

**ПРАВО НА КІБЕРБЕЗПЕКУ: СПІВПРАЦЯ ЩОДО ПРОТИДІЇ КІБЕРЗАГРОЗАМ
В УКРАЇНІ ТА ЄС****THE RIGHT TO CYBERSECURITY: COOPERATION ON COUNTERING CYBER THREATS
IN UKRAINE AND THE EU**

**Карвацька С.Б., д.ю.н., професор,
в.о. завідувача кафедри міжнародного права
та порівняльного правознавства**

Чернівецький національний університет імені Юрія Федьковича

**Маник А.З., к.ю.н.,
асистент кафедри міжнародного права
та порівняльного правознавства**

Чернівецький національний університет імені Юрія Федьковича

**Лабик А.Р., асистент кафедри міжнародного права
та порівняльного правознавства**

Чернівецький національний університет імені Юрія Федьковича

У статті досліджено право на кібербезпеку, яка в умовах геополітичних загроз, військових конфліктів є критично важливим глобальним викликом сучасності, а нові геополітичні проблеми надають міжнародній взаємодії у сфері кібербезпеки додаткового імпульсу. Проаналізовано, що багаторівневий характер кібербезпеки як явища та однієї з найбільш швидкозростаючих сфер політики глобального управління даними можемо розуміти у контексті того, що заходи з її забезпечення достатньо, інколи діаметрально протилежно, відрізняються у різних країнах та регіонах, тому, як наслідок, країни ЄС все частіше почали приймати закони з питань кібербезпеки, розробляти ефективну політику кібербезпеки, а також більш відкрито брати участь у зовнішній політиці, пов'язаній з питаннями кібербезпеки – від торговельних угод до санкцій. Установлено, що в умовах військових конфліктів проблема здатності країн, передовсім, України, ефективно захищати свої інформаційні ресурси стає ключовим фактором для забезпечення національної безпеки та економічного розвитку. Зазначено, що військова агресія РФ проти України призвела до посилення трансатлантичної співпраці та координації з метою запобігання, виявлення та реагування на зловмисну кібердіяльність. Доведено, що в умовах збройного конфлікту кібербезпека являє собою основу національної безпеки України. Обґрунтовано, що на практиці, як ЄС, так і Україна практично зміщують акценти з кіберзлочинності на кібербезпеку, як це і відбувається загалом все частіше і на міжнародному рівні. Зроблено висновок, що глибоке усвідомлення змін у сучасному ландшафті кіберзагроз, необхідність забезпечення стійкості критичної інфраструктури, протистояння кібератакам зумовлюють необхідність, з однієї сторони, як нових законодавчих ініціатив, так з іншої сторони, – ефективної співпраці щодо протидії кіберзлочинності, захисту даних та партнерства приватним сектором у сфері кібербезпеки з метою підвищення кіберстійкості – країн ЄС, України, та загалом світу.

Ключові слова: право на кібербезпеку, кіберзагрози, інформаційна безпека, захист даних, кібербезпека в ЄС, кіберстійкість, засади забезпечення кібербезпеки України.

The article examines the right to cybersecurity, which, in the context of geopolitical threats and military conflicts, is a critical global challenge of our time, and new geopolitical issues give international cooperation in the field of cybersecurity an additional impetus. It is analysed that the multilevel nature of cybersecurity as a phenomenon and one of the fastest growing areas of global data governance policy can be understood in the context of the fact that measures to ensure it differ significantly, sometimes diametrically, in different countries and regions. Therefore, as a result, EU countries have increasingly begun to adopt laws on cybersecurity, develop effective cybersecurity policies, and participate more openly in foreign policy related to cybersecurity issues, from trade agreements to sanctions. The author establishes that the problem of the ability of countries, primarily Ukraine, to effectively protect their information resources in the context of military conflicts is becoming a key factor for ensuring national security and economic development. It is noted that the military aggression of the Russian Federation against Ukraine has led to the strengthening of transatlantic cooperation and coordination in order to prevent, detect and respond to malicious cyber activities. It is proved that in the context of armed conflict, cybersecurity is the basis of Ukraine's national security. It is substantiated that in practice, both the EU and Ukraine are practically shifting the focus from cybercrime to cybersecurity, as is happening more and more often at the international level. The author concludes that a deep awareness of changes in the modern landscape of cyber threats, the need to ensure the resilience of critical infrastructure, and countering cyber attacks necessitate, on the one hand, new legislative initiatives, and, on the other hand, effective cooperation in combating cybercrime, data protection, and private sector partnership in the field of cybersecurity with a view to enhancing cyber resilience – in the EU, Ukraine, and the world at large.

Key words: right to cybersecurity, cyber threats, information security, data protection, cybersecurity in the EU, cyber resilience, principles of cybersecurity in Ukraine.

Постановка проблеми. Кібербезпека є критично важливим глобальним викликом сучасності, а нові геополітичні проблеми надали міжнародній взаємодії у сфері кібербезпеки додаткового імпульсу.

Кібербезпека є міждисциплінарною проблематикою, адже включає не лише норми міжнародного публічного права, міжнародного приватного права, міжнародного комерційного права, правові норми ЄС, а й також норми національного (внутрішнього) права, у тому числі, норми конституційного права, цивільного права, господарського права, кримінального права, адміністративного права, що регулюють питання кібербезпеки. Разом з тим, очевидно, що право кібербезпеки сформувалося як повноцінна

самостійна галузь права. Після визнання нового основоположного права на кібербезпеку наступним кроком для фахівців є переосмислення, чи має формулювання цього права базуватися на традиційному підході до прав людини у загальному сенсі, чи бути похідним від основних прав людини, а також, для кого воно призначене – лише для державних суб'єктів і приватних осіб, чи для світового суспільства загалом [1].

За умов збройного конфлікту, кібербезпека являє собою основу національної безпеки України. Військова агресія РФ проти України призвела до посилення трансатлантичної співпраці та координації з метою запобігання, виявлення та реагування на зловмисну кібердіяльність.

Дослідники наводять спостереження, що в умовах збройних конфліктів «кібертаки є інструментом впливу, який також активно виступає елементом спеціальних розвідувальних операцій для маніпулювання населенням та дискредитації України як держави [2].

Стан дослідження. Окремі аспекти визначення поняття кібербезпеки та механізму міжнародно-правового урегулювання у своїх наукових роботах висвітлюють як вітчизняні науковці та практики, так і зарубіжні – І. Д. Бондаренко, Є. Ю. Колосовський, Е. М. Круць, В. П. Поліщук, Л. А. Панасевич, Д. О. Ширяєв, Кьяра П'єр Джорджо (Chiara Pier Giorgio), Діба Ааламі Харанді (Diba Aalami Harandi), Рокко Белланова (Rocco Bellanova), Хелен Каррапіко (Helena Carrapico), Деніс Дуес (Denis Duez), Лі А. Байгрейв (Lee A. Bygrave).

Втім, аналіз публікацій за темою дослідження свідчить про наявну наукову дискусію, яка характеризується відсутністю єдиного підходу щодо визначення ознак, які характеризують кібербезпеку, та, головне – шляхів розбудови кіберстійкості та захисту.

Метою статті є аналіз права на кібербезпеку, його змісту, проблем реалізації у контексті сучасних викликів та шляхів співпраці щодо протидії кіберзагрозам в Україні та ЄС.

Виклад основних положень. Цифровізація економіки збільшує не тільки її вразливість, але й також транскордонний вимір, що у свою чергу створює все більше викликів для законодавства та політики. Це пов'язано, передовсім, з тим, що цифровізація економіки створює нові ризики, оскільки іноземні уряди чи недержавні суб'єкти можуть отримати доступ до конфіденційної інформації, або спробувати порушити роботу критично важливих функцій чи інфраструктури.

Кібербезпека характеризується: «1) як система спеціальних суб'єктів, які забезпечують комп'ютерну безпеку; 2) як рівень захищеності електронних інформаційних ресурсів держави у кіберпросторі від ризиків зовнішнього впливу; 3) як система виявлення та протистояння різним формам зовнішнього втручання через інформаційні системи; 4) як система елементів комп'ютерної безпеки, які взаємодіють між собою з метою забезпечення безпеки інформаційно-телекомунікаційних систем; 5) як здатність держави запобігати та уникати спрямованого негативного впливу» [3].

Багаторівневий характер кібербезпеки як явища та однієї з найбільш швидкозростаючих сфер політики глобального управління даними можемо розуміти у контексті того, що заходи з її забезпечення достатньо, інколи діаметрально, відрізняються у різних країнах та регіонах. Як наслідок, країни ЄС все частіше почали приймати закони з питань кібербезпеки, розробляти ефективну політику кібербезпеки, а також більш відкрито брати участь у зовнішній політиці, пов'язаній з питаннями кібербезпеки – від торговельних угод до санкцій.

Кібербезпека зараз домінує у законодавстві ЄС, хоча і законодавство ЄС у сфері кібербезпеки є відносно новим. Першим правовим актом про інформаційну безпеку Європейського економічного співтовариства (сьогодні – ЄС) стало Рішення Ради 92/242/ЄЕС від 31 березня 1992 року про безпеку інформаційних систем [4] – документ, що установлював План дій для розробки «стратегічних рамок» у контексті «безпеки інформаційних систем». Протягом двох десятиліть ЄС доклав значних зусиль до законотворчості у сфері кібербезпеки, що завершилося прийняттям 17 квітня 2019 року Закону про кібербезпеку (офіційно відомий як Регламент (ЄС) 2019/881) у рамках ширшої стратегії ЄС щодо посилення кібербезпеки в усьому регіоні, який сформував основу, спрямовану на підвищення загального рівня кібербезпеки в ЄС [5]. Разом з тим, варто зауважити, що власне сама стратегія кібербезпеки ЄС щодо кіберпростору не дає чіткого визначення дефініції «кібербезпеки».

В останні роки він був доповнений політичною риторикою щодо забезпечення «цифрового суверенітету» ЄС по відношенню до потужних третіх країн, таких як США і Китай [6]. І хоча уявлення про «цифровий суверенітет» потребує уточнення, однак, воно свідчить про пріоритетність європейської самодостатності, що чітко узгоджується з регуляторними зусиллями, спрямованими на

посилення режиму кібербезпеки ЄС. Саму, власне, риторичу навколо цифрового суверенітету можна розглядати як прагнення ЄС до більшого контролю над цифровою «територією». Основний закон ЄС стверджує, що «національна безпека залишається виключною відповідальністю кожної держави-члена», при цьому залишає термін «національна безпека» невизначеним [7].

Відсутність прецедентного права, яке б точно інтерпретувало правові вимоги до кібербезпеки, означає, що вони залишаються недостатньо визначеними нормами. Безумовно, регуляторні органи починають робити систематичні спроби усунути цю проблему, але слід зазначити, що поки що існує лише два рішення Суду ЄС, які безпосередньо стосуються вимог Загального регламенту про захист даних (GDPR) щодо захисту інформації після злому даних. Перше рішення було винесено у грудні 2023 року [8], а друге – у вересні 2024 року, які стосувалися зобов'язань наглядових органів здійснювати свої коригувальні повноваження відповідно до Загального регламенту після витоку даних [9]. Очевидно, що ця сфера потребує більш авторитетних судових приписів щодо того, які з цих стандартів мають юридичний пріоритет, і як вони застосовуються у конкретних випадках [10].

У цих зусиллях Європейська декларація про цифрові права і принципи для цифрового десятиліття від 15 грудня 2022 року (далі – Декларація) є свідченням формування фактичного змісту нового основоположного права на кібербезпеку. Головною політичною метою Декларації є ідея про те, що цінності та основні права ЄС однаково застосовні як в офлайн, так і в цифровому середовищі: «те, що є незаконним в офлайн, є незаконним і в онлайн». Цей принцип, покладений в основу Закону про цифрові послуги, прямо визнає, наскільки важливою є сьогодні цифрова сфера у житті громадян, і підтверджує, наскільки розмитими є межі між «онлайн» і «офлайн» вимірами [1]. У 16-му принципі Декларації йдеться про наступне: «Кожен повинен мати доступ до цифрових технологій, продуктів і послуг, які за своєю конструкцією є безпечними, захищеними і такими, що захищають приватне життя, що забезпечує високий рівень конфіденційності, цілісності, доступності та автентичності оброблюваної інформації» [11].

Окремий аспект дослідження – це аналіз кроків щодо посилення кібербезпеки в ЄС. Нова Директива з кібербезпеки NIS 2 (щодо безпеки мережевих та інформаційних систем – the security of network and information systems), яка набула чинності 16 січня 2023 року запровадила обов'язкові заходи інформаційної безпеки та вимоги до звітності про інциденти інформаційної безпеки, за невиконання яких компанії у певних секторах будуть піддаватися значним штрафам. Нещодавно, наприкінці 2024 року ЄС розпочав процес ухвалення нового Закону про кіберстійкість (CRA) – акту, спрямованого на посилення безпеки підключених цифрових пристроїв, які допомагають формувати «Інтернет речей» (IoT) [12]. Закон про захист від кібернетичної активності (CRA), який набув чинності 10 грудня 2024 року, є останнім доповненням до багатьох попередніх нещодавніх законодавчих актів, що повністю або частково стосуються кібербезпеки. До прикладу, до них належать Закон про кібербезпеку (CA) [13], Закон про цифрову операційну стійкість (DORA) [14], Загальний регламент про захист даних (GDPR) [15], Директиви про мережеву та інформаційну безпеку (NISD і NIS2D) [16] та Директива про стійкість критично важливих об'єктів (CERD) [17].

Надзвичайно актуальним є сучасний стан кібербезпеки України, надто, глибоке розуміння важливості захисту кіберпростору в умовах збройного конфлікту. Національні основи нормативного регулювання протидії кіберзагрозам містяться у Законі України «Про основні засади забезпечення кібербезпеки України» [18]. Окрім цього, даним законодавчим актом було надано нормативне визначення понять «кіберзлочину», «кібератаки», «критичної та інформаційної інфраструктури» тощо. Також варто зазначити й низку підзаконних нормативних актів, які регулюють питання кібербезпеки, передовсім, Укази Президента України: «Про Стратегію національної безпеки України» [19], «Про Стратегію кібербезпеки України» [20], «Про Стратегію інформаційної безпеки» [21]. Відповідно до положень

ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», під терміном «кібербезпека» слід розуміти «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [18].

Кібербезпека, як відзначає Д. О. Ширяєв, є складною та багатогранною проблемою, яка вимагає спільних і постійних зусиль усіх зацікавлених сторін; працюючи разом над розробкою найкращих практик, обміном інформацією та інвестуванням у нові технології, ми зможемо краще захистити себе та свою цифрову інфраструктуру від кіберзагроз» [22, с. 602]. Але найбільшого ефекту, як зазначається у сучасних дослідженнях, можна досягти через взаємодію суб'єктів забезпечення кібербезпеки, зокрема, «шляхом застосування цілісних та ефективних системних механізмів, адміністративно-правових методик та різних методів, за допомогою яких реалізується державна політика в секторі забезпечення кібербезпеки, яких складових частин національної безпеки України [3].

На сьогодні, за умов збройного конфлікту, кібербезпека являє собою «основу національної безпеки України, яка складає стан захищеності країни, суспільства, системи публічного управління в кібернетичному просторі шляхом утворення легітимних механізмів забезпечення кібербезпеки публічного управління» [3]. Поліщук В. П. та Панасевич Л. А. обстоюють позицію, що «інформаційне протистояння здійснюється для впливу на масову свідомість, за допомогою спотворення реальності щодо наслідків конфронтації сторін, і результатом кіберконфлікту можуть бути політичні рішення глобального значення, що мають вагомий вплив на процес прийняття найважливіших у світі політичних рішень» [2].

Свідченням інтеграції зусиль із розбудови кіберстійкості та захисту є поступальний процес ефективної

співпраці щодо протидії кіберзлочинності. До прикладу, у серпні 2022 року між Україною та Польщею був підписаний Меморандум про співпрацю у сфері кіберзахисту [23]. Важливим підсумком третього раунду Кібердіалогу між Україною та ЄС, який відбувся 15 липня 2024 року у Брюсселі, є інноваційна програма «Soft Power», яка має об'єднати «провідних інженерів, розробників та програмістів з приватного сектору та університетів України та країн-партнерів для створення передових рішень для безпілотних систем» [24]. Учасники не тільки дійшли згоди щодо плану дій та очікуваних результатів до проведення четвертого раунду Кібердіалогу у 2025 році, а й висловили сподівання щодо створення можливостей для співпраці з ЄС у кіберсфері, зокрема, через ІТ-коаліцію.

Висновки. Проблема здатності країн, передовсім, України ефективно захищати свої інформаційні ресурси стає ключовим фактором для забезпечення національної безпеки та економічного розвитку. В умовах збройного конфлікту кібербезпека являє собою основу національної безпеки України. І тому надважливим є досягнення консенсусу різних країн з конкретних питань кіберзахисту, що є ускладненим через різні національні інтереси та погляди на цифровий суверенітет, кібербезпеку та роль державного контролю над інформаційно-комунікаційними технологіями (ІКЕ).

На практиці, як ЄС, так і Україна практично зміщують акценти з кіберзлочинності на кібербезпеку, як це і відбувається загалом все частіше і на міжнародному рівні. Глибоке усвідомлення змін у сучасному ландшафті кіберзагроз, необхідність забезпечення стійкості критичної інфраструктури, протистояння кібератакам зумовлюють необхідність, з однієї сторони, як нових законодавчих ініціатив, так з іншої сторони, – ефективної співпраці щодо протидії кіберзлочинності, захисту даних та партнерства приватним сектором у сфері кібербезпеки з метою підвищення кіберстійкості – країн ЄС, України, та загалом світу.

ЛІТЕРАТУРА

- Chiara Pier Giorgio. Towards a right to cybersecurity in EU law? *Computer Law & Security Review*. 2024. Volume 53. URL: <https://www.sciencedirect.com/science/article/pii/S0267364924000281>
- 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.
- Колосовський Є. Ю., Круць Е. М. Сучасний стан кібербезпеки України в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. № 12. С. 402-405. URL: http://lsej.org.ua/12_2023/100.pdf
- Council Decision of 31 March 1992 in the field of security of information (92/242/EEC) URL: <https://www.legislation.gov.uk/eudn/1992/242/adopted>
- Harandi Diba Aalami. International Legal Frameworks on Cybersecurity and Data Protection. La January 7, 2025. URL: <https://djlpl.org/international-legal-frameworks-on-cybersecurity-and-data-protection-law/>
- Bellanova Rocco, Carrapico Helena and Duez Denis. Digital/sovereignty and European security integration: an introduction. *European Security*. 2022. № 31(3). URL: <https://doi.org/10.1080/09662839.2022.2101887>
- Consolidated version of The treaty on European Union. *Official Journal of the European Union*. C 326/13. 26.10.2012. URL: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF
- ECJ:EU. Case C-340/21. VB v. Natsionalna agentsia za prihodite, judgment of 14 December 2023.
- ECJ:EU. Case C 768/21. TR v. Land Hessen, judgment of 26 September 2024.
- Lee A. Bygrave. The emergence of EU cybersecurity law: A tale of lemons, angst, surf and grey boxes. *Computer Law & Security Review*. 2025. Volume 56, URL: <https://doi.org/10.1016/j.clsr.2024.106071> <https://www.sciencedirect.com/science/article/pii/S0267364924001377>
- EU Declaration on Digital Rights and Principles recital 3. URL: <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>
- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 (Cyber Resilience Act). URL: <https://www.european-cyber-resilience-act.com/>
- Regulation (EU) 2019/881.
- Regulation (EU) 2022/2554.
- Regulation (EU) 2016/679.
- Directive (EU) 2016/1148.
- Directive (EU) 2022/2557.
- Про основні засади забезпечення кібербезпеки України. Закон України. *Відомості Верховної Ради (ВВР)*. 2017. № 45, ст.403 URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
- Указ Президента України «Про Стратегію національної безпеки України» від 14.09.2020 р. № 392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037>
- Указ Президента України «Про Стратегію кібербезпеки України» від 26.08.2021 р. № 447/2021. URL: <https://www.president.gov.ua/documents/4472021-40013>
- Указ Президента України «Про Стратегію інформаційної безпеки» від 28.12.2021 р. URL: <https://www.president.gov.ua/documents/6852021-41069>
- Ширяєв Д.О. Кібербезпека та сучасний світ. *Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів*. Вінниця, 2023. С. 600–602.
- Уряди України та Польщі підписали меморандум про співпрацю у сфері кіберзахисту. URL: <https://thedigital.gov.ua/news/uryadi-ukraini-ta-polshchi-pidpisali-memorandum-pro-spiivpratsyu-u-sferi-kiberzakhistu>
- Заступниця міністра оборони Катерина Черногоренко за підсумками третього раунду Кібердіалогу між Україною та ЄС про поглиблення співпраці з партнерами у сфері кібербезпеки. URL: <https://www.ukrinform.ua/rubric-society/3887837-ukraina-ta-evrosouz-pogliblat-spiivpracu-u-sferi-kiberbezpeki-minoboroni.html>