

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ПІВДЕННИЙ РЕГІОНАЛЬНИЙ ЦЕНТР
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ



КАФЕДРА МІЖНАРОДНОГО ТА ЄВРОПЕЙСЬКОГО ПРАВА

«ПРАВА ЛЮДИНИ В ПЕРІОД ЗБРОЙНИХ КОНФЛІКТІВ»

Збірник матеріалів Міжнародної науково-практичної конференції
(м. Одеса, 31 жовтня 2025 року)

*Друкується за наказом ректора Національного університету
«Одеська юридична академія» О. В. Тодошчака
(наказ № 3110-44 від 02.10.2025 р.)*

Відповідальний редактор – проректор з наукової роботи Національного університету «Одеська юридична академія», доктор юридичних наук, професор, професор кафедри міжнародного та європейського права, Заслужений юрист України **Аракелян Мінас Рамзесович**

Заступник відповідального редактора – завідувач кафедри Філософії права Юридичного факультету Близькосхідного університету (Кіпр), член-кореспондент Міжнародної академії порівняльного права **Дамірлі Мехман Алишах огли**

Заступник відповідального редактора – доктор юридичних наук, професор, завідувач кафедри міжнародного та європейського права Національного університету «Одеська юридична академія» **Бехруз Хашматулла Набієвич**

Укладачі:

Бехруз Хашматулла Набієвич – доктор юридичних наук, професор, завідувач кафедри міжнародного та європейського права Національного університету «Одеська юридична академія»;

Мануїлова Катерина Вікторівна – кандидатка юридичних наук, доцентка, доцентка кафедри міжнародного та європейського права Національного університету «Одеська юридична академія»;

Грушко Мальвіна Валеріївна – кандидатка юридичних наук, доцентка, доцентка кафедри міжнародного та європейського права Національного університету «Одеська юридична академія»;

Войтович Павло Петрович – PhD в галузі права, доцент кафедри міжнародного та європейського права Національного університету «Одеська юридична академія».

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

Адреса редколегії:

Національний університет «Одеська юридична академія», кафедра міжнародного та європейського права, м. Одеса, 65009, вул. Фонтанська дорога, 23.
Тел. +38(048)719 8685.

«Права людини в період збройних конфліктів»: Міжнародна науково-практична конференція, присвячується Міжнародному дню прав людини, який відзначається міжнародною спільнотою 10 грудня. **31 жовтня 2025 р., м. Одеса: збірник матеріалів конференції. Одеса. 2025. 219 с.**

© НУ «Одеська юридична академія», 2025
© Кафедра міжнародного та європейського права НУ «ОЮА»

5. Kaye D. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. United Nations Human Rights Council, 2015. 28 p.
6. Kohl U. The right to be forgotten in data protection law and two western cultures of privacy. *International and Comparative Law Quarterly*. 2023. Vol. 72, no. 3. P. 737–769. URL: <https://doi.org/10.1017/S0020589323000258>
7. Moyakine E. Online Anonymity in the Modern Digital Age: Quest for a Legal Right. *Journal of Information Rights, Policy and Practice*. 2016. Vol. 1, no. 1. URL: <https://doi.org/10.21039/irpandp.v1i1.21>.
8. Pansu L. Evaluation of 'Right to Disconnect' Legislation and Its Impact on Employee's Productivity. *International Journal of Management and Applied Research*. 2018. Vol. 5, no. 3. P. 99–119. URL: <https://doi.org/10.18646/2056.53.18-008>.
9. Sartor G. The right to be forgotten in the Draft Data Protection Regulation. *International Data Privacy Law*. 2015. Vol. 5, no. 1. P. 64–72. URL: <https://doi.org/10.1093/idpl/ipu030>.
10. Yuste R. Advocating for neurodata privacy and neurotechnology regulation. *Nature Protocols*. 2023. Vol. 18, no. 10. P. 2869–2875. URL: <https://doi.org/10.1038/s41596-023-00873-0>.

Ключові слова: права людини, цифрові права людини, право на відключення, цифрова спадщина, нейроприватність, право бути забутим, цифрова анонімність.

Key words: human rights, digital human rights, right to disconnect, digital legacy, neuroprivacy, right to be forgotten, digital anonymity.

Грушко Мальвіна Валеріївна

кандидатка юридичних наук, доцентка, доцентка кафедри міжнародного та європейського права Національного університету «Одеська юридична академія»

КІБЕРПРОСТІР ЯК НОВА СФЕРА ЗБРОЙНОГО ПРОТИСТОЯННЯ: МІЖНАРОДНО-ПРАВОВІ ВИКЛИКИ

Дослідження кіберпростору у площині збройного протистояння є новим і надзвичайно актуальним питанням на сьогодні. Оскільки, коли розпочинається збройний конфлікт, то він має на меті не тільки загарбання територій та природних ресурсів, а й вплинути на психіку людей й змінити їх думку, стосовно цього.

У Підсумковій декларації 42-го саміту G7 від 26-27 травня 2016 року кіберпростір охарактеризовано як доступне, відкрите, взаємозалежне, надійне та захищене середовище. Згідно з міжнародною стратегією співробітництва у кіберпросторі, держави мають дотримуватися цілей і принципів, визначених у Статуті ООН, зокрема заборони застосування сили та обов'язку мирного врегулювання спорів, щоб забезпечити мир і безпеку в кіберпросторі. Усі країни повинні протидіяти проявам агресії, запобігати мілітаризації кіберпростору та розв'язанню конфліктів, а також вирішувати суперечки виключно мирними засобами [2].

У сучасних умовах, боротьба з кіберзагрозами розглядається як ключовий пріоритет національної безпеки та важливий чинник розвитку військової, соціальної, економічної та інших сфер. Перебіг російсько-української війни засвідчує зростання ролі інноваційних технологій у збройному протистоянні, активну цифровізацію бойових дій з метою збереження людських ресурсів, а також посилення кібератак на противника з метою психологічного тиску та підриву національних інтересів. Спостерігається, тенденція щодо

застосування асиметричних і непрямих стратегій у кіберпросторі, що поєднують військові, політичні, економічні та інформаційно-психологічні інструменти впливу для досягнення цілей, які раніше вирішувалися переважно збройним шляхом.

Попри відсутність у міжнародному праві чітко визначених критеріїв для застосування стандарту «збройного нападу», постає питання: чи можуть кібератаки вважатися таким нападом. На це питання міститься відповідь в міжнародних джерелах, зокрема, на запрошенні Центру передового досвіду з кіберзахисту НАТО Міжнародна група експертів розробила Талліннський механізм – міжнародний формат підтримки стійкості цивільної інфраструктури України перед кіберзагрозами, у якому беруть участь 11 країн. Цей документ визначає норми застосування міжнародного права до кібероперацій. Експерти дійшли згоди, що окремі кібероперації можуть бути настільки серйозними, що кваліфікуються як збройний напад, відповідно до консультативного висновку Міжнародного суду ООН щодо ядерної зброї, де зазначено, що спосіб здійснення нападу не впливає на кваліфікацію дії як збройного нападу.

Держави по-різному визначають, за яких умов кібератака може вважатися збройним нападом. Як, приклад Велика Британія зазначає, що втручання в роботу ядерного реактора, яке спричиняє масову загибель людей, може бути розцінене як незаконне застосування сили або збройний напад. Також до таких дій можуть належати атаки на ключові медіа-сервіси, здійснені за допомогою кіберзасобів.

Франція, вважає кібератаку збройним нападом, якщо вона спричиняє значні людські втрати, фізичну чи економічну шкоду, або паралізує критично важливу інфраструктуру, викликаючи технологічні чи екологічні катастрофи. А, у Нідерландах кваліфікація кібератаки залежить від масштабу, наслідків та транскордонного характеру інциденту. У Франції та Великій Британії кібератаки найвищого рівня (Рівень 5) розглядаються як збройний напад відповідно до статті 51 Статуту ООН, а Нідерланди визначають аналогічну категорію А для атак, що загрожують основним активам безпеки [1].

Загалом, виділяють три основні типи кібератак:

- кібершпигунство – розвідувальні дії, що можуть набувати ознак збройного нападу;
- маніпулювання інформаційним середовищем – вплив на громадську думку чи виборчий процес через соціальні мережі;
- знищення критичних активів безпеки – атаки на інфраструктуру (атомні станції, енергомережі, фінансові системи тощо).

Проблеми, пов'язані з доведенням фактів у міждержавних судових справах, зокрема при кваліфікації протиправних дій, не є унікальними для сфери кібероперацій. Ще до появи «кібер ери» Міжнародний суд ООН у справі «Нікарагуа проти США» (1986) зазначив, що основна складність полягає не у юридичному процесі приписування діяння державі, а у збиранні достовірних матеріальних доказів, які підтверджують особу порушника. Розслідування кібератак між державами ускладнюється тим, що в міжнародному праві відсутні єдині правила щодо надання доказів. У справах, де йдеться не про кримінальну відповідальність, міжнародні судові органи самостійно визначають стандарти доказування залежно від конкретних обставин. Міжнародний суд ООН, як головний судовий орган Організації Об'єднаних Націй, розглядає позови про відповідальність держав за порушення норм міжнародного права, якщо сторони процесу визнали його юрисдикцію.

Професор міжнародного права Марко Роскіні у своїх дослідженнях практики Міжнародного суду ООН щодо доказування у справах, пов'язаних із кіберопераціями, виділив основні чинники, які впливають на вирішення кіберпитань. По-перше, тягар доказування у кіберсправах залишається незмінним – він покладається на сторону, що

висуває певне твердження. По-друге, хоча єдиного стандарту доказування для всіх справ, пов'язаних із міжнародною відповідальністю за кібероперації, поки не визначено, заяви про самозахист від кібернападів мають підтверджуватися чіткими та переконливими доказами. Водночас доведення того, що певна держава здійснювала кібероперації, які становлять міжнародний злочин, також потребує вагомої доказової бази. По-третє, Міжнародний суд ООН може враховувати відмову сторони надати засекречені документи, однак не зобов'язаний робити з цього негативні висновки. Також, Суд надає підвищену доказову силу офіційним документам держав і міжнародних організацій, зокрема ООН, вважаючи їх більш надійними джерелами доказів [3].

У підсумку, можна зазначити, що міжнародне право не містить чітких критеріїв для визначення, коли кібератака може вважатися збройним нападом, однак низка джерел вказує, що атаки, які підривають або знищують критично важливі активи безпеки, особливо надзвичайного масштабу, можуть бути кваліфіковані як збройний напад. Водночас, розслідування таких інцидентів ускладнюється відсутністю єдиних правил доказування в міжнародному праві. Заяви про самозахист від кібероперацій мають підтверджуватися чіткими та переконливими доказами. При розгляді кіберсправ, Міжнародний суд ООН надає перевагу офіційним документам держав і міжнародних організацій та діє з обережністю у формуванні висновків. Якщо ж сторона не має доступу до прямих доказів через контроль їх іншою державою, Суд може допустити непрямі докази, за умови, що вони не викликають обґрунтованих сумнівів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Статут Організації Об'єднаних Націй і Статут Міжнародного Суду : Статут Орг. Об'єдн. Націй від 26.06.1945 : станом на 16 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/995_010#Text (дата звернення: 16.10.2025).
2. G7 Ise-Shima Leaders' Declaration G7 Ise-Shima Summit, 26-27 May 2016: <http://www.mofa.go.jp/files/000160266.pdf>; G7 Principles and Actions on Cyber. Ise-Shima, Japan, May 27, 2016. URL: <http://www.g8.utoronto.ca/summit/2016shima/cyber.html>.
4. Mačák Kubo. From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers. Leiden Journal of International Law. 2017. N 30 (4). P 877–899. doi:10.1017/S0922156517000358.

Ключові слова: кіберпростір, збройне протистояння, міжнародне право.

Key words: cyberspace, armed confrontation, international law.

Войтович Павло Петрович

*PhD з права, доцент кафедри міжнародного та європейського права
Національного університету «Одеська юридична академія»*

ПРАВО НА ПРАВДУ ТА ІНФОРМАЦІЙНІ ПРАВА ЛЮДИНИ: ПОСТАНОВКА ПРОБЛЕМИ

Сьогодні все частіше зустрічаються заклики щодо забезпечення реалізації права на правду. Втім, що розуміється під цим правом, що розуміється під «правдою», які складові такого права, як воно може бути реалізоване, чи може воно бути обмежене, кого стосується право на правду, чи є воно інформаційним, або як це право співвідноситься з інформаційними правами людини?

Секція № 9

Міжнародні універсальні механізми захисту прав людини

КАНЄНБЕРГ-САНДУЛ О.К.

Особливості міжнародно-правового регулювання статусу українських біженців в Європейському Союзі.....183

ФАСІЙ А.В.

Міжнародно-правові засади розроблення стратегій психічного здоров'я у післявоєнний період.....185

ЧЕРНЯВСЬКИЙ М.В.

Миротворчі операції ООН і забезпечення норм міжнародного гуманітарного права та прав людини у період збройних конфліктів.....188

БУГАЄЦЬ А.С.

Сучасні тенденції міжнародно-правового регулювання інтелектуальної власності.....191

Секція № 10

Захист прав людини в інформаційній сфері: сучасні виклики

ДРАКОХРУСТ Т.В., КРАВЕЦЬ А.А.

Перспективи розвитку біометричних технологій у сфері міграції (EES): виклики для права та суспільства.....194

ДРАКОХРУСТ Т.В., ПЕТРЕНКО В.А.

Вплив EES на свободу пересування осіб у Європейському Союзі.....196

ВИШНЯКОВА А.О., ДИМОВ К.Б.

Особливості доказування злочинів, які пов'язані із пропагандою.....197

ГРАБИНСЬКИЙ М.І.

Цифрові права людини: еволюція, виклики та перспективи правового регулювання....201

ГРУШКО М.В.

Кіберпростір як нова сфера збройного протистояння: міжнародно-правові виклики....204

ВОЙТОВИЧ П.П.

Право на правду та інформаційні права людини: постановка проблеми.....206

БОНДАРЬ О.В.

Адміністративні процедури доступу до публічної інформації як елемент належного врядування.....208

ОМЕЛЬЧЕНКО І.І.

Співвідношення принципу пропорційності з принципами міжнародного гуманітарного права.....211