Єлизавета НІКІТІНА,
студентка 4-го курсу
гуманітарно-правового факультету
Національного аерокосмічного університету
«Харківський авіаційний інститут»,
м. Харків, Україна
e-mail: nikitina2003liza@gmail.com

Науковий керівник: Наталія ФІЛІПЕНКО,
доктор юридичних наук, професор,
професор кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету
«Харківський авіаційний інститут»
ORCID: https://orcid.org/0000-0001-9469-3650
e-mail: n.filipenko@khai.edu

DOI: https://doi.org/10.32620/pls.2025.8.63

МІЖНАРОДНО-ПРАВОВІ ЗАСАДИ КІБЕРСОЛІДАРНОСТІ ЯК МЕХАНІЗМУ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

***Анотація**: У статті досліджено міжнародно-правові засади кіберсолідарності як нового механізму колективної безпеки у цифровому середовищі. Проаналізовано нормативну базу Європейського Союзу, зокрема Регламент (ЄС) 2025/38 «Про кіберсолідарність», а також визначено роль НАТО й ООН у формуванні принципів відповідальної поведінки держав у кіберпросторі. Розкрито участь України у становленні міжнародної системи кіберсолідарності через двосторонні та багатосторонні ініціативи, інтеграцію до євроатлантичних структур і розвиток правових механізмів захисту критичної інфраструктури. Обґрунтовано значення кіберсолідарності як складової сучасної системи міжнародної безпеки.*

***Ключові слова:** кіберсолідарність, міжнародне право, кібербезпека, критична інфраструктура, колективна кіберстійкість.*

У XXI столітті кіберпростір перетворився на сферу геополітичного протистояння, де атаки на критичну інфраструктуру стали інструментом гібридної війни. В умовах зростаючої цифрової взаємозалежності держав, питання забезпечення кібербезпеки виходить за межі національної юрисдикції та потребує ефективної міжнародно-правової відповіді. На перетині цих тенденцій постає концепція кіберсолідарності як новий простір колективного реагування на кіберзагрози. Водночас, незважаючи на існування міжнародно-правових норм щодо відповідальної поведінки держав у кіберпросторі, відсутність узгодженого й ефективного механізму їх практичної реалізації обумовлює актуальність наукового аналізу кіберсолідарності. Фрагментарність нормативної бази та недосконаліть координаційних процедур між державами створюють виклики для захисту об'єктів критичної інфраструктури, що потребує розробки нових правових і організаційних інструментів у межах міжнародного права для забезпечення комплексного захисту кібербезпеки.

Кіберсолідарність передбачає скоординовану взаємодію держав у сфері виявлення, стримування та нейтралізації кіберінцидентів, зокрема шляхом обміну інформацією, технічної підтримки, спільного реагування та правового засудження зловмисних дій. Цей підхід закріплюється в міжнародних документах, зокрема в Регламенті (ЄС) 2025/38 «Про кіберсолідарність» (EU Cyber Solidarity Act), який передбачає створення Європейського кіберщита, механізмів надзвичайного реагування та системи спільного аналізу інцидентів. Аналогічні підходи реалізуються в кіберстратегії НАТО та резолюціях Генеральної Асамблеї ООН щодо відповідальної поведінки держав у кіберпросторі.

Вразливість критичної інфраструктури в умовах війни наочно засвідчує необхідність дієвих механізмів кіберсолідарності. Війна Росії проти України виявила ступінь нашої залежності від цифрових технологій та крихкість цифрового простору. Вона спровокувала сплеск кібератак, які були особливо руйнівними, коли вони були спрямовані на критично важливу інфраструктуру, таку як енергетика, охорона здоров'я чи фінанси, через зростаючу залежність від інформаційних технологій, що робить цю інфраструктуру ще більш

вразливою. Як свідчать дані CERT-UA, кількість кіберінцидентів, спрямованих на критичну інфраструктуру України значно зросла, якщо у 2022 та 2023 році фахівці відреагували на 2,2 тисячі та 2,5 тисячі кіберінцидентів відповідно, то у 2024 році їх було вже 4,5 тисячі [1].

Практична реалізація кіберсолідарності щодо України здійснюється через систему двосторонніх і багатосторонніх міжнародних партнерств, програм технічної допомоги та участь держави в ініціативах ЄС, НАТО, G7 і США, спрямованих на підвищення кіберстійкості та захист критичної інфраструктури.

Національні правові механізми, що відображають принцип кіберсолідарності у сфері захисту критичної інфраструктури, закріпленні в Законі України «Про основні засади забезпечення кібербезпеки України»,який визначає засади державної політики у сфері кіберзахисту, передбачаючи міжнародну співпрацю суб'єктів кібербезпеки згідно з п. 3 ст. 14 через двосторонні та багатосторонні механізми. Крім того,відповідно до п. 7 ст. 8, Міністерство закордонних справ України сприяє євроінтеграції у сфері кібербезпеки, координує взаємодію з міжнародними партнерами для реагування на кібератаки, бере участь у формуванні міжнародних норм поведінки в кіберпросторі, узгоджує санкційні заходи у відповідь на деструктивну кіберактивність та забезпечує проведення спільних заходів з Європейським Союзом для посилення кіберстійкості України [2].

З огляду на визначені законодавчі механізми міжнародної взаємодії, пріоритетом реалізації Стратегії кібербезпеки України на 2025 рік передбачено забезпечення міжнародного співробітництва шляхом участі у спільних проектах з партнерами, впровадження кращих світових практик та міжнародних стандартів (зокрема у співпраці з такими організаціями, як NATO Cyber Defence Management Board, Cyberspace Operations Centre, NATO Computer Incident Response Capability, NATO Cooperative Cyber Defence Centre of Excellence), а також гармонізацію національної нормативної бази з європейськими і світовими вимогами у сфері кібербезпеки [3].

Під час повномасштабної війни в Україні принцип кіберсолідарності набув реального змісту як інструмент міжнародно-правового захисту критичної інфраструктури. США, Естонія та IT-коаліція багатьох західних держав надавали Україні технологічну, фінансову й експертну допомогу для захисту об'єктів енергетики, зв'язку й операторів критичної інфраструктури. Наприклад, спільний проєкт з Естонською Академією електронного управління (eGA) допомагав розвивати системи управління ризиками, кризовими ситуаціями, резервне копіювання даних і навчання IT-фахівців [4]. Також одним із результатів успішного партнерства є проєкт «Готовність кібербезпеки для критичної інфраструктури в Україні», який втілює Академія електронного управління (eGA) у партнерстві з Державною службою спеціального зв'язку та захисту інформації України, яку профінансували уряд Сполучених Штатів Америки та Естонський центр міжнародного розвитку (ESTDEV).Метою якого було посилення стійкості українських органів влади та операторів критичної інфраструктури до кіберзагроз. Він допомагає розвивати системи управління ризиками й кризами та підвищувати загальний рівень кіберготовності [5].

У цьому контексті доцільним є визначення поняття критичної інфраструктури. Зокрема, «критична інфраструктура» визначена як сукупність об'єктів, які є стратегічно важливими для економіки і національної безпеки (п.9 ст 1 ЗУ «Про критичну Інфраструктуру»), а «об'єкти критичної інфраструктури» становлять складові елементи критичної інфраструктури, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам (п.13 ст.1 ЗУ «Про критичну Інфраструктуру») [6]. Це можуть бути електростанції, системи водопостачання, місця зберігання та виготовлення харчових продуктів, важливі транспортні вузли, телекомунікаційні мережі, медичні установи та багато інших пріоритетних об'єктів. Безпека цих об'єктів та їх функціонування як у нормальних умовах, так і в умовах надзвичайних ситуацій, таких як воєнний стан — один із пріоритетів держави [7].

Правовий режим захисту критичної інфраструктури тісно пов'язаний з міжнародним правом кібербезпеки, оскільки обидва спрямовані на запобігання кіберзагрозам, забезпечення стабільності цифрового простору та розвиток міжнародної співпраці у сфері безпеки.

У межах системи ООН питання кібербезпеки розглядається крізь призму принципів незастосування сили, суверенної рівності та невтручання у внутрішні справи держав. Як підкреслив Міжнародний суд ООН у Дорадчому висновку щодо законності застосування ядерної зброї (1996), положення статей 2, 4, 42 і 51 Статуту ООН «не стосуються конкретної зброї вони застосовуються до будь-якого застосування сили, незалежно від зброї, що використовується» [8]. Це положення є підставою для поширення заборони застосування сили на дії у кіберпросторі, включно з масштабними кібератаками. Як зазначає М. Яцишин, норми сучасного міжнародного права «є чинними і для кіберпростору», що означає заборону актів агресії у цифровій сфері на підставі принципів суверенітету та невтручання [8]. Розвиваючи ці положення, Генеральна Асамблея ООН у Резолюції № 73/266 від 22 грудня 2018 року «Заохочення відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки» закликала держави відповідально використовувати інформаційно-комунікаційні

технології з метою усунення загроз в сфері інформаційної безпеки. Водночас відсутність єдиної позиції держав щодо порогу «збройного нападу» у кіберпросторі залишає питання самооборони відкритим для наукової дискусії [8, 9].

Україна посідає активну позицію у формуванні міжнародно-правової системи кіберсолідарності, інтегруючись у глобальні механізми протидії кіберзлочинності та кіберзагрозам. Приєднання до Будапештської конвенції у 2006 році забезпечило гармонізацію національного законодавства з міжнародними стандартами у сфері кібербезпеки, а також участь у спільних розслідуваннях, обміні електронними доказами та розбудові правової співпраці між державами. Розширення партнерства відбувається завдяки проєкту CyberEast+ (2024–2027),що спрямований на вдосконалення української політики та законодавства відповідно до норм Конвенції. Водночас Україна орієнтується на європейські стандарти, передбачені Директивою ЄС 2013/40/EU щодо атак на інформаційні системи, адаптуючи власне кримінальне законодавство для уніфікації визначень кіберзлочинів та санкцій [10].

Крім того, важливими платформами міжнародної співпраці стали Європол і Європейський центр боротьби з кіберзлочинністю (EC3), через які Україна долучається до спільних операцій із розслідування кібератак і кіберзлочинів, зокрема в межах Joint Cybercrime Action Taskforce (J-CAT). Підписання у листопаді 2023 року угоди з Агентством ЄС з кібербезпеки (ENISA) закріпило стратегічне партнерство, що передбачає обмін досвідом, спільні навчання та консультації щодо імплементації європейських норм. Участь України в ініціативах ЄС, як-от CyberEast, CyberEurope чи освітніх програмах Європолу та ENISA, сприяє підвищенню кваліфікації фахівців і розвитку кіберстійкості держави [10].

У межах посилення колективної кіберстійкості, Європейська Комісія презентувала Європейський акт про кіберсолідарність 18 квітня 2023 року (COM/2023/209 final) як законодавчу ініціатива, що мала на меті зміцнення спроможностей Європейського Союзу у виявленні, підготовці та реагуванні на кіберзагрози. Документ передбачав створення трьох взаємопов'язаних механізмів. Першим є Європейський кіберщит (European Cyber Shield), який об'єднує національні та транскордонні центри безпеки для спільного моніторингу, виявлення та аналізу кіберінцидентів. Другим є Механізм кібернадзвичайних ситуацій (Cyber Emergency Mechanism), що включає формування Резерву кібербезпеки ЄС (EU Cybersecurity Reserve) для оперативного реагування на масштабні атаки. Третім є Механізм перегляду кіберінцидентів (Cybersecurity Incident Review Mechanism), який забезпечує оцінку значних кіберінцидентів і формування рекомендацій для підвищення готовності держав-членів [11].

Реалізація запропонованих механізмів отримала подальший розвиток у грудні 2024 року, коли було ухвалено Регламентт (EU) 2025/38, який набув чинності 15 січня 2025 року. Регламент визначає правові рамки функціонування пан'європейської системи кіберсповіщення (European Cybersecurity Alert System) та спрямований на підвищення колективної кіберстійкості, розвиток кадрового потенціалу і посилення координації між державами-членами з урахуванням принципів добровільності та поваги до національної безпеки, посилюючи тим самим стратегічну автономію Союзу в кіберпросторі [12].

Паралельно з розвитком нормативної бази ЄС, Україна розширює свою участь у спільних оборонних кіберпроєктах. 16 травня 2023 року, Україна отримала статус країни-контрибутора Центру передового досвіду співпраці з кіберзахисту НАТО (CCDCOE), що засвідчило визнання її ролі у спільній системі міжнародної кібербезпеки. Україна бере участь у найбільшому у світі навчанні Locked Shields під керівництвом НАТО, отримує технічну допомогу (зокрема ліцензії, програмне забезпечення та консультації) через Cyber Defense Trust Fund та використовує платформу спільного реагування на інциденти. Відповідно, інтеграція України в європейські та євроатлантичні кіберструктури сприяє її становленню як повноправного учасника глобальної системи кіберсолідарності, зміцнюючи як власну, так і колективну безпеку [13].

Таким чином, враховуючи сучасний стан кібербезпеки та роль міжнародного права, можна відзначити, що механізм формування кіберсолідарності є необхідною умовою для підтримки стабільності функціонування критичної інфраструктури в умовах цифрової інтеграції та глобальних ризиків. Україна активно інтегрується в міжнародні правові та інституційні структури, що дозволяє зміцнити національні підходи до захисту цифрового простору, впроваджувати сучасні технології та нормативні практики. Скоординовані дії з міжнародними партнерами, впровадження загальновизнаних стандартів та участь у спільних ініціативах сприяють формуванню ефективної системи кіберзахисту, яка відповідає сучасним вимогам реалізацій міжнародного співтовариства. Отже, кіберсолідарність розширює уявлення про міжнародну безпеку, додаючи до неї цифровий вимір і закріплюючи відповідальність держав за спільне реагування на кіберзагрози. Це формує нову практику взаємодії, де безпека в кіберпросторі стає частиною загального правового порядку між державами.

Бібліографічні посилання

1. Наймасштабніші кібератаки на Україну. Слово і Діло. 2025 URL: https://www.slovoidilo.ua/2025/03/24/infografika/bezpeka/najmasshtabnishi-kiberataky-ukrayinu

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.Редакція від 19.10.2025 URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 15.11.2025)

3. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України від 07.03 2025 р. № 204-р URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#top

4. Посилення захисту критичної інфраструктури України:Стратегічні висновки й кращі міжнародні практики. Естонська академія електронного урядування (eGA). 2025 URL: https://ega.ee/wp-content/uploads/2025/06/ciip-ua-204x275mm-ua-webi.pdf

5. Критична інфраструктура під прицілом: як Україна вибудовує кіберстійкість і чого світ може в нас повчитись. Громадське.2025 URL: https://hromadske.ua/specials/254318-krytychna-infrastruktura-pid-prytsilom-iak-ukrayina-vybudovuye-kiberstiykist-i-choho-svit-moze-v-nas-povchytys

6. Закон України «Про критичну Інфраструктуру» від 16 листопада 2021 року № 1882-IX. Редакція від 21.09.2024 URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

7. Об'єкти критичної інфраструктури України: все, що варто знати. Київ Пост.2024 URL: https://www.kyivpost.com/uk/post/28283 (дата звернення 12.11.2025)

8. Карвацька С.Б., Маник А.З., Яремчук В.В. Кіберпростір: міжнародно-правове регулювання та практика застосування прецедентного права МС ООН. Електронне наукове видання «Аналітично-порівняльне правознавство».2025 URL: https://app-journal.in.ua/wp-content/uploads/2025/04/182.pdf

9. Цебенко С.Б. Міжнародні та європейські гарантії забезпечення прав людини в кіберпросторі. Юридичний науковий електронний журнал.2022 URL: http://lsej.org.ua/5_2022/161.pdf

10. Костюченко Я. М.Співпраця україни та єс у сфері кібербезпеки: механізми боротьби з кіберзлочинністю.Проблеми сучасних трансформацій. серія: право, публічне управління та адміністрування.2025 URL: https://reicst.com.ua/pmtl/article/view/2025-15-01-10/2025-15-01-10

11. Car P. Regulation on measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. In «A Europe Fit for the Digital Age».2024 URL: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-cyber-solidarity-act

12. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act). Official Journal of the European Union. 2025 URL: https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng (дата звернення 15.11.2025)

13. National Security and Defense Council of Ukraine.Ukraine becomes a member of the NATO's Cooperative Cyber Defense Center of Excellence.2023 URL: https://www.rnbo.gov.ua/en/Diialnist/6335.html?PRINT#:~:text=Council%20of%20Ukraine-,Ukraine%20becomes%20a%20member%20of%20the%20NATO's%20Cooperative%20Cyber%20Defense,status%20of%20a%20contributing%20country.

E. Nikitina

International legal basis of cyber solidarity as a mechanism for protecting critical infrastructure.

Abstract: The article analyzes the international legal foundations of cyber solidarity as a new mechanism for collective security in the digital environment. It analyzes the regulatory framework of the European Union, in particular Regulation (EU) 2025/38 on cyber solidarity, and defines the role of NATO and the UN in shaping the principles of responsible behavior of states in cyberspace. It reveals Ukraine's participation in the formation of an international cyber solidarity system through bilateral and multilateral initiatives, integration into Euro-Atlantic structures, and the development of legal mechanisms for protecting critical infrastructure. It substantiates the importance of cyber solidarity as a component of the modern international security system.

Keywords: cyber solidarity, international law, cybersecurity, critical infrastructure, collective cyber resilience.

Зразок для цитування:

Нікітіна Є. Міжнародно-правові засади кіберсолідарності як механізму захисту критичної інфраструктури. Пропілеї права та безпеки, 2025. №8. С. 247-250. DOI: https://doi.org/10.32620/pls.2025.8.63.