https://doi.org/10.26565/2075-1834-2025-39-06
УДК 004.056

О.С. ПЕРЕДЕРІЙ
кандидат юридичних наук, доцент,
доцент кафедри державно-правових дисциплін
E-mail: perederii@karazin.ua ORCID: https://orcid.org/0000-0003-4898-876X
Харківський національний університет імені В. Н. Каразіна
м. Харків, 61022, майдан Свободи 4

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ПРОТИДІЇ ЗАГРОРЗАМ КІБЕРБЕЗПЕКИ В АСПЕКТІ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ УКРАЇНИ

АНОТАЦІЯ. *Вступ.* У статті обґрунтовано викладено важливість дослідження проблематики забезпечення безпеки національного кібернетичного простору. Висвітлено зміст основних організаційно-правових засад протидії загрозам кібербезпеки в сучасній Україні.

Короткий зміст основних результатів дослідження. На основі аналізу чинного законодавства України про забезпечення безпеки кіберпростору, а також узагальнення положень документів Ради національної безпеки і оборони України з питань кібербезпеки виокремлено основні загрози національному кіберпростору. Зокрема, це постійні агресія Російської Федерації проти України у кіберпросторі, зростання рівня кіберзлочинності, кібершпигунство, розвідувально-підривна діяльність, використання терористичними організаціями кіберпростору для вчинення актів кібертероризму.

Викладено авторський варіант систематизації управлінсько-правових засад протидії загрозам кібербезпеки в Україні: формування цілісної інституційної системи протидії загрозам кібербезпеки на чолі з РНБО, впровадження конкретних форм реагування на кіберзагрози (заходи кібероборони України, забезпечення безперервного здійснення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав в кіберпросторі, застосування економічних, дипломатичних, розвідувальних заходів, залучення потенціалу приватного сектору), постійний розвиток активної політики співробітництва з Європейським Союзом задля розробки і впровадження спільних дій, спрямованих на протидію кіберзагрозам.

Висновок. Узагальнено викладено висновок про те, що сучасна Україна сформувала систему організаційно-правових засад попередження і протидії кіберзагрозам, які постають перед національним інформаційним середовищем. Задля моніторингу рівня їх ефективності запропоновано поглибити об'єднання зусиль представники юридичної науки, експертного середовища, працівників органів управління, Сектору безпеки і оборони задля оперативного вироблення спільних дієвих підходів до відвернення кіберзагроз.

КЛЮЧОВІ СЛОВА: *Україна, кібербезпека, кіберзлочинність, європейська інтеграція, правова система, національна безпека, Європейський Союз, європейська кібербезпека.*

Як цитувати: Передерій О.С. Організаційно-правові засади протидії загрозам кібербезпеки в аспекті європейської інтеграції України. *Вісник Харківського національного університету імені В. Н. Каразіна, серія «Право».* 2025. Вип. 39. С. 70-74. https://doi.org/10.26565/2075-1834-2025-39-06

In cites: O. S. Perederii (2025) Organizational and legal principles of countering cyber security threats in the aspect of Ukraine's European integration.. *The Journal of V.N. Karazin Kharkiv National University, Series "Law"*, (39), P. 70-74. https://doi.org/10.26565/2075-1834-2025-39-06 (in Ukrainian)

Постановка проблеми. У сучасному світі питання, які пов'язані із убезпеченням кіберпростору від загроз і ризиків набули першочергової актуальності для самого широкого кола суб'єктів.

Усі, починаючи з приватних користувачів побутових гаджетів та фрілансерів і закінчуючи державами, міжнародними організаціями і транснаціональними корпораціями зацікавлені в існування ефективної системи попередження і реагування на порушення сталого режиму функціонування цифрового простору. Відповідно, зазначені питання постійно перебувають у центрі уваги на самому найвищому політичному рівні. Теза з виступу Генерального секретаря ООН на дебатах високого рівня у Раді Безпеки ООН у червні 2024 р. про те, що небезпека використання цифрових технологій як зброї збільшується з кожним роком є як ніколи значущою [1].

Реалії сьогоднішнього дня характеризуються зростанням кількості незаконних посягань на кібербезпеку у кожній державі світу. Так, лише в Україні в останні роки кількість виявлених кіберзлочинів збільшується в середньому на 2,5 тисячі в рік [2, с. 59].

Для України, як і для інших держав світу, забезпечення кібербезпеки і протидія кіберзлочинності в сучасних умовах є надзвичайно важливим завданням. Прикладний аспект цьому надають прямі юридичні зобов'язання перед Європейським Союзом (далі – ЄС) щодо удосконалення державної політики у сфері юстиції, свободи і безпеки. Так, у ст. 22 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (далі – Угода про асоціацію) визначено, що протидія кіберзлочинності є одним із ключових форматів посилення двостороннього, регіонального та міжнародного співробітництва України і ЄС [3]. Відповідно, розбудова ефективної національної організаційно-правової системи протидії загрозам кібербезпеки є конкретною передумовою прискорення входження України у склад ЄС. В зазначеному аспекті, актуальним науково-практичним завданням для вітчизняної юридичної науки є наукова розробка організаційно-правових засад протидії загрозам кібербезпеки і захист національного цифрового середовища.

Стан наукового дослідження теми. Питання щодо організаційно-правових засад протидії загрозам кібербезпеки України у вітчизняній теоретичній юриспруденції потрапляло у центр уваги вітчизняних правників у різних конотаціях. Проте, наукова розробка питань забезпечення кібербезпеки в аспекті європейської інтеграції України є незначною. Інформаційним базисом для сформульованих у статті ідей і позицій стали положення нормативних актів про кібербезпеку, а також окремі наукові позиції таких вчених як Н. Лесько, А. Кириченко, С. Кіра, Ю. Онищенко, М. Сироватченко, та ін.

Метою дослідження є висвітлення організаційно-правових засад протидії загрозам кібербезпеки як умови прискорення процесів інтеграції Україні до ЄС.

Основні результати дослідження. Експертне середовище одностайне у тому, що Україна на сучасному етапі історії перебуває на передовій самої технологічної в історії нашої цивілізації кібервійни. Незважаючи на те, що постійні кібератаки агресора на державні органи України завдають значних збитків, а також акції з цілеспрямованої дезінформації українського суспільства негативно впливають на наше життя, їх можна використати для тестування нових ідей та технологій у галузі захисту інформації [4]. Поряд із пошуком технічних інновацій забезпечення кібербезпеки України, набутий досвід спонукає також і правників формувати новітній ідейний базис для оновлення юридичної основи кіберзахисту національних інтересів. Це надає певного імпульсу правотворчим інституціям.

Станом на теперішній час, у правовій системі України кібербезпека є окремим правовим інститутом, який забезпечений значним переліком нормативних конструкцій. Слід відзначити, що цілеспрямована політика із правового забезпечення політики кібербезпеки в Україні розпочалася у 2016 р., коли Рада національної безпеки і оборони України (далі – РНБО) уперше ухвалила Стратегію кібербезпеки, яка буда затверджена Указом Президента України від 15 березня 2016 року № 96 [5]. Реалізація стратегії мала свої позитивні результати. Зокрема, було оновлено нормативно-правову базу із забезпечення кібербезпеки, створено при РНБО Національний координаційний центр кібербезпеки, який розробляє найбільш актуальні рішення з питань кібербезпеки, налагодилася системна міжнародна співпраця з цих питань.

На виконання Стратегії було прийнято спеціалізований закон, який урегулював зазначений інститут. Так, у відповідності до Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII кібербезпека визначається як 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 [6]. Основою змісту забезпечення кібербезпеки у відповідності до згаданого закону є комплексна протидія кіберзагрозам, тобто наявним або потенційно можливим явищам і чинникам, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан інфраструктури об'єктів кібербезпеки.

Разом із тим, станом на 2021 р. стало очевидним, що Стратегія кібербезпеки 2016 р. потребувала оновлення через низку соціальних, організаційних, технічних і політико-правових причин. Зокрема – документ зразка 2016 р. не враховував положення прийнятої у грудні 2020 р. Стратегії кібербезпеки ЄС на цифрове десятиліття (далі – Стратегія на десятиліття) [7]. Так, ЄС у Стратегії десятиліття, на основі комплексного прогнозування, визначив кілька найбільш небезпечних загроз кібербез-

пеці та магістральних заходів протидії ним. Базовою засадою зазначеного документа є те, що «кібербезпека є невід'ємною частиною безпеки європейців» і громадяни держав-членів ЄС мають право на гарантії захисту від кіберзагроз. Покращення кібербезпеки є надзвичайно важливим для забезпечення довіри людей у ЄС до інновацій, взаємозв'язку та автоматизації, отримання вигід від них, а також для захисту основних прав і свобод, зокрема права на приватність та захист персональних даних, а також свободу вираження поглядів та інформації. Саме зазначені положення можна вважати визначальним для України з огляду на інтеграцію України до правового простору ЄС в цілому і приведення концепції національної державної політики у відповідність до загальноєвропейських правових нормативів у зазначеній сфері. Через це у серпні 2021 р. Указом Президента України було введено у дію нову Стратегію кібербезпеки України [8].

Стратегія кібербезпеки України визначає діяння, які визначаються як загрози кібербезпеці України:

— постійні агресія Російської Федерації проти України у кіберпросторі (Росія невпинно нарощує арсенал кіберзброї наступального призначення, постійно здійснює кібердиверсії на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу, отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності, реалізує спеціальні інформаційні операції з метою маніпулятивного впливу на населення, втручання у політичні процеси та дискредитації української державності);

— кіберзлочинність (поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей);

— організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності (являють собою продовжувані у часі тривалі дії, що ускладнює їх попередження, виявлення та нейтралізацію);

— використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності.

Відзначимо, що зазначені загрози сформульовані РНБО України на основі європейської Стратегії десятиліття. Це забезпечує досягнення загальноєвропейського колективного ситуативного усвідомлення кіберзагроз. Прикметною особливістю Стратегії кібербезпеки 2021 р. є визначення основних управлінсько-правових засад протидії загрозам кібербезпеки. Узагальнюючи основні положення документу, виокремимо базові з них.

Так, першою засадою є формування цілісної інституційної системи протидії загрозам кібербезпеки. Так, реалізація Стратегії безпосередньо здійснюється Національним координаційним центром кібербезпеки РНБО, основними суб'єктами забезпечення національної системи кібербезпеки, Міністерством закордонних справ України, Міністерством цифрової трансформації України, Міністерством освіти і науки України та іншими суб'єктами забезпечення кібербезпеки в межах їх компетенції. Діяльність зазначеної системи органів здійснюється під координацією Президента України та РНБО. Саме РНБО здійснює розроблення планових заходів, які необхідні для забезпечення національних інтересів у сфері кібербезпеки, захисті інформаційної національної інфраструктури. У зазначеному контексті слід погодитися з деякими науковцями, які РНБО у питаннях забезпечення кібербезпеки відводять роль координаційного і інформаційно-аналітичного хабу у системі органів державної влади [9, с. 318].

Другою засадою є формування на управлінському рівні конкретних форм реагування на кіберзагрози. Зокрема, це забезпечення дієвої кібероборони України (кадровий і технологічний розвиток підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі, регулярне вдосконалення зазначених структур), забезпечення безперервного здійснення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав, забезпечення набуття правоохоронними органами та державним органом спеціального призначення з правоохоронними функціями спроможностей для мінімізації загроз кіберзлочинності, посилення їх технологічного і кадрового потенціалу для проведення превентивних заходів та розслідування кіберзлочинів,

розвиток асиметричних інструментів стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу приватного сектору. Так, сьогодні у системі Збройних Сил України функціонують кібервійська і, як справедливо зазначає Н. Лесько, такі підрозділи постійно перебувають на етапі формалізації у правовому полі та складаються як із самоорганізованих добровольців, так і представників різних держорганів [10, с. 225].

Третьою засадою є проведення і постійний розвиток активної політики співробітництва з Європейським Союзом задля розробки і впровадження спільних дій, спрямованих на протидію кіберзагрозам. Так, розділ 7 Стратегії кібербезпеки 2021 р. передбачає необхідність поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС, вжиття узгоджених з європейськими партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі. У період 2022-2025 рр. Україна зробила колосальний крок уперед в аспекті поглиблення міжнародного співробітництва не лише з ЄС, а й з іншими стратегічними партнерами держави включаючи зарубіжні країни і військово-політичні блоки (НАТО).

Висновки. Україна станом на 2025 р. сформувала систему організаційно-правових засад попередження і протидії кіберзагрозам, які постають перед національним інформаційним середовищем. Представники юридичної науки, експертне середовище, працівники органів управління та, зокрема, Сектору безпеки і оборони, мають постійно тримати діалог задля оперативного вироблення спільних дієвих підходів до відвернення кіберзагроз. Від цього безпосередньо залежить ефективність національної економіки, динаміка гуманітарних процесів у суспільстві, стан правопорядку у державі та рівень захисту прав і свобод особи. Лише за таких умов Україна розширюватиме вікно можливостей для входження у загальноєвропейський цифровий простір з метою набуття членства у ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Небезпека використання цифрових технологій як зброї зростає – Генсек ООН: повідомлення від 20.06.2024 р. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-world/3877104-nebezpeka-vikoristanna-cifrovih-tehnologij-ak-zbroi-zrostae-gensek-oon.html (дата звернення: 02.04.2025)

2. Онищенко Ю., Герасимюк В. Проблеми забезпечення кібербезпеки як складової публічної безпеки. URL:chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/15.pdf (дата звернення: 01.04.2025)

3. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09. 2014 р. № 1678-VII. Відомості Верховної Ради України. 2014 р. № 40. Стаття 2021

4. Кириченко А. Кібербезпека в Україні: шляхи розвитку та можливості: 03.05.2023 р. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html (дата звернення: 02.04.2025)

5. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 року № 96/2016. Офіційний вісник Президента України. 2016. № 10. Ст. 198

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIIIВідомості Верховної Ради. 2017. № 45. Ст. 403

7. The EU's Cybersecurity Strategy for the Digital Decade. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164 (дата звернення: 01.04.2025)

8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. *Офіційний вісник України*. 2021. № 70. Ст. 4417

9. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки».* Т. 11. № 1(41). С. 314-320.

10. Лесько Н. В., Кіра С. О. Кібербезпека як частина національної безпеки України в умовах війни. *Юридичний електронний науковий журнал.* 2023. № 5. С. 224-226. URL: https://doi.org/10.32782/2524-0374/2023-5/55 (дата звернення: 29.03.2025)

Стаття надійшла до редакції 15.03.2025
Стаття рекомендована до друку 17.05.2025

O.S. PEREDERII
PhD (Law), associate professor,
Associate Professor of the Department of State and Legal Disciplines
E-mail: perederii@karazin.ua ORCID: https://orcid.org/0000-0003-4898-876X
V.N. Karazin Kharkov National University
Kharkiv, 61022, Svobody squere, 4

ORGANIZATIONAL AND LEGAL PRINCIPLES OF COUNTERING CYBER SECURITY THREATS IN THE ASPECT OF UKRAINE'S EUROPEAN INTEGRATION.

ANNOTATION. *Introduction.* The article substantiates the importance of studying the issues of ensuring the security of the national cyberspace. The content of the main organizational and legal principles of countering cyber security threats in modern Ukraine is highlighted.

Summary of the main results of the study. Based on the analysis of the current legislation of Ukraine on ensuring the security of cyberspace, as well as a generalization of the provisions of the documents of the National Security and Defense Council of Ukraine on cybersecurity, the main threats to national cyberspace are identified. In particular, these are the constant aggression of the Russian Federation against Ukraine in cyberspace, the growth of the level of cybercrime, cyber espionage, intelligence and subversive activities, and the use of cyberspace by terrorist organizations to commit acts of cyberterrorism.

The author's version of the systematization of the administrative and legal principles of countering cybersecurity threats in Ukraine is presented: the formation of a holistic institutional system for countering cybersecurity threats led by the National Security and Defense Council, the implementation of specific forms of response to cyber threats (cyber defense measures of Ukraine, ensuring the continuous implementation of counterintelligence measures to detect, prevent and terminate intelligence and subversive activities of foreign states in cyberspace, the use of economic, diplomatic, intelligence measures, and the involvement of the potential of the private sector), the constant development of an active policy of cooperation with the European Union to develop and implement joint actions aimed at countering cyber threats.

The provisions of the EU Cybersecurity Strategy for 2020-2030 are analyzed in terms of borrowing its provisions into regulatory documents on the prevention of cyber threats at the national level.

Conclusion. The conclusion is summarized that modern Ukraine has formed a system of organizational and legal principles for preventing and countering cyber threats that face the national information environment. In order to monitor the level of their effectiveness, it is proposed to deepen the joint efforts of representatives of legal science, the expert community, employees of government bodies, the Security and Defense Sector in order to promptly develop joint effective approaches to preventing cyber threats.

KEY WORDS: *Ukraine, cybersecurity, cybercrime, European integration, legal system, national security, European Union, European cybersecurity.*

REFERENCES

1. The danger of using digital technologies as weapons is growing - UN Secretary General: message dated 06/20/2024. *Ukrinform*. URL: https://www.ukrinform.ua/rubric-world/3877104-nebezpeka-vikoristanna-cifrovih-tehnologij-ak-zbroi-zrostae-gensek-oon.html (date of access: 02.04.2025) (in Ukrainian)

2. Onyshchenko Yu., Herasymiuk V. Problems of ensuring cybersecurity as a component of public security. URL:chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/15.pdf (data zvernennia: 01.04.2025) (in Ukrainian)

3. On the ratification of the Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their Member States, on the other hand: Law of Ukraine dated 16.09. 2014 No. 1678-VII. *Bulletin of the Verkhovna Rada of Ukraine*. 2014. № 40. Art. 2021 (in Ukrainian)

4. Kyrychenko A. Cybersecurity in Ukraine: development paths and opportunities: 03.05.2023 r. *Ukrinform.* URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html (date of access: 02.04.2025) (in Ukrainian)

5. On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine. 2016. March 15. No. 96/2016. *Official Gazette of the President of Ukraine.* 2016. No. 10. Art. 198 (in Ukrainian)

6. On the basic principles of ensuring cybersecurity in Ukraine: Law of Ukraine dated October 5, 2017 No. 2163-VIII. *Bulletin of the Verkhovna Rada of Ukraine*. 2017. No. 45. Art. 403 (in Ukrainian)

7. The EU's Cybersecurity Strategy for the Digital Decade. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164 (date of access: 01.04.2025) (in Ukrainian)

8. On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 “On the Cybersecurity Strategy of Ukraine”: Decree of the President of Ukraine dated August 26, 2021 No. 447/2021. Official Gazette of Ukraine. 2021. No. 70. Art. 4417 (in Ukrainian)

9. Syrovatchenko M. Legal aspects of ensuring cybersecurity in Ukraine: modern challenges and the role of national legislation. *Bulletin of the National University "Lviv Polytechnic". Series: "Legal Sciences".* Vol. 11. No. 1(41). P. 314-320. (in Ukrainian)

10. Lesko N. V., Kira S. O. Cybersecurity as a part of the national security of Ukraine in times of war. *Legal Electronic Scientific Journal.* 2023. No. 5. P. 224-226. URL: https://doi.org/10.32782/2524-0374/2023-5/55 (date of access: 29.03.2025) (in Ukrainian)

The article was received by the editors 15.03.2025
The article is recommended for printing 17.05.2025