УДК 341.1.7
DOI https://doi.org/10.24144/2307-3322.2025.87.4.39

КІБЕРБЕЗПЕКА: СУЧАСНІ ВИКЛИКИ ТА МІЖНАРОДНО-ПРАВОВІ РАМКИ ЩОДО ЗАХИСТУ ДАНИХ

Карвацька С.Б.,
доктор юридичних наук, професор,
в.о. завідувача кафедри міжнародного права
та порівняльного правознавства
Чернівецького національного університету імені Юрія Федьковича
ORCID: 0000-0001-9948-4866
e-mail: s.karvatska@chnu.edu.ua

Маник А.З.,
кандидат юридичних наук,
асистент кафедри міжнародного права
та порівняльного правознавства
Чернівецького національного університету імені Юрія Федьковича
ORCID: 0009-0005-5667-391
e-mail: a.manyk@chnu.edu.ua

Строїч М.І.,
асистент кафедри міжнародного права
та порівняльного правознавства
Чернівецького національного університету імені Юрія Федьковича
ORCID: 0000-0003-0328-2851
e-mail: m.stroich@chnu.edu.ua

Карвацька С.Б., Маник А.З., Строїч М.І. Кібербезпека: сучасні виклики та міжнародно-правові рамки щодо захисту даних.

Стаття присвячена дослідженню поняття та характеристики кібербезпеки як багатовимірної реальності сучасного інформаційного світу, ключових викликів та основних міжнародно- правових рамок щодо захисту даних. Окрему увагу приділено аналізу політичних, безпекових, економічних, правових, соціальних, технологічних, психологічних та культурних аспектів, які загалом мають вагомий вплив на еволюцію загальних і конкретних проблем, які виникають у сфері кібербезпеки. Зі збільшенням кількості атак кібербезпека стає необхідною для глобальної стабільності, що вимагає міжнародної співпраці, стратегічних інвестицій та колективних зусиль для боротьби з цими загрозами. Доведено, що поява у сучасному світі надскладних кіберзагроз та проблема убезпечення конфіденційності даних підштовхнуло багато країн до розробки відповідних правових рамок, що мають урегулювати захист даних і безпеку кіберпростору. Акцентовано увагу на тому, що вирішення міжнародних проблем кібербезпеки та захисту даних вимагає поєднання співпраці між державами, зміцнення технічних і правових можливостей, а також формування глобальної культури кібербезпеки. Проаналізовано, що однією з найважливіших віх у цьому відношенні є Конвенція Ради Європи про кіберзлочинність, спрямована на гармонізацію національних законодавств і зміцнення міжнародного співробітництва у боротьбі з кіберзлочинністю. На сьогодні ЄС відіграє провідну роль у просуванні стандартів захисту даних захисту даних за допомогою Загального регламенту про захист даних (GDPR). Аргументовано, що хоча прогрес у цьому напрямку має підстави для певного оптимізму, багато роботи ще належить виконати для забезпечення безпечного кіберпростору. Наголошено, що продовження співпраці між урядами, бізнесом і громадянським суспільством матиме вирішальне значення для вирішення цього спільного завдання

та захисту наших прав у цифровому світі. Акцентовано, що головне в умовах ескалації кіберзагроз, зокрема, у контексті збройних конфліктів, – створити гармонізовану міжнародно-правову базу для урегулювання питань кібербезпеки та захисту даних.

Ключові слова: безпекове середовище, глобальні виклики, міжнародна безпека, кібербезпека, кіберзлочинність, кібератаки, міжнародно- правові рамки захисту даних, Конвенція Ради Європи про кіберзлочинність.

Karvatska S.B., Manyk A.Z., Stroich M.I. Cyber security: current challenges and international legal framework for data protection.

The article is devoted to the study of the concept and characteristics of cybersecurity as a multidimensional reality of the modern information world, key challenges and the main international legal framework for data protection. Particular attention is paid to the analysis of political, security, economic, legal, social, technological, psychological and cultural aspects, which in general have a significant impact on the evolution of general and specific problems arising in the field of cybersecurity. With the increasing number of attacks, cybersecurity is becoming essential for global stability, which requires international cooperation, strategic investment and collective efforts to combat these threats. The author proves that the emergence of sophisticated cyber threats in the modern world and the problem of data privacy have prompted many countries to develop appropriate legal frameworks to regulate data protection and cyberspace security. The author emphasises that solving international cybersecurity and data protection problems requires a combination of cooperation between States, strengthening of technical and legal capabilities, and formation of a global cybersecurity culture. It is analysed that one of the most important milestones in this regard is the Council of Europe Convention on Cybercrime, which aims to harmonise national legislation and strengthen international cooperation in the fight against cybercrime. Today, the EU plays a leading role in promoting data protection standards through the General Data Protection Regulation (GDPR). It is argued that although the progress in this direction is cause for some optimism, much work remains to be done to ensure a secure cyberspace. It is emphasised that continued cooperation between governments, business and civil society will be crucial to address this common challenge and protect our rights in the digital world. It is emphasised that the main thing in the context of escalating cyber threats, in particular in the context of armed conflicts, is to create a harmonised international legal framework for regulating cybersecurity and data protection.

Key words: security environment, global challenges, international security, cybersecurity, cybercrime, cyberattacks, international legal framework for data protection, Council of Europe Convention on Cybercrime.

Постановка проблеми. Проблема кібербезпеки є багатовимірною, оскільки, окрім різних правових аспектів, вона охоплює велику кількість різноманітних політичних, безпекових, економічних, правових, соціальних, технологічних, психологічних та культурних аспектів. І загалом усі вони мають вагомий вплив на еволюцію загальних і конкретних проблем, які виникають у сфері кібербезпеки, тому лише глибокий системний, та правовий аналіз питань, пов'язаних з кібербезпекою, надасть міжнародному співтовариству держав належні відповіді та прагматичні рішення щодо ефективного реагування на виклики, які стрімко з'являються.

Зростання у сучасному світі надскладних кіберзагроз та проблема убезпечення конфіденційності даних підштовхнуло багато країн до розробки відповідних правових рамок, що мають на меті урегулювати захист даних і безпеку кіберпростору. Однак глобальний характер кіберризиків і несистемних потоків інформаційних даних вимагає створення спільних міжнародно-правоввої системи координат для забезпечення узгоджених стандартів кібербезпеки та заходів захисту даних. Ця потреба спонукала такі організації, як ООН, Європейський Союз (надалі – ЄС), Рада Європи та Організація економічного співробітництва та розвитку (надалі – ОЕСР), запровадити договори, правила та керівні принципи, спрямовані на узгодження правових приписів щодо кібербезпеки та конфіденційності даних.

Метою статті є аналіз природи та основних характеристик кібербезпеки як багатовимірної реальності сучасного інформаційного світу, ключових викликів та основних міжнародно-правових рамок щодо захисту даних.

Стан опрацювання проблематики. Визначення змісту дефінції «кібербезпека», окремі аспекти загальної дослідницької проблематики, зокрема, на національному рівні досліджуються

такими ученими як: І.Д. Бондаренко, Ю.В. Завгородня М. Падалка, Л. Панасевич, І. Пашинська, В.П. Поліщук Варті уваги активні найновіші дослідницькі пошуки та праці у цій сфері іноземних учених та практиків як: Ліндемалдер Грегг (Lindmulder Gregg), Косінскі Метт (Kosinski Matt), Мішра Неха (Mishra Neha), Петер Вршанський (Peter Vršanský), Даніель Беднар (Daniel Bednár), Скотт А. Броун (S.A. Brown), Діба Аалямі Харанді (Diba Aalami Harandi). Але попри активні дослідницькі зусилля, спрямовані на вивчення цього дискусійного і, водночас, актуального питання, варто констатувати потребу у її багаторівневому та системному вивченні.

Виклад основного матеріалу. Кібербезпека є однією з політичних сфер глобального управління даними, що швидко розвивається, і міжнародна спільнота дедалі більше розуміє, що кіберпростір виходить далеко за межі технічних аспектів безпеки мереж і даних, а включає національну та економічну безпеку [1, p. 62]. За оцінками Центру дослідження комп'ютерних злочинів, до 2025 року збитки від кіберзлочинності перевищать 12 трильйонів доларів США [1].

Перш за все, важливо зрозуміти, що таке кібербезпека, і визначити її найбільш нагальні проблеми. Агентство кібербезпеки і безпеки інфраструктури США (CISA) визначає кібербезпеку як захист мереж, пристроїв і даних від несанкціонованого доступу та забезпечення конфіденційності, цілісності і доступності інформації, яка включає технології, практики і політику, спрямовані на запобігання кібератакам і захист комп'ютерних систем, додатків, даних, фінансових активів і людей від таких загроз, як програми-вимагачі, шкідливе програмне забезпечення, фішинг і крадіжка даних [2]. Розвиток кіберконфліктів відбувається у зв'язку виявленням політичного інциденту, який не має механізму правового продовження в інформаційній площині. Дуже важко забезпечувати достовірність інформації, в умовах відсутності санкційної форми захисту швидкого реагування в праві. В свою чергу виникає необхідність у цифровій трансформації, як діяльності направленій на пошук ефективних механізмів захисту інформаційного середовища загалом та окремих видів інформації частково [3]. Визначення та розмежування кібербезпеки для будь-якої юрисдикції пов'язане з багатьма проблемами: у світі існує понад 400 визначень кібербезпеки, а також численні концептуальні суперечки щодо відповідного формулювання кіберзлочинності та кібербезпеки [4].

Варто зауважити, що багато питань кіберзагроз та кібервійн є одночасно, з одного боку, технологічно унікальними і новими, але, з іншого, водночас історично повторюваними та юридично визначеними. Також окремі специфічні характеристики кібератак – у тому числі низька видимість атак і контрдій, ймовірні суперечки щодо ключових фактів і складнощі у встановленні авторства – роблять досягнення міжнародного правового консенсусу в оцінці реальних сценаріїв особливо складним. Тому у найближчій перспективі державам доведеться розробляти наступальні та оборонні стратегії у рамках чинної міжнародно-правової бази, що регулює застосування сили, з огляду на поступову еволюцію інтерпретацій у державній практиці.

Узагальнено фахівці називають «основними характерними ознаками кіберконфліктів, які відмежовують їх від інших загроз, – просторові межі, можливість глобального розвитку у найкоротші терміни, відсутність суб'єктної прив'язки до конкретних дій у кіберпросторі (як правило кібератаками займаються компетентні особи з відповідного розпорядження суб'єктів протиборства)» [5 , с. 504].

За даними міжнародної асоціації телекомунікаційної індустрії GSM Association, «з огляду на прогресуючу взаємодію між цифровим і фізичним вимірами («Інтернет речей» – IoT), тобто пристроїв, підключених до Інтернету, які безперервно взаємодіють з фізичною реальністю через системи датчиків і приводів, до 2025 року на планеті буде 25 мільярдів таких пристроїв [6], ще більше актуалізує досліджувану проблему.

Скотт А. Броун (Brown) з Університету Данді (Велика Британія) наводить спостереження, що «кібербезпека має багато міжнародних і транснаціональних елементів, і її нелегко розділити на «внутрішню», «національну» або «державну» по обидва боки Атлантики, однак з часом кіберзлочинність набула меншого значення по обидва боки Атлантики, оскільки зовнішні або міжнародні виміри кіберпростору стають все більш важливими, наприклад, використання кібервійни в Україні та китайське стеження і дезінформація [7].

На глобальному рівні Організація Об'єднаних Націй також визнала важливість вирішення викликів кібербезпеки та захисту даних. Резолюція Генеральної Асамблеї ООН 70/237 встановлює фундаментальні принципи, такі як повага до прав людини в кіберпросторі та міжнародне співробітництво для запобігання та пом'якшення наслідків кіберінцидентів [8]. Однак, незважаючи на

ці зусилля ці зусилля, залишаються значні прогалини у впровадженні та забезпеченні дотримання міжнародних стандартів кібербезпеки.

Недостатні заходи кібербезпеки роблять економіку, уряди та окремих осіб вразливими до крадіжки персональних даних та порушень приватності. Зі збільшенням кількості атак кібербезпека стає необхідною для глобальної стабільності, що вимагає міжнародної співпраці, стратегічних інвестицій та колективних зусиль для боротьби з цими загрозами [10].

Очевидним є факт, що кіберзлочинці можуть діяти з будь-якої точки світу, користуючись відсутністю координації між національними та міжнародними юрисдикціями щодо вчинення злочинів, не боячись бути притягнутими до відповідальності. Саме тому ця реальність підкреслює нагальну необхідність посилення міжнародної співпраці у сфері кібербезпеки.

У відповідь на таку зростаючу загрозу різні міжнародні та регіональні органи активно співпрацюють над установленням спільних стандартів і загальних принципів у сфері кібербезпеки та захисту даних. Однією з найважливіших віх у цьому відношенні є Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), прийнята у 2001 році і чинна з 2004 року, спрямована на гармонізацію національних законодавств і зміцнення міжнародного співробітництва у боротьбі з кіберзлочинністю. Окрім того, на сьогодні ЄС відіграє провідну роль у просуванні стандартів захисту даних захисту даних за допомогою Загального регламенту про захист даних (GDPR). Це нормативна база, що застосовується до всіх компаній, які обробляють персональні дані громадян ЄС, та встановлює чіткі правила щодо згоди користувачів на обробку їхніх даних, безпеки даних та відповідальності за їх недотримання, незалежно від географічного розташування суб'єкта, що обробляє дані [11].

Щодо місця кібербезпеки у системі міжнародно-правового урегулювання. Міжнародне співтовариство в цілому, окремі держави, відповідні міжнародні та регіональні організації - всі вони повинні приділяти свою увагу подальшому детальному аналізу проблеми кібербезпеки на міжнародному, регіональному та національному рівнях. На сьогодні проблема кібербезпеки як ніколи раніше стає пріоритетною, оскільки вона зачіпає багато сфер діяльності суверенних держав. Надто тому, що масштаби небезпеки, які виникають у результаті сприятливих обставин, пов'язаних з кіберзлочинністю, є непередбачуваними. Аналогічно, масштаб можливих збитків, пов'язаних з кіберзлочинністю, наразі є непередбачуваним. Тим не менш, випадки кіберзлочинності, які вже мали місце в міжнародних відносинах, чітко вказують на загрозу. Кіберзлочинність щодня ставить під загрозу глобальний мир і безпеку, мирний розвиток міжнародних відносин Кіберзлочинність щодня ставить під загрозу глобальний мир і безпеку, мирний розвиток міжнародних відносин [8].

Однією з головних перешкод для ефективного регулювання в кіберпросторі є розбіжність інтересів між державами, а також відмінності в їхніх законодавчих базах і технічних можливостях. У той час як деякі країни виступають за більш обмежувальний і контрольований підхід до Інтернету в інтересах національної безпеки, інші захищають свободу в Інтернеті та конфіденційність користувачів як ключові пріоритети. Цей конфлікт інтересів ускладнює досягнення глобального консенсусу щодо правил і принципів, які повинні регулювати кіберпростір. Більше того, швидкий розвиток технологій створює додаткові виклики для розробки законів і нормативних актів, які були б достатньо гнучкими, щоб адаптуватися до змін у цифровому ландшафті. Штучний інтелект, інтернет речей та інші технологічні інновації створюють нові загрози кібербезпеці, які вимагають гнучкого та проактивного реагування з боку законодавців та регуляторів [11].

Слід визнати, що чинні міжнародно-правові норми досягли своєї певної операційної межі, і сучасне міжнародне право починає «відставати у часі» щодо багатьох сфер регулювання через затримку з прийняттям нових норм та приписів. Також відповідні звичаєві норми міжнародного права не з'явилися через відсутність елементів usus longaevus та opinio iuris. Це стосується і створення нових принципів міжнародного права, «визнаних цивілізованими країнами», допоміжними засобами, як -то судові рішення, щодо урегулювання відносин у кіберпросторі [4].

У вітчизняних дослідженнях наголошується, що «очікується значний розвиток та удосконалення кібератак, включаючи не тільки державні кібероперації, а й атаки на критичну інфраструктуру, саме власне протистояння у кіберпросторі стане однією з основних складових глобальних конфліктів» [14, с. 438]. І.Д. Бондаренко пропонує розглядати як ключове питання той факт, що «у запитах обґрунтовується застосування до кейсів кібератак на Україну концепт «втрати функціональності» – тобто, що «втрата функціональності цивільних критичних інфраструктур (енергетичних, медичних, комунікаційних) через кібератаки повинна розглядатися як напад у контексті МГП, навіть якщо фізичного руйнування не відбулося, оскільки може мати такий самий руйнів-

ний вплив як і фізичні атаки» [13, с. 502]. Автор відстоює позицію, що «реальні кейси масштабних кібератак рф на Україну, розуміння у світі значення фактичних наслідків таких атак, їх здатності до масштабування та впливу на критичні для функціонування держави і життя соціуму сервіси, – все це сприяло посиленню позиції щодо необхідності переосмислення міжнародно-правового змісту кібератак крізь призму міжнародного гуманітарного та міжнародного кримінального права, і Україна є у фарватері цього процесу, а формування національної правової позиції щодо застосування норм міжнародного гуманітарного права до кібероперацій, вірогідно, матиме визначальні міжнародно-правові наслідки у майбутньому» [13].

Висновки. Кіберзлочинність щодня ставить під загрозу глобальний мир і безпеку, мирний розвиток міжнародних відносин. Загалом кібербезпека є складним та міждисциплінарним питанням. Поява у сучасному світі надскладних кіберзагроз та проблема убезпечення конфіденційності даних підштовхнуло багато країн до розробки відповідних правових рамок, що мають урегулювати захист даних і безпеку кіберпростору. Вирішення міжнародних проблем кібербезпеки та захисту даних вимагає багатогранного підходу, що поєднує співпрацю між державами, зміцнення технічних і правових можливостей, а також формування глобальної культури кібербезпеки. Хоча прогрес у цьому напрямку має підстави для певного оптимізму, багато роботи ще належить виконати для того, щоби забезпечення безпечного та захищеного кіберпростору було можливим для всіх. Продовження співпраці між урядами, бізнесом і громадянським суспільством матиме вирішальне значення для вирішення цього спільного завдання та захисту наших прав у цифровому світі. Але головне – в умовах ескалації кіберзагроз, зокрема, у контексті збройних конфліктів, нагальною є потреба у створенні гармонізованої міжнародно-правової бази для ефективної кібербезпеки та захисту даних. Системні та масштабні кібератаки рф на Україну та їх вплив на критичні для функціонування держави сервіси зумовлює необхідність переосмислення застосування практики міжнародного урегулювання відносин кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Mishra Neha. International Trade Law and Global Data Governance:Aligning Perspectives and Practices – An Overview. 2024. February 28. URL: https://ssrn.com/abstract=4741678.
2. Lindemulder Gregg & Kosinski Matt. What Is Cybersecurity?, IBM. https://www.ibm.com/topics/cybersecurity (Aug. 12, 2024).
3. Deibert, R. Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs*. 2018. N 32 (4): 411. https://doi.org/10.1017/S0892679418000618. URL: https://www.cambridge.org/ core/journals/ethics-and-international-affairs/article/abs/toward-a-humancentric-approach-to-cybersecurity/4E8819984202A24186BB0F52E51BC1E4.
4. Vršanský Peter & Daniel Bednár Daniel. Cyber security and the international law *Bratislava Law Review.* 2017. 1(2): 38–49 December. DOI: 10.46282/blr.2017.1.2.74. URL: https://www.researchgate.net/publication/ 340993524_Cyber_security_and_the_international_law.
5. Поліщук В.П., Панасевич Л.А. Міжнародне право і кібербезпека: визначення правового статусу кібератак та кібервійськових операцій. *Юридичний науковий електронний журнал.* 2024. № 2. С. 503–506. DOI https://doi.org/10.32782/2524-0374/2024-2/124.
6. GSMA. The Internet of Things by 2025. URL: https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf.
7. Brown, S.A.W. Beyond the Great Firewall: EU and US Responses to the China Challenge in the Global Digital Economy. *Journal of European Integration.* 2024. N 46 (7). 1089–1110. https://doi.org/10.1080/07036337.2024.2402752. URL: https://www.tandfonline.com/ doi/full/10.1080/07036337.2024.2402752.
8. United Nations. General Assembly Distr.:30 December 2015. Seventieth session. Agenda item 92. 15-16991 (E).
9. Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455)]. URL: https://digitallibrary.un.org/record/ 815989/files/A_RES_70_237-EN.pdf.
10. Harandi Diba Aalami. International Legal Frameworks on Cybersecurity and Data Protection Law. *Denver Journal of International Law & Policy.* 2025. January 7. URL: https://djilp.org/international-legal-frameworks-on-cybersecurity-and-data-protection-law.

11. Cybersecurity and International Law: Addressing Global Challenges in Cyberspace. *The Impact Lawyers Newsroom.* URL: https://theimpactlawyers.com/a rticles/cybersecurity-and-international-law-addressing-global-challenges-in-cyberspace.
12. The Impact Lawyers Newsroom. 2025. 15 February. URL: https://theimpactlawyers.com/articles/cybersecurity-and-international-law-addressing-global-challenges-in-cyberspace.
13. Бондаренко І.Д. Концепт «втрати функціональності» в контексті визнання кібератак воєнним злочином. *Юридичний науковий електронний журнал.* 2024. № 10. С. 500–503 DOI: https://doi.org/10.32782/2524-0374/2024-10/115. URL: http://www.lsej.org.ua/ 10_2024/117.pdf.
14. Падалка М., Пашинська І. Основні тенденції розвитку безпекового середовища на глобальному рівні. *Юридичний науковий електронний журнал.* 2024. № 12. С. 436–439 DOI https://doi.org/10.32782/2524-0374/2024-12/99. URL: http://www.lsej.org.ua/12_2024/101.pdf.