають шкоди об'єктам або людям[4].

[1] Конвенція Ради Європи про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

[2] Convention on Cybercrime (Budapest Convention). Council of Europe. 23 November 2001. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[3] Schmitt M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017. P. 23.

[4] Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року. URL: https://zakon.rada.gov.ua/laws/show/995_199#o315

Окремі міжнародні організації також формулюють власні визначення. Наприклад, НАТО розглядає кібератаку як «навмисне використання комп'ютерних технологій для створення руйнівного впливу на інформаційні системи», а Європейський Союз у Директиві 2013/40/EU визнає «незаконний доступ, втручання та перехоплення даних» як ключові форми кібератак[1].

Таким чином, міжнародно-правові підходи до визначення кібератаки відзначаються відсутністю уніфікованого визначення, але в загальному сенсі охоплюють умисні дії, спрямовані на порушення роботи інформаційних систем, завдання шкоди інфраструктурі або отримання неправомірного доступу до даних.

На національному рівні визначення кібератак також варіюються залежно від правової традиції на рівні регулювання кіберпростору. В українському законодавстві термін «кібератака» прямо не визначений, проте Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII визначає «кіберінцидент» як подію, яка може призвести до порушення кібербезпеки, а «кіберзагрозу» як сукупність умов та чинників, що створюють небезпеку в кіберпросторі[2]. Таким чином, на рівні законодавства кібератаки можуть розглядатись через призму кіберзагроз та інцидентів. Для повного та всебічного розуміння специфіки даних понять необхідно визначити їх співвідношення та черговість проявів в цифровому просторі. Так, поняття «кіберінцидент», «кіберзагроза» та «кібератака» є ключовими в сфері кібербезпеки, кожне з яких відображає різні аспекти взаємодії з інформаційними системами та мережами. Розуміння їх співвідношення є важливими для ефективного управління ризиками та забезпечення захисту інформаційних ресурсів.

Кіберзагроза (англ. cyber threat) – це потенційно можливі явища або чинники, які можуть створювати небезпеку для інформаційних систем, мереж або даних. Вони включають у себе вразливості, які можуть бути використані зловмисниками для несанкціонованого доступу або пошкодження інформації. Загрози можуть бути як внутрішніми (наприклад, недбалість працівників), так і зовнішніми (наприклад, дії хакерів).

[1] Directive 2013/40/EU on attacks against information systems. Official Journal of the European Union. 2013. L218. P. 8-14.

[2] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

Кібератака (англ. cyber attack) – це цілеспрямовано дія, спрямована на реалізацію кіберзагрози. Вона передбачає використання вразливостей в інформаційних системах для досягнення певних цілей, таких як крадіжка даних, порушення роботи систем або їх знищення. Прикладом кібератаки є використання шкідливого програмного забезпечення для отримання несанкціонованого доступу до системи.

Кіберінцидент (англ. cyber incident) – це подія або сукупність подій, які ставлять під загрозу цілісність, конфіденційність або доступність інформаційних систем, мереж або даних. Кіберінцидент може бути результатом як навмисних дій (кібератак), так і ненавмисних подій (технічні збої, посилки користувачів). Він є фактичним проявом кіберзагрози, яка може або не може бути результатом кібератаки.

Отже, співвідношення між цими поняттями можна представити наступним чином: кіберзагроза є потенційною можливістю виникнення небезпеки для інформаційних систем. Коли ця загроза реалізується через цілеспрямовані дії зловмисників, ми маємо справу з кібератакою. Якщо внаслідок кібератаки або інших факторів відбувається подія, яка порушує нормальне функціонування інформаційних систем, це вважається кіберінциндентом.

Таким чином, кіберзагроза є потенційною небезпекою, кібератака – це реалізація цієї небезпеки через навмисні дії, а кіберінцидент – це результат, який може виникнути внаслідок кібератаки або інших подій, що впливають на інформаційну безпеку.

У Кримінальному кодексі України поняття кібератаки також прямо не закріплено, проте його можна розглядати через такі склади злочинів:

– несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України);
– Створення, розповсюдження або збут шкідливих програмних чи технічних засобів, а також несанкціоноване збирання, зберігання та передача інформації з обмеженим доступом (ст. 361-1, 362 КК України)[1].

[1] Кримінальний кодекс України: Закон України. *Відомості Верховної Ради України.* 2001. № 25-26. Ст. 131.

Щодо зарубіжних країни, то у США згідно із Законом про комп'ютерне шахрайство та зловживання (Computer Fraud and Abuse Act, 1986) кібератака визначається як «несанкціоноване проникнення або пошкодження інформаційної системи, що призводить до значних фінансових втрат або загрози національній безпеці»[1]. У Німеччині Закон про безпеку інформаційних технологій (IT-Sicherheitsgesetz, 2015) визначає кібератаку як «навмисне використання шкідливих програм або інших технічних засобів для порушення функціонування цифрових інфраструктур»[2].

Зіставлення національних та міжнародних нормативних актів, які містять згадку про кібератаки, дає можливість виокремити такі основні підходи до розуміння даного явища:

1. Функціональний підхід – робить акцент на наслідках кібератаки (порушення конфіденційності, цілісності даних, того).

2. Суб'єктний підхід – визначення відповідальності держав, приватних осіб або транснаціональних організацій за проведення кібератак.

3. Технологічний підхід – увага до технічних аспектів атак, таких як використання шкідливого програмного забезпечення, DDoS-атаки тощо.

4. Правовий підхід – кваліфікація кібератак в межах національного кримінального, цивільного або адміністративного права.

З точки зору цивільного права, кібератака може бути визначена як протиправне посягання на інформаційні системи, електронні комунікаційні мережі чи дані з метою завдання шкоди фізичній особі, юридичній особі чи державі, що може спричинити майнову та немайнову шкоду, порушення договірних зобов'язань або іншим чином вплинути на приватно-правові відносини. Таким чином, у цивільному праві кібератака розглядається не лише як технологічний злочин, а й як юридичний факт, що тягне за собою правові наслідки, зокрема відшкодування збитків та відновлення порушених прав.

Загалом, проблема визначення кібератак залишається дискусійною, і сучасні тенденції вказують на необхідність розробки єдиного міжнародного підходу, який би врахував транскордонний характер кіберзагроз та встановлював уніфіковані критерії відповідальності за

[1] Computer Fraud and Abuse Act (CFAA). U. S. Code, Title 18, Section 1030, 1986.

[2] IT-Sicherheitsgesetz. Bundesministerium des Innern, 2015. URL: https://www.bmi.bund.de

їх вчинення. Наприклад, лише в листопаді та грудні 2016 року Україна зазнала 6500 кібератак. Окрім інформаційної пропаганди та викрадення важливих даних, російські хакери атакували й енергетичну інфраструктуру столиці. 17 грудня 2016 року в Києві на короткий час зникло електропостачання. Розслідування показало, що ця атака була пов'язана з іншими зломами – систем «Укрзалізниці», Міністерства фінансів і Пенсійного фонду України. Подібні втручання траплялися й раніше. У грудні 2015 року без світла тимчасово залишилися 230 тисяч жителів Києва. Експерти з Information Systems Security Partners (ISSP), які досліджували ситуацію для «Укренерго», вважають, що ці атаки були взаємопов'язаними. Хоча їхні наслідки вдалося швидко ліквідувати, фахівці припускають, що вони мали на меті продемонструвати можливості зловмисників. Україна стала випробувальним майданчиком для російських хакерів. Ще одна масштабна кібератака, відома як BugDrop, відбулася в лютому 2017 року. Її організатори залишаються невідомими. Загрозу виявила міжнародна компанія CyberX, яка оприлюднила офіційне розслідування на своєму сайті[1].

Відомий український дослідник у сфері кібербезпеки, професор В. Л. Бурячок, визначає поняття «кібератака» як комплекс узгоджених за метою, змістом і часом дій (кіберакцій), спрямованих на певний об'єкт впливу. Метою таких атак є порушення конфіденційності, цілісності, доступності, спостережуваності або авторства інформації, що в ньому циркулює, враховуючи її вразливість. Також кібератаки можуть призводити до збоїв у роботі ІТ-систем і мереж цього об'єкта[2].

Як влучно зазначають Бондаренко І. Д. та Шестаков В. І. більшість кібератак, спрямовані на Україну, не спричинили безпосереднього фізичного руйнування обладнання чи загибелі людей, однак під час розробки Tallinn Manual 2.0 його автори розглядали саме ці фактори як визначальні для набуття кібератакою правового статусу «атаки» відповідно до норм міжнародного гуманітарного права, адже здійснення таких дій проти цивільних об'єктів і населення є воєнним злочином. Попри це, кібератаки, подібно до застосування кінетичної зброї, виводили з ладу критично важливі інфраструктурні об'єкти

[1] Всесвітній огляд економічних злочинів. *Кіберзлочини в центрі уваги.* URL: https://www.pwc.com/ua/en/services/forensic/assets/gecs_2011_report_ukraine_ukr.pdf

[2] Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ: НАУ, 2013. 432 с.

шляхом знищення або пошкодження їхнього штатного програмного забезпечення, що призводило до порушення основних функцій цих об'єктів, включно з життєво необхідними для цивільного населення[1]. Наприклад, відключення електропостачання значної кількості споживачів, а також систем теплогенерації та лікарень у зимовий період створювало безпосередню загрозу життю та здоров'ю населення.

Реальне усвідомлення критичної небезпеки наслідків кібератак упродовж останніх років зумовило значний перегляд підходів європейських і американських науковців до так званого «порогу серйозності» (gravity threshold), який визначає, чи може певний кіберінцидент бути кваліфікований як «атака» за нормами міжнародного гуманітарного права. Зокрема, у науковій спільноті посилюється позиція щодо того, що самі комп'ютерні дані, особливо в системах управління критичною інфраструктурою, можуть розглядатися як об'єкт атаки, навіть за відсутності фізичних руйнувань чи людських жертв[2].

На основі вищезазначеного, може стверджувати, що кібератака є складним і багатогранним явищем, що потребує міждисциплінарного дослідження, оскільки вона має широкий вплив на суспільство, державу, економіку та міжнародну безпеку. З технічної точки зору кібератаки пов'язані з використанням шкідливого програмного забезпечення, фішингових атак, DDoS-атак та інших методів, що спрямовані на компрометацію інформаційних систем. Правовий підхід до дослідження кібератак дає можливість вивчити межі відповідальності, правові наслідки та способи правового реагування. Кібератаки також розглядаються у військовому та геополітичному контексті, оскільки вони стали інструментом гібридної війни, інформаційних конфліктів та дипломатичного тиску. З економічної точки зору кібератаки досліджують як дії, що завдають значних фінансових втрат підприємствам, банківським установам і державним органам, що порушує економічну стабільність та підриває довіру до цифрових технологій. З соціальної точки зору, кібератаки вивчають механізми впливу на суспільні настрої, породжують страх, дестабілізують громадську думку та сприяють поширенню дезінформації.

[1] Бондаренко І. Д. Шестаков В. І. Кібератаки РФ на Україну – воєнний злочин. *Юридичний науковий електронний журнал.* 2023. № 11. С. 614-619. URL: http://www.lsej.org.ua/11_2023/152.pdf

[2] The Gravity of Russia's Cyberwar against Ukraine. OpinioJuris: веб-сайт. URL: https://opiniojuris.org/2023/04/19/the-gravity-of-russias-cyberwar-against-ukraine/

Кібератаки як форма неправомірного впливу на інформаційні системи та цифрові ресурси можуть бути класифіковані за різними критеріями, включаючи мету атаки, методи реалізації, рівень завданої шкоди та правові наслідки.

1. Залежно від мети, кібератаки можуть бути спрямовані на:
- порушення доступності інформаційних систем (наприклад, DDoS-атаки);
- несанкціоноване отримання доступу до інформаційних ресурсів (хакерські атаки, фішинг);
- модифікацію або знищення даних (ransomware, дефейсинг);
- шахрайство та маніпулювання даними (спуфінг, соціальна інженерія);
- підрив національної або корпоративної безпеки (APT-атаки, кібершпигунство).

2. Залежно від методів здійснення розрізняють наступні види кібератаки:
- *DDoS-атаки (Distributed Denial of Service).* DDoS-атаки є найбільш поширеним видом кібератак, які мають на меті перевантаження інформаційної системи великою кількістю запитів. Юридична кваліфікація таких дій може ґрунтуватися на нормах кримінального права, зокрема як несанкціоноване втручання в роботу комп'ютерних мереж (ст. 361 КК України, аналогічні норми передбачені в CFAA у США та в Директиві 2013/40/EU в ЄС)[1].
- *фішингові атаки (Phishing).* Фішинг є однією з найбільш небезпечних форм соціальної інженерії, яка спрямована на обманне отримання доступу до конфіденційної інформації (логінів, паролів, банківських реквізитів). З точки зору правового регулювання фішинг може кваліфікуватися як шахрайство (ст. 190 КК України) або як Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах) (ст. 362 КК України)[2].
- *програмне забезпечення – здирник (Ransomware*). Ransomware є формою шкідливого програмного забезпечення, яке блокує

[1] Directive 2013/40/EU on attacks against information systems. Official Journal of the European Union. 2013. URL: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng

[2] Кримінальний кодекс України: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

доступ до даних або пристроїв, вимагаючи викуп за відновлення доступу. Правові аспекти таких атак охоплюють кримінальну відповідальність за вимагання (ст. 189 КК України) та несанкціоноване втручання в комп'ютерні системи (ст. 361 КК України). Також, з міжнародно-правової точки зору, ransomware – кодифікація міститься у Будапештській конвенції про кіберзлочинність[1].

– *хакерські атаки (Hacking, SQL-injection, Brute-force).* Хакерські атаки охоплюють широкий спектр методів несанкціонованого доступу до інформаційних систем. SQL-ін'єкції та brute-force атаки використовуються для отримання контролю над базами даних, викрадення інформації або саботажу цифрової інфраструктури. Вони підпадають під дію законодавчих норм щодо комп'ютерного саботажу та кіберзлочинності (ст. 361-1 КК України, CFAA у США)[2].
– *атаки типу «Людина посередині» (Man-in-the-Middle, MitM).* MitM-атаки передбачають перехоплення та модифікацію даних між двома сторонами, які не підозрюють про втручання. Використовуються переважно для крадіжки конфіденційної інформації або змінення фінансових транзакцій.
– *кібершпигунство (Cyber Espionage, APT-атаки).* Кібершпигунство є однією з найсерйозніших загроз на рівні національної безпеки та корпоративного сектору. Атаки цього типу передбачають таємний, довготривалий доступ до інформаційних систем для отримання державних або комерційних таємниць. Юридично можуть кваліфікуватися як державна зрада (ст. 111 КК України), промислове шпигунство або незаконне розголошення комерційної таємниці.
– *шкідливе програмне забезпечення (Malware, Trojans, Worms, Spyware).* Категорія шкідливого програмного забезпечення охоплює віруси, трояни, черв'яки та програми-шпигуни, які можуть бути використані для викрадення даних, саботажу або несанкціонованого контролю над пристроями. В Україні такі дії можуть кваліфікуватися як розповсюдження шкідливого програмного забезпечення (ст. 361-1 КК Украї-

[1] Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
[2] Computer Fraud and Abuse Act (CFAA). U. S. Code, Title 18, Section 1030, 1986.

ни), а в міжнародному праві – підпадати під Будапештську конвенцію[1].

Кібератаки є одним із найнебезпечніших викликів сучасного інформаційного суспільства, що можуть спричинити суттєві порушення цивільних прав фізичних та юридичних осіб. У правовій доктрині кібератаки розглядаються як протиправні діяння, що порушують принцип непорушності прав суб'єктів цивільних правовідносин, завдають шкоди їх майновому та немайновому становищу, а також підривають засади правового регулювання кіберпростору.

Кібератаки можуть спричинити безпосереднє або опосередковане *порушення права власності*, зокрема через:

– несанкціоноване заволодіння цифровими активами (крадіжка криптовалюти, цифрових сертифікатів, електронних грошей тощо);
– знищення, модифікацію або блокування доступу до майнових об'єктів (наприклад, ransomware – атаки, які обмежують доступ до інформаційних ресурсів та вимагають викуп);
– несанкціоноване використання програмного забезпечення або баз даних, що може призвести до економічних збитків.

Правова кваліфікація таких порушень ґрунтується на положеннях ст. 316-319 ЦК України щодо здійснення права власності та його захисту, а також міжнародних норм щодо захисту цифрових активів.

Кібератаки можуть спричинити несанкціоноване *втручання в приватне життя*, що проявляється в:

– перехопленні, викраденні або розголошенні персональних даних (зокрема, внаслідок фішингових атак, атак типу Man-in-the-Middle);
– несанкціонованому доступі до електронної пошти, соціальних мереж, цифрових профілів;
– розповсюдженні чутливих даних, що може мати репутаційні, економічні або психологічні наслідки для потерпілої особи.

Правовий захист таких прав ґрунтується на положеннях ст. 32 Конституції України, ст. 270 ЦК України, а також на міжнародних нормах, зокрема GDPR (Regulation (EU) 2016/679), що встановлює жорсткі вимоги щодо обробки та захисту персональних даних.

[1] IT-Sicherheitsgesetz 2.0. URL: https://www.openkritis.de/it-sicherheitsgesetz/ausblick-it-sicherheitsgesetz-2-0.html#:~:text=Das%20IT%2DSicherheitsgesetz%202.0%20ist,Neue%20KRITIS%2DPflichten.

Деструктивні кібератаки, спрямовані на компрометацію осіб або компаній, можуть порушувати п*раво на недоторканність честі, гідності та ділової репутації.* До таких дій можна віднести:

– дифамаційні кампанії, поширення неправдивої інформації, маніпулятивні вкиди в медіа та соціальних мережах;
– несанкціоноване розповсюдження компрометуючих матеріалів (відредагованих зображень, особистої переписки тощо);
– фальсифікацію комунікацій та цифрових слідів, зокрема через дипфейки та інші технології обману.

Ці аспекти регулюються ст. 277-299 ЦК України, а також міжнародними стандартами щодо боротьби з кібербулінгом та онлайн-наклепом.

Кібератаки можуть спричинити *порушення договірних відносин* та заподіяння шкоди господарській діяльності через:

– підрив комерційної діяльності шляхом атак на сайти, електронні платформи, фінансові системи (DDoS-атаки, хакерські зломи, маніпуляції з фінансовими транзакціями);
– фальсифікацію комерційних даних, що призводить до втрати довіри контрагентів та клієнтів;
– несанкціонований доступ до комерційної таємниці та використання конфіденційної інформації в конкурентних цілях (промислове шпигунство, кібершпигунство).

Охорона прав гарантується на основі ст.ст. 6, 627-629 ЦК України (щодо свободи договору), Закону України «Про захист від недобросовісної конкуренції».

У разі завдання шкоди фізичним або юридичним особам унаслідок кібератак потерпілі мають право вимагати відшкодування завданих збитків. Цивільно-правова відповідальність за кібератаки охоплює:

– відшкодування майнової шкоди (ст. 22, 1166 ЦК України);
– відшкодування моральної шкоди (ст. 23, 1167 ЦК України);
– відшкодування шкоди, завданої незаконним розповсюдженням персональних даних або компрометуючої інформації (ст. 277, 280 ЦК України).

Кібератаки можуть завдавати шкоди як фізичним, так і юридичним особам, порушуючи їхні майнові та немайнові права. Хоча деякі права є спільними для обох категорій суб'єктів, є й специфічні аспек-

ти, що відрізняють порушення прав фізичних осіб та порушення прав юридичних осіб.

Фізичні особи можуть зазнати порушення права власності та інших речових прав внаслідок несанкціонованого вилучення або блокування доступу до цифрових активів, викрадення криптовалюти, електронних грошей, цінних цифрових документів, знищення або модифікації особистих файлів і даних внаслідок атак типу ransomware, а також у разі несанкціонованого контролю над пристроями та акаунтами особи, що може мати наслідком як матеріальні збитки, так і втрату важливої особистої інформації. Крім того, кібератаки можуть посягати на право фізичної особи на приватність та захист персональних даних, зокрема шляхом несанкціонованого збирання, використання або розповсюдження персональних даних, перехоплення особистої кореспонденції, а також використання персональних даних для шахрайських схем, таких як оформлення кредитів або продаж чужих даних у Darknet. Порушенням немайнових прав є також посягання на честь, гідність і ділову репутацію фізичної особи через поширення неправдивої інформації, створення фейкових акаунтів, використання дипфейків, а також розголошення приватного життя. Окрему загрозу становлять фішингові схеми та соціальна інженерія, що вводять особу в оману та можуть спричинити серйозні фінансові втрати. Також порушується право на безпечне користування цифровими платформами, адже особа може втратити доступ до власних ресурсів або стати жертвою нав'язування шкідливого програмного забезпечення, що ставить під загрозу її цифрову безпеку. Важливим аспектом є також право на відшкодування завданої шкоди, оскільки фізична особа має право вимагати компенсації матеріальних збитків, зокрема у разі викрадення коштів або пошкодження особистого майна, а також моральної шкоди у випадках, коли кібератака спричинила серйозний психологічний стрес, шантаж або публікацію конфіденційної інформації.

Юридичні особи, у свою чергу, зазнають порушень права власності та інших майнових прав унаслідок несанкціонованого проникнення в корпоративні системи, крадіжки комерційної інформації, знищення або модифікації баз даних підприємства, зокрема клієнтських баз або бухгалтерських записів, а також через несанкціонований доступ до фінансових рахунків компанії, що може спричинити

значні економічні втрати. Важливим є також право на комерційну таємницю та захист конфіденційної інформації, адже кібершпигунство, незаконне отримання стратегічної інформації компанії, витік корпоративної інформації та використання викрадених даних для недобросовісної конкуренції можуть мати катастрофічні наслідки для підприємств, зокрема підрив довіри клієнтів і партнерів. Юридичні особи також стикаються з порушенням права на ділову репутацію через кампанії з дезінформації, поширення фейкових відгуків, наклепів, дискредитацію в інформаційному просторі, а також використання шахрайських схем, наприклад, фішингових атак від імені компанії, що завдає шкоди її іміджу. Окремим аспектом є порушення права на договірну діяльність та ведення господарської діяльності, адже кібератаки можуть призвести до зриву контрактів через блокування серверів або корпоративних систем, фальсифікації договірних відносин, маніпуляції цифровими підписами та підробки електронних контрактів, а також до несанкціонованого втручання в бізнес-процеси, що може паралізувати діяльність онлайн-магазинів, банківських установ, біржових платформ. У зв'язку з цим юридичні особи мають право на судовий захист та відшкодування завданих збитків, включаючи вимоги про компенсацію матеріальних втрат, зокрема недоотриманого прибутку, додаткових витрат на кібербезпеку, а також про відшкодування репутаційної шкоди, якщо через кібератаки було зруйновано довіру клієнтів та партнерів.

Таким чином, кібератаки завдають суттєвої шкоди як фізичним, так і юридичним особам, однак характер цих порушень відрізняється. Фізичні особи зазнають переважно порушень приватності, викрадення особистих даних, шахрайства, тоді як юридичні особи стикаються з економічними загрозами, витоком комерційної інформації, порушенням договірних зобов'язань.

Цивільно-правова відповідальність за шкоду, завдану кібератаками, ґрунтується на загальних положеннях деліктного права, що передбачають наявність правопорушення, шкоди, причинно-наслідкового зв'язку та вини заподіювача шкоди. Проте особливості кіберпростору, зокрема анонімність правопорушників, складність ідентифікації джерела атаки та глобальний характер правопорушень, зумовлюють специфічні підходи до встановлення відповідальності. Основою для притягнення до цивільно-правової відповідальності є

норми Цивільного кодексу України, міжнародні конвенції у сфері кіберзлочинності, а також спеціальне законодавство щодо захисту персональних даних та інформаційної безпеки.

Однією з ключових підстав цивільно-правової відповідальності за шкоду, завдану кібератаками, є неправомірне втручання в інформаційні системи, що порушує право власності на цифрові активи. Таке втручання може включати несанкціонований доступ до баз даних, знищення, модифікацію або шифрування інформації, блокування доступу до цифрових ресурсів, що спричиняє значні матеріальні та нематеріальні збитки потерпілим особам. Згідно зі ст. 1166 ЦК України, шкода, заподіяна неправомірними діями, підлягає відшкодуванню в повному обсязі, що передбачає компенсацію витрат на відновлення даних, втрачений прибуток та інші фінансові втрати.

Підставою цивільно-правової відповідальності є також порушення права особи на конфіденційність та захист персональних даних. Внаслідок кібератак часто відбувається неправомірне збирання, обробка або поширення персональної інформації, що суперечить Закону України «Про захист персональних даних» та Регламенту ЄС 2016/679 (GDPR). Витік конфіденційної інформації може спричинити фінансові втрати, порушення права на недоторканність приватного життя, репутаційні ризики. У таких випадках відповідальними можуть бути як безпосередні ініціатори кібератаки, так і володільці баз даних, які не забезпечили належного рівня кіберзахисту.

Окрему категорію правопорушень становлять кібератаки, що спричиняють шкоду корпоративним правам, зокрема порушують комерційну таємницю або завдають шкоди діловій репутації. Несанкціоноване оприлюднення бізнес-стратегій, фінансових звітів, що може суттєво підірвати конкурентні позиції компаній та завдати значних збитків. Відповідно до ст. 22 ЦК України, юридичні особи мають право на відшкодування реальних збитків та упущеної вигоди, якщо доведено, що розголошення комерційної інформації або її модифікація внаслідок кібератаки призвели до фінансових втрат.

Ще однією підставою для цивільно-правової відповідальності є шкода, заподіяна внаслідок використання соціальної інженерії та маніпулятивних кіберметодів, таких як фішинг, ransomware або DDoS-атаки. Такі дії можуть призвести до прямого фінансового збитку, оскільки жертви, введені в оману, здійснюють неправомірні платежі

або передають доступ до своїх фінансових ресурсів. У таких випадках судова практика визнає можливість відшкодування шкоди за рахунок винних осіб, а також відповідальність третіх осіб (наприклад, власників цифрових платформ), які не вжили належних заходів для запобігання шахрайським схемам.

Встановлення причинно-наслідкового зв'язку у випадках кібератак є складним процесом, що вимагає комплексного підходу та залучення різних спеціалістів. Особливо важливим є визначення, чи є кібератака форс – мажорною обставиною, що може звільнити сторону від відповідальності за невиконання зобов'язань[1].

Форс-мажорні обставини – це надзвичайні, непередбачувані та невідворотні події, які унеможливлюють виконання зобов'язань. Кібератака може бути визнана форс-мажором, якщо вона відповідає цим критеріям і безпосередньо впливає на здатність виконати зобов'язання. Наприклад, якщо компанія не може провести розрахунки через відсутність доступу до клієнт-банку внаслідок кібератаки, це може бути підставою для визнання форс-мажору[2].

Для встановлення причинно-наслідкового зв'язку необхідно підтвердити факт кібератаки. Це можна зробити шляхом звернення до правоохоронних органів, залучення експертів у сфері IT-технологій або аналізу документів досудового розслідування. Зокрема, протоколи огляду місця події можуть зафіксувати факт кібератаки та перелік уражених комп'ютерів та обладнання.

Для підтвердження факту кібератаки необхідно встановити, що вона безпосередньо призвела до неможливості виконання зобов'язань. Для цього слід аналізувати документи та звіти, оцінити вплив на діяльність та у разі необхідності, залучити фахівців для детального аналізу.

Всі етапи встановлення причинно-наслідкового зв'язку повинні бути належним чином задокументовані. Це включає підготовку звітів та забезпечення належного зберігання всіх доказів, включаючи електронні дані, протоколи та висновки експертів.

---

[1] Подоляка Н. В. Інтеграція методів причинно-наслідкового зв'язку та SWOT-аналізу щодо визначення інформаційних ризиків: пояснювальна записка до атестаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 125 Кібербезпека. Харків, 2020. 69 с.

[2] Висіцька І. Кібератака як форс-мажор: особливості визнання. URL: https://vysitska.com/2017/12/03/кібератака-як-форс-мажор-особливості/?utm_source=chatgpt.com

Встановлення причинно-наслідкового зв'язку у випадках кібератак є важливим етапом у визначенні відповідальності та можливості застосування форс-мажору. Врахування всіх вищезазначених аспектів дозволяє забезпечити об'єктивність та достовірність процесу.

Ідентифікація правопорушника та визначення суб'єкта відповідальності в контексті кіберзлочинності є надзвичайно складним завданням, що зумовлені низкою специфічних факторів.

По-перше, анонімність та глобальний характер Інтернету ускладнюють встановлення особи правопорушника. Зловмисники можуть використовувати технології для приховування своєї особистості, що ускладнює процес ідентифікації. Наприклад, використання проксі-серверів або VPN дозволяє маскувати реальне місцезнаходження та особисті дані зловмисника.

По-друге, відсутність фізичних слідів та традиційних доказів, характерних для злочинів у реальному світі, ускладнює процес доказування. Цифрові докази можуть бути легко змінені або знищені, що ставить перед правоохоронними органами додаткові виклики.

Щодо суб'єкта відповідальності, то відповідно до законодавства, суб'єктами кіберзлочинів можуть бути фізичні осудні особи, які до моменту вчинення злочину досягли шістнадцятирічного віку. Водночас, спеціальний суб'єкт має місце у двох випадках: коли особа є посадовою особою або коли злочин вчинено з використанням спеціальних технічних засобів або програмного забезпечення[1].

З точки зору цивільного права, питання вини та безвинної відповідальності набувають особливої актуальності при розгляді випадків кібератак. Цивільно-правова відповідальність за шкоду, заподіяну внаслідок кібератак, може бути заснована як на вині, так і на шкоді, що була завдана без умислу, залежно від обставин конкретної справи.

Вина в цивільному праві розглядається як психічне ставлення особи до своєї протиправної поведінки та її наслідків. Вона може бути у формі умислу або необережності. У випадку кібератак, якщо особа свідомо та навмисно вчиняє дії, що призводять до шкоди іншій особі, така поведінка кваліфікується як умисел. Якщо ж особа не передба-

[1] Савчук Н. В. Кіберзлочинність: зміст та методи боротьби. *Теоретичні та прикладні питання економіки*: зб. наук. пр. К.: Київ. ун-т, 2009. Вип. 19. С. 338-342

чала можливості настання шкоди, але повинна була і могла її передбачити, то відповідальність настає за необережність[1].

У цивільному праві, відповідальність за шкоду завдану внаслідок необережності може бути встановлена у випадках, коли закон прямо передбачає таку відповідальність, наприклад, за шкоду, заподіяну внаслідок діяльності, що створює підвищену небезпеку для оточуючих. Щодо кібератак, відповідальність за шкоду завдану необережними діями може бути застосована, якщо особа здійснює діяльність, пов'язану з підвищеним ризиком виникнення кібератак, і навіть при відсутності вини з її боку, шкода все одно повинна бути відшкодована. При розгляді справ про кібератаки необхідно ретельно аналізувати обставини, що призвели до шкоди. Важливо встановити, чи діяла особа умисно або з необережності, а також чи здійснювала вона діяльність, пов'язану з підвищеним ризиком виникнення кібератак. У разі встановлення умислу або необережності, особа несе відповідальність за заподіяну шкоду. Якщо ж шкода була заподіяна внаслідок діяльності, що створює підвищену небезпеку, і навіть при відсутності вини, відповідальність настає без вини.

Що стосується юридичних осіб, то вони несуть відповідальність за неналежний рівень кібербезпеки у випадках, коли їх дії або бездіяльність призводять до порушення законодавства у сфері кібербезпеки. Основним нормативно-правовим актом, що регулює ці питання, є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. Згідно з цим законом, особи, винні у порушенні законодавства у сферах національної безпеки, оборони, захисту державної таємниці, несуть відповідальність відповідно до закону.

Відповідальність може наставати у випадках, коли юридична особа не забезпечила належний захист інформаційних систем, що призвело до несанкціонованого доступу, витоку конфіденційної інформації або інших кіберінцидентів. Також відповідальність може бути застосована, якщо організація не виконала законних вимог посадових осіб Служби безпеки України або Державної служби спеціального зв'язку та захисту інформації України щодо забезпечення кібербезпеки.[2]

---

[1] Тихомиров О. О. Інформаційний делікт як підстава «інформаційної» юридичної відповідальності: відмітні ознаки. *Інформація і право.* 2019. № 1. С. 37-44.

[2] Доронін І. М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави. *Інформація і право.* 2017. № 1(20). С. 107. URL: https://ippi.org.ua/sites/default/files/13_3.pdf

Крім того, міжнародні стандарти, такі як Конвенція Ради Європи про кіберзлочинність, передбачають відповідальність юридичних осіб за кримінальні правопорушення, вчинені на їх користь особами, які займають керівні посади. Це означає, що організація може бути притягнута до відповідальності, якщо її керівництво не забезпечило належний рівень кібербезпеки, що призвело до правопорушення[1].

Кібератаки становлять серйозну загрозу для сучасних організацій, завдаючи різноманітних видів шкоди, серед яких матеріальна, моральна та репутаційна. Розуміння природи та наслідків кожного з цих типів шкоди є сьогодні важливим для розробки ефективних стратегій захисту та відшкодування.

Матеріальна шкода внаслідок кібератак проявляється у прямих фінансових втратах, які можуть включати витрати на відновлення систем, втрату прибутку через простої. Наприклад, атаки типу «відмова в обслуговуванні» (DDoS) можуть призвести до тривалих простоїв веб-сайтів або сервісів, що безпосередньо впливає на доходи компанії. Крім того, витрати на залучення експертів з кібербезпеки для усунення наслідків атаки та впровадження додаткових заходів захисту також складають значну частину матеріальних збитків.

Матеріальна шкода, завдана кібератаками, є суттєвою проблемою сучасного інформаційного суспільства, оскільки такі атаки можуть призвести до значних фінансових втрат, порушення бізнес-процесів та зниження довіри до цифрових технологій.

Фінансові втрати внаслідок кібератак можуть включати прямі витрати, такі як витрати на відновлення систем, виплату викупу при атаках типу ransomware, а також непрямі втрати, пов'язані з простоєм бізнесу та втратою клієнтів. Наприклад, у січні 2024 року повідомлялося про зростання активності хакерських груп, що займаються програмами-вимагачами, які все частіше атакують медичні заклади, завдаючи їм значних фінансових збитків. До прикладу, колишнього розробника Trickbot Володимира Дунаєва було притягнуто до відповідальності за злочин, який полягав у зараженні американських лікарень і підприємств ransomware Trickbot, що коштувало жертвам збитків у десятки мільйонів доларів. За даними Національного агент-

[1] Правова база української кібербезпеки: загальний огляд і аналіз. *Міжнародна фундація виборчих систем в Україні.* 2019. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf

ства зі злочинності Великобританії, зловмисники виманили щонайменше 180 мільйонів доларів США (145 мільйонів фунтів стерлінгів) у людей і організацій по всьому світу[1].

Порушення бізнес-процесів є ще одним наслідком кібератак. Збої в роботі інформаційних систем можуть призвести до тимчасової недоступності послуг або продуктів, що негативно впливає на репутацію компанії та її конкурентоспроможність. Наприклад, атака програми-вимагача на компанію TietoEVRY у Швеції вплинула на послуги для деяких клієнтів, що підкреслює вразливість бізнесу до кібератак.

Витрати на відновлення та посилення систем безпеки після кібератак також є значними. Компанії змушені інвестувати в оновлення інфраструктури, навчання персоналу та впровадження нових заходів безпеки, щоб запобігти майбутнім інцидентам.

Окрім прямих фінансових втрат, кібератаки можуть спричинити моральну шкоду, яка стосується психологічного впливу на постраждалих осіб. Це може включати стрес, тривогу та інші негативні емоційні реакції, пов'язані з втратою конфіденційної інформації або порушенням приватності. Особливо це стосується випадків, коли особисті дані співробітників або клієнтів стають доступними зловмисникам, що може призвести до відчуття небезпеки та вразливості серед постраждалих. Оцінка моральної шкоди внаслідок кібератак є складним завданням через нематеріальний характер таких втрат[2]. Відсутність чітких критеріїв оцінки та стандартизованих методик може призводити до суб'єктивності в судових рішеннях.

Репутаційна шкода є ще одним критичним аспектом наслідків кібератак. Публічне розголошення фактів про успішні атаки на компанію може суттєво підірвати довіру клієнтів, партнерів та інвесторів. Втрата репутації часто має довгострокові наслідки, які важко піддаються кількісній оцінці, але безпосередньо впливають на конкурентоспроможність та ринкову позицію організації. Відновлення довіри після таких інцидентів вимагає значних зусиль та ресурсів, включаючи проведення PR-кампаній та впровадження додаткових заходів безпеки. Особливо небезпечними є атаки, пов'язані з розголошенням

[1] Cyber Digest: Огляд подій в сфері кібербезпеки, січень 2024 С. 20. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest/Cyber%20digest_Jan_2024_UA.pdf

[2] Особливості відшкодування моральної шкоди. URL: https://legalaid.gov.ua/novyny/osoblyvosti-vidshkoduvannya-moralnoyi-shkody/

персональних даних, оскільки вони можуть викликати скандали та судові позови. Публічне висвітлення таких інцидентів у засобах масової інформації часто погіршує ситуацію, формуючи негативний імідж компанії або особи. Це, у свою чергу, може спричинити фінансові втрати, оскільки клієнти починають уникати співпраці з організацією, яка не змогла забезпечити належний рівень захисту інформації. Багато компаній після масштабних кібератак стикаються зі зниженням вартості акцій, оскільки інвестори втрачають довіру до їхньої здатності захистити свої активи. У деяких випадках, особливо якщо йдеться про державні установи або великі корпорації, наслідки можуть бути ще серйознішими, адже кібератаки можуть підривати національну безпеку або довіру громадськості до ключових інституцій. Часто постраждалі компанії намагаються мінімізувати наслідки шляхом кризових комунікацій, але відновлення довіри може тривати роками. Захист від таких загроз потребує не лише впровадження сучасних технологій кібербезпеки, а й продуманої стратегії управління репутаційними ризиками. Відкритість та оперативне інформування клієнтів про заходи, яких вжито для усунення загроз, може допомогти пом'якшити удар по репутації. Однак навіть швидка реакція не завжди може компенсувати репутаційні втрати, особливо якщо атака була масштабною або сталася повторно. У цифрову епоху, коли будь-яка інформація швидко поширюється мережею, репутація стає одним із найцінніших активів, і її пошкодження через кібератаки може мати довгострокові наслідки.

Важливо зазначити, що ці види шкоди взаємопов'язані та можуть посилювати один одного. Наприклад, матеріальні втрати через кібератаку можуть призвести до моральної шкоди серед співробітників, які переживають за своє майбутнє, а репутаційні втрати можуть спричинити додаткові фінансові збитки через відтік клієнтів. Тому комплексний підхід до оцінки та управління ризиками кібератак є необхідним для мінімізації потенційних збитків.

Крім безпосередніх втрат, кібератаки можуть мати довгострокові наслідки для інноваційного потенціалу компанії. Витік конфіденційної інформації, такої як комерційні таємниці або дані про розробки, може призвести до втрати конкурентних переваг. Це, в свою чергу, впливає на здатність компанії впроваджувати нові продукти або послуги, що негативно позначається на її позиції на ринку.

Крім того, кібератаки можуть призвести до штрафів та інших санкцій з боку регуляторних органів. Це додає додатковий фінансовий тягар та може ще більше погіршити репутацію компанії. Тому дотримання нормативних вимог у сфері кібербезпеки є критично важливим для мінімізації таких ризиків. У контексті глобалізації бізнесу, кібератаки можуть мати міжнародні наслідки, впливаючи на партнерські відносини та ринки збуту в інших країнах. Витік даних або компрометація систем може призвести до втрати довіри з боку міжнародних партнерів, що ускладнює вихід на нові ринки або підтримку існуючих бізнес-зв'язків.

Отже, кібератаки можуть завдавати багатогранної шкоди організаціям, охоплюючи матеріальні, моральні та репутаційні аспекти. Розуміння та оцінка кожного з цих видів шкоди є необхідними для розробки ефективних стратегій захисту та відшкодування, що дозволить мінімізувати негативні наслідки та забезпечити стійкість організації в умовах сучасних кіберзагроз.

Складним є процес доведення шкоди та її розміру після кібератаки, адже це вимагає системного підходу та залучення різних фахівців. Цей процес включає кілька ключових етапів:

1. Виявлення та документування інциденту – це є першим кроком задля фіксації факту кібератаки, що включає збереження скріншотів та інших доказів. Важливо забезпечити цілісність цих даних для подальшого аналізу.

2. Оцінка обсягу та характеру втрат – після виявлення атаки необхідно визначити, які системи та дані були скомпрометовані, а також оцінити тривалість та інтенсивність впливу. Це дозволяє встановити масштаби шкоди.

3. Визначення фінансових втрат – оцінка матеріальних збитків включає підрахунок витрат на відновлення систем, втрати доходів через простої, витрати на юридичні послуги та можливі штрафи. Цей етап вимагає залучення фінансових експертів для точного розрахунку.

4. Оцінка моральної та репутаційної шкоди – визначення впливу на моральний стан співробітників та клієнтів, а також на репутацію компанії, є складним завданням. Для цього можуть використовуватися опитування, аналіз відгуків та моніторинг медіа.

5. Залучення експертів з кібербезпеки – фахівці з кібербезпеки проводять технічний аналіз інциденту, визначають вразливості та

оцінюють ефективність існуючих заходів захисту. Їхні висновки є важливими для розуміння причин та наслідків атаки.

7. Використання методичних рекомендацій – згідно з Методичними рекомендаціями щодо визначення ризиків та оцінки їхнього впливу, для визначення ризику застосовуються дані щодо загроз, вразливостей, їх ймовірностей та рівня шкоди. Це дозволяє системно підходити до оцінки потенційних втрат[1].

Загалом, процес доведення шкоди та її розміру після кібератаки вимагає комплексного підходу, залучення різних фахівців та використання спеціалізованих методик для точного визначення масштабів втрат та розробки ефективної стратегії відшкодування[2].

Відшкодування шкоди, завданої кібератаками, здійснюється відповідно до загальних принципів цивільного права України, з урахуванням специфіки кіберзлочинів. Основними способами відшкодування є грошова компенсація та відновлення порушених прав у натурі.

Грошова компенсація передбачає виплату потерпілому суми, еквівалентної завданим збиткам. Згідно зі ст. 22 ЦК України, збитками визнаються:

1. втрати, яких особа зазнала у зв'язку зі знищенням або пошкодженням майна;

2. витрати, які особа зробила або мусить зробити для відновлення свого порушеного права;

3. неодержані доходи, які особа могла б реально одержати за звичайних обставин, якби її право не було порушене.

Відновлення порушених прав у натурі полягає в реальному відновленні стану, який існував до порушення. Це може включати повернення викрадених даних або відновлення працездатності інформаційних систем. Стаття 1192 ЦК України передбачає, що за вибором потерпілого особа, яка завдала шкоди майну, може бути зобов'язана відшкодувати її в натурі або компенсувати завдані збитки у повному обсязі.

---

[1] Правова база української кібербезпеки: загальний огляд і аналіз. *Міжнародна фундація виборчих систем в Україні.* 2019. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf?utm_source=chatgpt.com

[2] Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест. Відп. ред. О. Довгань; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В. І. Вернадського. К., 2024. № 6. 364 с.

У випадках, коли кібератака призвела до витоку конфіденційної інформації, що спричинило моральну шкоду, потерпілий має право на її компенсацію. Розмір такої компенсації визначається судом з урахуванням характеру правопорушення та глибини моральних страждань.

Варто зазначити, що відшкодування шкоди, завданої кібератаками, може бути ускладнене через труднощі в ідентифікації винних осіб та міжнародний характер таких злочинів. Тому важливу роль відіграє співпраця з правоохоронними органами та міжнародними організаціями для встановлення винних та притягнення їх до відповідальності.

Таким чином, відшкодування шкоди, завданої кібератаками, базується на загальних принципах цивільного права України, але потребує врахування специфіки кіберзлочинів та можливих труднощів у притягненні винних до відповідальності.

Страхування кіберризиків є важливим інструментом управління ризиками в умовах цифровізації, забезпечуючи фінансовий захист від наслідків кібератак та інших кіберзагроз. Цей вид страхування спрямований на компенсацію збитків, завданих порушенням інформаційної безпеки, та допомагає підприємствам швидко відновити свою діяльність після інцидентів.

Основною метою кіберстрахування є забезпечення фінансового механізму відновлення після значних збитків, допомагаючи підприємствам повернутися до нормального функціонування, зберегти стабільність, платоспроможність та знизити втрати в результаті перерви у виробництві[1].

Кіберстрахування покриває широкий спектр ризиків, включаючи втрату даних, зниження репутації, відшкодування збитків клієнтам та інші опції[2]. Це дозволяє підприємствам ефективно управляти потенційними загрозами та мінімізувати фінансові втрати від кібератак.

В Україні розвиток кіберстрахування стикається з певними проблемами, такими як відсутність цього виду страхування у більшості страхових компаній та недостатня обізнаність підприємств про його

[1] Розвиток кіберстрахування як сегменту глобального страхового ринку. URL: https://kon-insurance.mnau.edu.ua/files/work_2020/6.pdf

[2] Попович Д. В., Бундз Н. Б., Іванків В. О. Проблеми та перспективи розвитку страхування кіберризиків на національному ринку. *Молодий вчений.* № 4 (116). 2023. С. 864-867.

переваги[1]. Однак, з огляду на зростання кіберзлочинності та впровадження цифрових технологій, потреба в кіберстрахуванні стає все більш актуальною.

Важливим аспектом кіберстрахування є необхідність оцінки кіберризиків та визначення умов страхування, розміру страхового покриття і премій. Це вимагає від страхових компаній глибокого розуміння специфіки кіберзагроз та здатності проводити незалежну фахову експертизу кіберризиків.

Таким чином, страхування кіберризиків виступає ефективним механізмом компенсації шкоди, завданої кібератаками, та є невід'ємною частиною сучасної системи управління ризиками в умовах цифрової економіки.

Правове регулювання відповідальності за шкоду, завдану кібератаками, в Україні стикається з низкою прогалин, що ускладнюють ефективну боротьбу з кіберзлочинністю та захист прав потерпілих. Основні проблеми включають недостатню деталізацію законодавства, відсутність чітких визначень ключових термінів та неузгодженість між нормативно-правовими актами.

По-перше, в українському законодавстві відсутні чіткі та загальновизнані визначення таких понять, як «кібератака», «кіберзагроза», «кіберзлочин» тощо. Це призводить до неоднозначного тлумачення та застосування норм права на практиці. Запропоновано законодавчо закріпити основні терміни кібербезпеки, що сприятиме уніфікації підходів до їх розуміння та застосування.

По-друге, існує проблема неузгодженості між різними нормативно-правовими актами, що регулюють сферу кібербезпеки. Це створює труднощі у визначенні відповідальності за кіберзлочини та механізмів компенсації шкоди. Необхідно провести комплексний аналіз чинного законодавства з метою виявлення та усунення суперечностей, а також розробити єдину стратегію кібербезпеки, яка б враховувала сучасні виклики та загрози[2].

По-третє, наявні прогалини у визначенні відповідальності за кіберзлочини, вчинені в умовах війни. Запровадження відповідально-

[1] Іванова Т. Г. Перспективи розвитку ринку кіберстрахування в Україні. URL: https://ir.kneu.edu.ua/server/api/core/bitstreams/f44303d4-aa69-42bb-b043-5519e3394df6/content

[2] Федорін М., Заєць Я. Про особливості правового забезпечення кібернетичної безпеки (кібербезпеки) в Україні. URL: http://lawdrafting.org/pro-osoblivosti-pravovogo-zabezpechennya-kibernetichnoyi-bezpeki-kiberbezpeki-v-ukrayini/

сті за такі дії є необхідним для забезпечення національної безпеки та захисту суспільних інтересів України.

Для усунення зазначених прогалин, на нашу думку, необхідно:

1. Розробити та впровадити спеціалізоване законодавство у сфері кібербезпеки, яке б чітко визначало правовий статус суб'єктів кіберпростору, їх права та обов'язки, а також встановлювало відповідальність за порушення у цій сфері.

2. Гармонізувати національне законодавство з міжнародними стандартами та практиками у сфері кібербезпеки. Це сприятиме ефективній міжнародній співпраці у боротьбі з кіберзлочинністю та забезпечить належний рівень захисту прав потерпілих.

3. Підвищити кваліфікацію правоохоронних органів та суддівського корпусу у сфері кібербезпеки. Це забезпечить ефективне застосування законодавства та належний захист прав потерпілих від кібератак.

Таким чином, усунення прогалин у правовому регулюванні відповідальності за шкоду, завдану кібератаками, вимагає комплексного підходу, який включає вдосконалення законодавства, гармонізацію його з міжнародними стандартами та підвищення професійного рівня фахівців у сфері кібербезпеки.

Цивільно-правова відповідальність за шкоду, завдану кібератаками – це встановлений законом обов'язок особи, яка вчинила неправомірне втручання в інформаційні системи, електронні комунікаційні мережі або дані, відшкодувати матеріальні збитки та/або моральну шкоду, заподіяну потерпілій особі чи організації. Вона ґрунтується на загальних принципах деліктного та договірного права, передбачаючи можливість відшкодування матеріальних збитків, компенсації моральної шкоди та відновлення порушених прав.

Важливим аспектом є складність ідентифікації порушників у кіберпросторі, що ускладнює процес притягнення їх до відповідальності. Відсутність чітких правових механізмів для боротьби з міжнародними кіберзлочинцями також є серйозною проблемою. Основними способами відшкодування шкоди виступають грошова компенсація, відновлення в натурі та компенсація моральної шкоди. Проте правозастосовна практика щодо таких справ в Україні ще не є достатньо розвиненою, що потребує додаткового законодавчого врегулювання та роз'яснень. Необхідно вдосконалювати правові механізми,

зокрема гармонізувати українське законодавство з міжнародними стандартами, забезпечити ефективне страхування кіберризиків і розробити спеціалізовані процедури для розгляду справ про кібератаки в судовому порядку. Державі слід активізувати міжнародну співпрацю у сфері кібербезпеки для ефективного розслідування злочинів, а також розвивати спеціалізовані підрозділи, що займаються кіберзлочинністю.

Важливим напрямом є підвищення обізнаності бізнесу та громадян щодо засобів захисту від кіберзагроз, а також впровадження обов'язкових стандартів кібербезпеки для підприємств, що працюють із конфіденційними даними.

Отже, цивільно-правова відповідальність за кібератаки потребує подальшого розвитку та адаптації до сучасних викликів. Створення дієвої системи правового захисту потерпілих сприятиме підвищенню рівня безпеки у цифровому середовищі та зміцненню довіри до правових механізмів відшкодування шкоди.

Ключові слова: цивільно-правова відповідальність, відшкодування шкоди, майнові права, немайнові права, ділова репутація, кібератака, кібербезпека, кіберстрахування, методи цивільно-правового регулювання, національна безпека, кіберзагроза, гібридна війна, інформаційна війна.