УДК 342.95:004:341.41/.46
DOI https://doi.org/10.32850/sulj.2025.1.17

МІЖНАРОДНИЙ ДОСВІД АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗАГРОЗАМ

Кочман К. П., Форос Г. В.

Стаття є дослідженням міжнародного досвіду адміністративно-правового забезпечення протидії кіберзагрозам, у якому обґрунтовано значення нормативно-правових підходів, інституційних механізмів та міжнародного співробітництва для забезпечення кібербезпеки. Розглянуто основні підходи до правового регулювання у країнах Європейського Союзу, США, Китаї, Канаді та інших держав, де питання кібербезпеки є пріоритетними у забезпеченні національної безпеки та збереженні стабільності цифрових інфраструктур. Окрема увага приділена аналізу правових норм, які регулюють діяльність у кіберпросторі, встановлюють відповідальність за кіберзлочини та визначають заходи для захисту інформаційних ресурсів.

Здійснено порівняння різних підходів до боротьби з кіберзлочинністю, захисту критичної інфраструктури, управління даними та кібердипломатії. У статті розглядаються переваги та виклики впровадження загальних стандартів кібербезпеки, таких як Директива NIS2 Європейського Союзу, яка спрямована на посилення кібербезпеки критичних об'єктів та Конвенція про кіберзлочинність Ради Європи, що сприяє уніфікації підходів до криміналізації правопорушень у кіберпросторі. Такі документи встановлюють спільні рамки, які допомагають різним державам координувати зусилля у сфері протидії кіберзагрозам і сприяють міжнародному обміну інформацією.

Також розглянуто роль кібердипломатії у встановленні загальноприйнятих принципів поведінки держав у кіберпросторі. Це сприяє запобіганню конфліктам та забезпеченню стабільності міжнародної обстановки, що є особливо актуальним у контексті зростання глобальних кіберзагроз. Підкреслено значення таких ініціатив ООН, як рекомендації для держав щодо відповідальної поведінки в кіберпросторі, які є важливими для запобігання ескалації напруженості між країнами.

Наукова новизна дослідження полягає у комплексному аналізі міжнародних підходів до кібербезпеки, порівнянні регуляторних механізмів різних держав та обґрунтуванні можливостей їхнього застосування для вдосконалення адміністративно-правових механізмів протидії кіберзагрозам в Україні.

Ключові слова: *кіберзлочини, кібердипломатія, міжнародна співпраця, шифрування, системи виявлення, блокчейн-технології.*

Kochman K. P., Foros H. V. International experience in administrative and legal support for countering cyber threats

The article is a study of international experience in the administrative and legal support for countering cyber threats. It substantiates the importance of regulatory approaches, institutional mechanisms, and international cooperation in ensuring cybersecurity. The study examines the main approaches to legal regulation in the European Union, the USA, China, Canada, and other countries, where cybersecurity is a priority for national security and the stability of digital infrastructure. Particular attention is given to analyzing legal norms that regulate activities in cyberspace, establish accountability for cybercrimes, and outline measures to protect information resources.

The article compares various approaches to combating cybercrime, protecting critical infrastructure, data management, and cyber diplomacy. It discusses the advantages and challenges of implementing common cybersecurity standards, such as the European Union's NIS2 Directive, which aims to enhance the cybersecurity of critical entities, and the Council of Europe's Convention on Cybercrime, which promotes the unification of approaches to criminalizing offenses in cyberspace. Such documents establish a common framework that assists different states in coordinating efforts in countering cyber threats and fosters international information sharing.

The role of cyber diplomacy in establishing universally accepted principles of state behavior in cyberspace is also considered. This fosters conflict prevention and supports international stability, particularly in the context of rising global cyber threats. The importance of UN initiatives, such as recommendations for responsible state conduct in cyberspace to prevent escalation of tensions among countries, is highlighted.

The research novelty lies in the comprehensive analysis of international approaches to cybersecurity, comparing regulatory mechanisms of different countries, and justifying

their applicability for improving administrative and legal mechanisms to counter cyber threats in Ukraine.

Key words: *cybercrime, cyber diplomacy, international cooperation, encryption, detection systems, blockchain technologies.*

Постановка проблеми та її актуальність. У сучасному світі з розвитком інформаційних технологій і цифрової економіки кіберзагрози стають однією з найактуальніших проблем національної та міжнародної безпеки. Ці загрози, що включають кіберзлочинність, шпигунство, тероризм та інші форми протиправної діяльності у кіберпросторі, значно впливають на функціонування як державних інститутів, так і приватного сектору. Відповідно, адміністративно-правове забезпечення протидії кіберзагрозам набуває критичного значення для збереження стабільності, захисту персональних даних громадян, а також забезпечення безперервності економічних і соціальних процесів.

Міжнародний досвід у цій сфері свідчить про важливість скоординованих зусиль держав, міжурядових організацій та приватних структур у створенні ефективних механізмів боротьби з кіберзагрозами. Кожна держава розробляє власну систему протидії, спираючись на нормативно-правові акти, інституційні підходи та стратегії, що відповідають її специфічним викликам і ресурсним можливостям. Однак спільним завданням для всіх країн є забезпечення належного рівня кібербезпеки через міжнародну співпрацю, адаптацію найкращих практик та гармонізацію правових норм.

Аналіз останніх досліджень і публікацій. Робота ґрунтується на аналізі законодавства зарубіжних країн, науково-методичної літератури, наукових статей, напрацювань сучасних та попередніх дослідників, серед яких: В. Шемчук, В. Горулько, М. М. Сливка, А. Тарасюк, M. F. Safitra тощо.

Дослідження в сфері міжнародного адміністративно-правового забезпечення кібербезпеки фокусуються на регуляторних підходах, ефективних механізмах співпраці та стандартизації для протидії кіберзагрозам. Основні аспекти включають аналіз правового регулювання в умовах зростання кіберзагроз, досвід міжнародної співпраці в цій сфері, а також розробку стратегічних документів і стандартів для забезпечення кібербезпеки на глобальному рівні. Значна увага приділяється ролі національних і міжнародних стратегій, що враховують як адміністративно-правові, так і технічні заходи захисту кіберпростору.

Метою цієї статті є аналіз міжнародного досвіду адміністративно-правового забезпечення протидії кіберзагрозам, оцінка ефективності правових та організаційних підходів, що застосовуються різними країнами, та визначення можливостей їхнього використання в Україні.

Виклад основного матеріалу. Нормативно-правове регулювання кібербезпеки є ключовим елементом захисту держав і суспільства від кіберзагроз. Воно включає систему правових актів, стандартів та інструкцій, спрямованих на попередження, виявлення та протидію кіберзлочинам і кіберінцидентам. Становлення законодавчого забезпечення у цій сфері має особливе значення, оскільки дозволяє формувати правові основи для діяльності суб'єктів, відповідальних за кібербезпеку, а також забезпечувати належний рівень захисту інформаційних ресурсів та персональних даних громадян [1, с. 151].

Одним із найважливіших міжнародних документів у сфері кібербезпеки є Конвенція про кіберзлочинність Ради Європи (Будапештська конвенція), яка була ухвалена в 2001 році. Вона встановлює загальні принципи для боротьби з кіберзлочинністю і є першою глобальною угодою, яка створює єдиний підхід до криміналізації певних видів діяльності в кіберпросторі, таких як несанкціонований доступ, втручання у роботу систем, підробка даних та інші правопорушення. Конвенція передбачає також механізми міжнародного співробітництва, що значно полегшують обмін інформацією і взаємну правову допомогу між державами-учасницями [4, с. 149].

Інші міжнародні документи, такі як резолюції ООН, Рекомендації Міжнародного союзу електрозв'язку (ITU) та Політика кібербезпеки Європейського Союзу, формують додаткові рамки та стандарти для забезпечення кібербезпеки. Вони не мають такої юридичної сили, як конвенції, але встановлюють орієнтири для національних урядів у формуванні власної політики у сфері кібербезпеки [2, с. 490].

Багато країн розробляють і вдосконалюють свої нормативно-правові акти для забезпечення кібербезпеки. Наприклад, у США діє цілий комплекс законів, зокрема Закон про кібербезпеку (Cybersecurity Act) та Закон про захист критичної інфраструктури (Critical Infrastructure Protection Act), які регулюють діяльність державних і приватних суб'єктів у сфері захисту інформаційних систем. У Європейському Союзі було прийнято Директиву NIS (Network and Information Security Directive), що вимагає від держав-членів вживати

заходів для захисту основних послуг і цифрових провайдерів, а також сприяє координації між державами-членами щодо кіберзахисту [8].

Інші держави, як, наприклад, Японія, Індія та Південна Корея, мають також спеціальні законодавчі акти для забезпечення кібербезпеки, що передбачають обов'язкові вимоги для органів державного управління та приватного сектору, встановлюючи правові наслідки за недотримання відповідних стандартів безпеки [3, с. 169].

Вивчення правових систем різних держав свідчить про значні розбіжності в підходах до нормативно-правового регулювання кібербезпеки. Наприклад, у країнах Європейського Союзу основний акцент робиться на захисті персональних даних громадян та посиленні відповідальності операторів критичної інфраструктури, тоді як у США основною метою є протидія кіберзлочинності на національному рівні та залучення приватного сектору до забезпечення безпеки. Китай демонструє підхід до кібербезпеки як до елементу національної безпеки, запроваджуючи суворий контроль за використанням інтернету і зберіганням даних у межах країни [5, с. 120].

Порівняння різних нормативно-правових підходів дозволяє виявити їхні сильні та слабкі сторони. Наприклад, суворий регламент ЄС щодо персональних даних сприяє захисту приватності, але водночас ускладнює обмін інформацією з країнами, що не забезпечують аналогічного рівня захисту даних. Модель кібербезпеки США є більш гнучкою і швидше адаптується до нових загроз, проте її сильна залежність від приватного сектору може спричиняти недостатню захищеність державних інтересів.

Тож, міжнародний досвід у сфері нормативно-правового регулювання кібербезпеки може слугувати основою для створення ефективних правових механізмів боротьби з кіберзагрозами, враховуючи специфіку кожної держави [2, с. 491].

Інституційні механізми забезпечення кібербезпеки визначають організаційну структуру та роль різних суб'єктів у системі протидії кіберзагрозам. Важливою складовою цих механізмів є розподіл повноважень між державними органами, визначення ролі приватного сектору та побудова системи координації дій національного та міжнародного рівнів. У різних країнах існують відмінні моделі організації кібербезпеки, які відображають їхній підхід до вирішення завдань безпеки, зокрема залежно від національних пріоритетів, ресурсних можливостей та специфічних кіберзагроз.

Держави також по-різному організовують інституційне забезпечення кібербезпеки, залежно від масштабів та пріоритетів у цій сфері. Більшість розвинених країн створили спеціалізовані агентства або департаменти, відповідальні за кібербезпеку. Наприклад, у США діє Агентство з кібербезпеки та інфраструктурної безпеки (CISA), яке займається захистом критичної інфраструктури та координує зусилля щодо кіберзахисту на національному рівні. CISA тісно співпрацює з іншими відомствами, такими як ФБР та Агентство національної безпеки (NSA), що дозволяє ефективно реагувати на загрози [5, с. 121].

У Європейському Союзі важливу роль у забезпеченні кібербезпеки виконує Агентство ЄС з кібербезпеки (ENISA), яке координує діяльність держав-членів у сфері кіберзахисту, надає консультації та забезпечує обмін інформацією про кіберзагрози [8].

У Великій Британії діє Національний центр кібербезпеки (NCSC), який також відповідає за розробку рекомендацій для державних органів і приватного сектору, а також координує операції з кіберзахисту в країні [7].

Важливо зазначити, що міжнародні організації відіграють значну роль у розробці стандартів, регулювань і рекомендацій у сфері кібербезпеки, а також у сприянні співпраці між державами. Основними організаціями є:

– ООН - в рамках ООН діють кілька програм і комітетів, які розглядають питання кібербезпеки. Один із таких – Група урядових експертів ООН з питань кібербезпеки (GGE), яка розробляє норми відповідальної поведінки держав у кіберпросторі та сприяє врегулюванню кіберконфліктів;

– Інтерпол - організація виконує важливу функцію в протидії кіберзлочинності, особливо через забезпечення координації між національними правоохоронними органами різних країн. Інтерпол організовує операції з виявлення кіберзлочинців, сприяє тренінгам для співробітників поліції та надає технологічну допомогу;

– Європейський Союз (ЄС) - у межах ЄС кібербезпека координується через агентства та ініціативи, зокрема як вже зазначалось це – ENISA (Агентство ЄС з кібербезпеки), що працює над розробкою стандартів кібербезпеки, а також координує заходи з підготовки та реагування на кіберзагрози в усіх країнах-членах ЄС [3, с. 169–170];

– НАТО - військово-політичний альянс НАТО надає важливу підтримку країнам-членам у забезпеченні кібербезпеки, особливо у контексті

гібридних загроз. Центр передового досвіду з кіберзахисту НАТО в Таллінні (CCDCOE) займається дослідженнями у сфері кібербезпеки, розробляє рекомендації для членів альянсу та проводить регулярні тренування з кіберзахисту [6, с. 5].

Попри досягнення в галузі міжнародної співпраці, існує чимало викликів. Один із основних викликів полягає у різниці правових систем і підходів до кібербезпеки у різних країнах. Також важливим викликом є питання конфіденційності і дотримання прав людини, що може суперечити потребам держав у сфері національної безпеки.

Інший виклик полягає в розбіжностях у технологічному розвитку країн, які впливають на їхню здатність реагувати на кіберзагрози. Країни з обмеженими ресурсами можуть потребувати технічної допомоги, щоб забезпечити належний рівень кібербезпеки.

Міжнародна співпраця в галузі кібербезпеки є необхідною умовою для ефективного протистояння кіберзагрозам на глобальному рівні. Успішна координація, обмін інформацією та правова допомога значно підвищують спроможність держав запобігати кіберінцидентам, розслідувати кіберзлочини та залучати кіберзлочинців до відповідальності. Проте для повноцінної реалізації цих заходів країнам необхідно постійно вдосконалювати механізми співпраці, гармонізувати свої правові норми та розвивати нові форми взаємодії для протидії кіберзагрозам [7].

Технологічні засоби та стратегії захисту від кіберзагроз є важливою складовою системи кібербезпеки, що забезпечує захист інформаційних систем, мереж і даних. З огляду на швидкий розвиток технологій і постійно зростаючий рівень складності кібератак, держави та організації мають постійно оновлювати свої технологічні інструменти та адаптувати стратегії захисту для протидії новим загрозам.

Системи ідентифікації та управління доступом (Identity and Access Management, IAM) є ключовими інструментами, що дозволяють контролювати доступ користувачів до критичних ресурсів та інформаційних систем. Сучасні системи IAM використовують багатофакторну аутентифікацію (MFA), що значно знижує ризик несанкціонованого доступу до мереж. Біометричні технології, такі як розпізнавання відбитків пальців, сканування райдужної оболонки ока та розпізнавання обличчя, забезпечують додатковий рівень захисту, роблячи процес аутентифікації більш надійним.

Національні уряди та великі корпорації активно впроваджують ці системи для захисту своїх внутрішніх ресурсів. Наприклад, у США у державних установах широко використовуються технології двофакторної аутентифікації з використанням криптографічних токенів для захисту даних від кіберзагроз [9].

Системи виявлення (Intrusion Detection Systems, IDS) і запобігання вторгненням (Intrusion Prevention Systems, IPS) дозволяють фіксувати аномалії в мережевій активності та запобігати потенційним кібератакам. IDS аналізує мережевий трафік і виявляє ознаки можливого вторгнення, тоді як IPS може активно блокувати підозрілу активність. Ці системи часто базуються на аналізі сигнатур і виявленні аномалій за допомогою алгоритмів машинного навчання, що дозволяє ефективно реагувати на атаки, такі як DDoS, фішинг та малваре.

Європейський Союз розробляє спільні стандарти та рекомендації для запровадження IDS та IPS на рівні національних інфраструктур, щоб підвищити рівень захисту держав-членів. Великі компанії, як-от Google і Microsoft, також активно використовують ці системи для захисту своїх серверів і хмарних сервісів [11].

Слід зазначити, що шифрування є одним із найбільш ефективних способів захисту конфіденційних даних від несанкціонованого доступу. Сучасні методи шифрування, такі як AES (Advanced Encryption Standard) і RSA, дозволяють забезпечити надійний захист даних як під час їхнього зберігання, так і під час передавання через мережі. Багато країн, включаючи США, Китай та країни Європейського Союзу, встановлюють національні стандарти шифрування для критичних інфраструктур, таких як банківський сектор та енергетика.

Квантове шифрування стає новим напрямком у розвитку технологій захисту даних. Квантова криптографія використовує властивості квантової фізики для забезпечення абсолютної захищеності каналів передачі даних, що робить її перспективним інструментом для захисту надчутливих даних у майбутньому [10].

Штучний інтелект (ШІ) та машинне навчання (МН) також значно розширюють можливості кібербезпеки, забезпечуючи автоматизацію процесів моніторингу та аналізу кіберзагроз. МН-алгоритми можуть виявляти нові загрози на основі аномалій у поведінці мережевих користувачів і застосовуються для виявлення фішингових атак, виявлення вірусів та інших загроз у режимі реального часу. Наприклад, IBM Watson та Watsonx (сучасні системи штучного інтелекту, яка спеціалізується на обробці

та аналізі великих обсягів неструктурованих даних) використовують ШІ для виявлення кіберзагроз, аналізуючи великі обсяги даних, і пропонує рекомендації з реагування на інциденти.

Deep learning технології дозволяють автоматизувати процеси виявлення кіберзагроз і прогнозування атак на основі історичних даних, а також запобігати новим атакам шляхом аналізу поведінкових шаблонів. Використання ШІ вже стало стандартом у кібербезпеці для багатьох великих корпорацій, таких як Amazon та Microsoft [11].

Окрім систем запобігання атакам, важливою частиною технологічного забезпечення кібербезпеки є створення систем резервного копіювання та відновлення після інцидентів. Ці системи дозволяють швидко відновити інформаційні системи у разі успішної атаки, мінімізуючи можливі збитки та забезпечуючи безперебійність бізнес-процесів. США та Європейський Союз рекомендують впроваджувати резервні копії критичних даних і зберігати їх на захищених серверах або в хмарних сервісах, а також регулярно тестувати процеси відновлення.

Cloud-based резервні копії забезпечують більшу гнучкість та швидкість відновлення, що робить їх популярним рішенням для малих і середніх підприємств, які прагнуть підвищити рівень кібербезпеки за обмежених ресурсів.

Блокчейн-технології стають все більш популярними для захисту даних і забезпечення цілісності інформаційних систем. Блокчейн дозволяє створювати розподілені реєстри, які є практично несанкціонованими для змін, що робить його корисним для захисту критичних даних. Наприклад, Естонія впровадила блокчейн у свої державні системи для захисту даних громадян і забезпечення прозорості процесів, що стосуються зберігання й обробки персональних даних [10].

Міжнародне регулювання кібербезпеки стикається з численними викликами через швидкий розвиток кіберзагроз, різницю в правових системах, політичних інтересах та економічних можливостях держав. Відсутність універсальних стандартів і правових норм, що ускладнює співпрацю між країнами, а також прагнення деяких держав захищати цифрові кордони, як фізичні, посилює труднощі у сфері. Важливим викликом є протидія кіберзлочинності та захист критичної інфраструктури, що вимагають скоординованих зусиль і правової взаємодії між країнами. Наприклад, зусилля Ради Європи через Конвенцію про кіберзлочинність спрямовані на правову співпрацю в боротьбі з кіберзлочинністю.

Перспективи розвитку міжнародного співробітництва включають створення глобальних стандартів, таких як Директива NIS2 Європейського Союзу, що охоплюють технічні, регуляторні та юридичні аспекти кібербезпеки. Важливим напрямком є кібердипломатія, де міжнародні ініціативи ООН спрямовані на досягнення принципів поведінки держав у кіберпросторі для забезпечення стабільності. Окрім цього, актуальним є підвищення рівня кіберосвіченості населення, що сприятиме формуванню безпечного кіберпростору, як це демонструють програми в Канаді та кампанії на кшталт Cyber Awareness Month у Північній Америці.

Висновки. Таким чином, узагальнюючи проведений аналіз міжнародного досвіду адміністративно-правового забезпечення кібербезпеки, можна стверджувати, що ця сфера є однією з ключових у сучасному глобалізованому світі, де кіберзагрози набувають дедалі складніших форм та масштабів. Міжнародна спільнота вже має значні досягнення у боротьбі з кіберзагрозами, але необхідність ефективнішої гармонізації законодавства, розробки універсальних стандартів та посилення співпраці між країнами й надалі залишається актуальною. Ключовими аспектами, що потребують подальшої уваги, є стандартизація правових норм, розвиток кібердипломатії, захист критичної інфраструктури та посилення ролі міжнародних організацій у протидії кіберзлочинності.

Подальші дослідження у цій галузі мають зосередитися на вдосконаленні адміністративно-правових механізмів регулювання кіберпростору з урахуванням швидких технологічних змін. Зокрема, важливим напрямом є дослідження ефективних моделей співпраці між країнами для захисту критичної інфраструктури та створення механізмів обміну інформацією про кіберзагрози.

Література

1. Горулько В. Значення правового регулювання у забезпеченні кібербезпеки в умовах війни: досвід для України. *Вісник Харківського національного університету імені В. Н. Каразіна. Сер.: Право.* 2024. №37. С. 150–155. DOI: https://doi.org/10.26565/2075-1834-2024-37-17.

2. Сливка М. М. Міжнародне співробітництво у сфері забезпечення кібербезпеки України. *Юридичний науковий електронний журнал.* 2022. Вип. 10. С. 489–491.

3. Тарасюк А. Актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях. *Visegrad Journal on Human Rights.* 2020. № 1, С. 167–172.

4. Федонюк С. Політика ЄС в аспекті основних глобальних концепцій інформаційної (кібер) безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2021. № 3 (11). С. 144–168. DOI: https://doi.org/10.29038/2524-2679-2021-03-144-168.

5. Шемчук В. Національна стратегія кібербезпеки США: досвід для України. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 4. С. 119–124.

6. Christou G. Cyber Diplomacy: From Concept to Practice. № 14. Tallinn, 2024. 18 p.

7. Cyber Diplomacy: A New Frontier in International Relations and Professional Practice. *EDRM*. 2024: веб-сайт. URL: https://edrm.net/2024/06/cyber-diplomacy-anew-frontier-in-international-relations-and-professional-practice/ (дата звернення: 11.11.2024).

8. Cybersecurity: how the EU tackles cyber threats: веб-сайт. URL: https://www.consilium.europa.eu/en/policies/cybersecurity/ (дата звернення: 11.11.2024).

9. National Cybersecurity Strategy. The White House. 2023: веб-сайт. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата звернення: 12.11.2024).

10. Safitra M. F., Lubis M., Fakhrurroja H. Counter-attacking cyber threats: a framework for the future of cybersecurity. *Sustainability* 2023. № 15. URL: https://www.mdpi.com/2071-1050/15/18/13369(дата звернення: 12.11.2024).

11. Yampolskiy A. What does 2024 have in store for the world of cybersecurity? *World Economic Forum*. 2024: веб-сайт. URL: https://www.weforum.org/agenda/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/ (дата звернення: 12.11.2024).

Кочман К. П.,
аспірант кафедри кримінального аналізу
та інформаційних технологій
Одеського державного університету
внутрішніх справ

Форос Г. В.,
кандидат юридичних наук, доцент,
завідувач кафедри кримінального аналізу
та інформаційних технологій
Одеського державного університету
внутрішніх справ