НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**28 листопада 2025 року**

# КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

**МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

УДК 004.056

**Відповідальній редактор:**

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

*Секція 4. НОРМАТИВНО-ПРАВОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ*

# НОРМАТИВНО-ПРАВОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

***Задерейко Олександр***

*доцент, кандидат технічних наук, доцент кафедри інформаційних технологій факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»*

***Іванов Володимир***

*студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»*

У сучасному світі інформація і цифрові сервіси [1] стали фундаментальною інфраструктурою суспільного життя. Шкала використання інформаційних технологій у державному управлінні, енергетиці, банківській сфері, медицині та освіті вимагає надійних правових механізмів, які б забезпечували не лише технічний захист, а й відповідальність, координацію та прозорість. Поняття кібербезпеки розглядається сьогодні як комплексна категорія, що включає правові, організаційні, технічні та соціальні складові. Тенденції останнього десятиліття свідчать про те, що масштабні кібератаки отримали стратегічний характер: вони можуть впливати на економічну стабільність, критичні системи життєзабезпечення і навіть на результати політичних процесів. Для держави таке явище стає питанням не лише безпеки, а й суверенітету [2].

Нормативно-правове поле [3], яке регулює відносини у сфері кібербезпеки, має дві взаємопов'язані цілі. Перша полягає у створенні умов для превентивного захисту, що передбачає впровадження стандартів, сертифікацію засобів захисту, встановлення обов'язків щодо оцінки ризиків та реалізації заходів захисту у критичних і некритичних інформаційних системах. Друга мета — забезпечення дієвих механізмів реагування та правозастосування у випадку інцидентів. Законодавство має бути спроможним не лише визначити відповідальність, але й забезпечити оперативну міжнародну співпрацю у сфері розслідування кіберзлочинів, екстрадицію, обмін інформацією та координацію технічної допомоги.

В Україні правове регулювання в цій сфері базується на низці ключових нормативних актів, серед яких центральне місце займає Закон України «Про основні засади забезпечення кібербезпеки України». Цей акт визначає понятійний апарат, статус суб'єктів системи кібербезпеки, базові принципи державної політики, а також інструментарій захисту критичної інформаційної

інфраструктури. У законі закріплено підходи до створення національних центрів реагування, визначення ролей державних установ та встановлення механізмів взаємодії з приватними операторами. Паралельно з національними актами, правове поле доповнюється правилами, що стосуються захисту інформації в інформаційно-телекомунікаційних системах, регулюванням обігу персональних даних та правами громадян у цифровому просторі.

Законодавство про захист персональних даних має спеціальне значення у загальній системі кібербезпеки. Воно формує правові гарантії приватності, є інструментом захисту фізичних осіб від безпідставного збору, обробки або передачі інформації, яка може завдати шкоди. У рамках цифрової взаємодії між громадянами, бізнесом і державою правила обробки персональних даних визначаються прозорі процедури надання згоди, термінів зберігання, механізмів доступу до інформації та прав на видалення. Гармонізація національного законодавства з міжнародними нормами, зокрема з правилами ЄС, сприяє підвищенню довіри та інтеграції на транснаціональному рівні.

Міжнародно-правовий контекст відіграє ключову роль у формуванні ефективних механізмів протидії кіберзагрозам [4]. Асамблеї і договори, ініціативи у межах Організації Об'єднаних Націй, рамкові документи Ради Європи та положення НАТО створюють базис для узгодження підходів. Конвенція Ради Європи про кіберзлочинність встановлює стандарти криміналізації деяких дій у кіберпросторі і механізми міжнародної співпраці у справах розслідування злочинів. Міжнародні стандарти також формують практики ведення цифрової криміналістики, обміну інформацією про загрози та спільного реагування на інциденти. Для України важливим є не лише приєднання до міжнародних угод, а й активна участь у розробці процедур співпраці, які враховують специфіку національного інформаційного простору.

Сучасні технологічні тенденції висувають на перший план такі питання, як захист систем, що використовують штучний інтелект [5]. Моделі штучного інтелекту можуть застосовуватися для виявлення загроз, проте водночас вони стають об'єктом атак: атаки на дані навчання, маніпуляції вхідними даними або створення шкідливих автоматизованих сценаріїв. Deepfake - технології, які дозволяють створювати реалістичні підроблені аудіо і відео, ставлять під сумнів довіру до цифрових джерел інформації і вимагають відповідних юридичних інструментів для захисту прав і репутації громадян та інституцій. Законодавство має передбачати відповідальність за створення і поширення матеріалів, що використовуються для введення в оману, однак при цьому не повинно обмежувати свободу вираження поглядів.

Критична інформаційна інфраструктура є особливо вразливою ланкою держави. Порушення роботи енергетичних мереж, систем водопостачання, транспортних вузлів або платіжних систем може мати безпосередні гуманітарні та економічні наслідки. Тому нормативно-правові засади мають

передбачати спеціальні режими захисту таких систем, вимоги до операторів критичної інфраструктури щодо інвестицій у кіберзахист, регулярних аудитів та моделювання сценаріїв атак. Законодавчі норми повинні стимулювати впровадження відновлювальних планів та резервних механізмів для забезпечення безперебійності роботи у кризових ситуаціях.

Інституційна система кібербезпеки [6] передбачає чіткий розподіл обов'язків між державними органами і створення національних центрів, які забезпечують моніторинг, виявлення та реагування на кіберінциденти. Координація дій між різними відомствами, оперативний обмін інформацією з приватним сектором, а також створення механізмів довірчого обміну даними є ключовими умовами ефективності. Одночасно важливим є розвиток людського капіталу: підготовка експертів, створення навчальних програм у вищих навчальних закладах і підвищення кваліфікації працівників держсектору.

Правозастосування у випадках кіберзлочинів має свою специфіку. Слід зазначити, що цифрові докази потребують особливої процедури вилучення, збереження та аналізу. Доказова база у кіберсправах часто має транскордонний характер, що ускладнює оперативність розслідувань без налагоджених міжнародних каналів співпраці. Тому законодавство повинно забезпечувати як внутрішні механізми для ефективного розслідування, так і правову базу для міжнародної допомоги. Крім того, важливою є роль превентивних заходів: розроблення нормативів розробки безпечного програмного забезпечення, впровадження практик захисту на етапі життєвого циклу продукту та стимулювання прозорості у ланцюгах поставок цифрових рішень.

Особливу увагу слід приділяти питанням балансу між забезпеченням безпеки і захистом прав людини. Державні інструменти моніторингу та контролю інформаційних потоків можуть бути ефективними у виявленні загроз, але без належних правових гарантій вони ризикують стати механізмом утиску свободи слова та порушення приватності. Конституційні норми, міжнародні цивільні стандарти і практика Європейського суду з прав людини повинні лягти в основу будь-яких оперативних заходів, спрямованих на захист у кіберпросторі.

Розвиток цифрової економіки [7] вимагає стимулювання інновацій при одночасному забезпеченні захисту споживачів та інтересів національної безпеки. Законодавчі ініціативи повинні створювати прозорі умови для розвитку стартапів, захищати інтелектуальну власність і забезпечувати стандарти кібербезпеки, які не стануть надмірним бар'єром для входу на ринок. Регулятор має враховувати технологічну нейтральність і надавати можливості для добровільної сертифікації та інструментів самоорганізації у галузі.

На завершення, нормативно-правові засади кібербезпеки та захисту інформації вимагають системного підходу, який поєднує законодавчу чіткість, розвиток інституційних механізмів та інвестиції у людський капітал. Тільки при поєднанні цих елементів держава може створити стійку систему, здатну протистояти сучасним загрозам і забезпечити безпечний розвиток цифрового суспільства. У майбутньому важливо фокусуватися на адаптивності правових норм, міжнародній співпраці та інклюзивних підходах, що дозволять поєднати безпеку, права людини і економічний розвиток.

**Список використаних джерел:**

1. Нікітін, Ю. О., Кульчицький, О. І. Цифрова парадигма як основа визначень: цифровий бізнес, цифрове підприємство, цифрова трансформація. Маркетинг і цифрові технології, 3(4), 2019, С. 77-87.
2. Задерейко О.В., Троянський О.В., Чанишев Р.І., Дика А.І. Концептуальні основи захисту інформаційного суверенітету України : монографія / О.В. Задерейко, О.В. Троянський, Р.І. Чанишев, А.І. Дика. Одеса : Фенікс, 2022. 220 с. ISBN 978-966-928-812-7. URL: https://hdl.handle.net/11300/22733.
3. Корж-Усенко, Л., Рибалко, П. Нормативно-правові засади розвитку вищої освіти в україні в умовах євроінтеграції. Фізико-математична освіта, 29(3), 2021, С. 74–80. DOI: https://doi.org/10.31110/2413-1571-2021-029-3-012/.
4. Ґеник, Микола Антонович. "Методологічні проблеми дефініції термінів «кібербезпека» і «кіберзагроза»." (2025). URL: https://lib-old.pnu.edu.ua/handle/123456789/23115/.
5. Баранов, О. А. (2023). Визначення терміну “штучний інтелект”. Інформація і право, (1 (44)), 32-49. URL: http://il.ippi.org.ua/article/view/287537/281385/.
6. САМОТУГА, А. (2022). Організаційно-інституційне забезпечення інформаційної безпеки України. Науковий вісник Дніпропетровського державного університету внутрішніх, 195. URL: https://lnk.ua/R4aMRyq4J/.
7. Закусило, В., Гавловська, Н., & Власюк, І. (2025). Цифрова економіка та її вплив на управління підприємствами. Рекомендовано до друку науково-технічною радою Хмельницького національного університету, протокол № 11 від 24.12. 2024, 94. URL: https://lnk.ua/Men0bLLNg/.

**Ключові слова:** кібербезпека; захист інформації; нормативно-правове регулювання; критична інформаційна інфраструктура; кіберзлочинність; захист персональних даних; міжнародне право; штучний інтелект; цифрові докази.

**Keywords:** cybersecurity; information protection; legal regulation; critical information infrastructure; cybercrime; personal data protection; international law; artificial intelligence; digital evidence.

# КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ ТА ПРАКТИКА

**МАТЕРІАЛИ**
**VI МІЖНАРОДНОЇ**
**НАУКОВО-ПРАКТИЧНОЇ**
**КОНФЕРЕНЦІЇ**

*28 листопада 2025 року*
*м. Одеса*

**Відповідальній редактор: О.В. Дикий**

Дизайн та верстка:
М.Ю. Овчинников