УДК 341.1/.8
DOI https://doi.org/10.32782/2524-0374/2024-11/139

ТЕНДЕНЦІЇ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ КІБЕРБЕЗПЕКИ

TRENDS IN INTERNATIONAL COOPERATION IN THE FIELD OF CYBERSECURITY

Вареник О.С., д.ю.н.,
професор кафедри міжнародного та європейського права
факультету міжнародних відносин
Національний авіаційний університет

У статті здійснено комплексний аналіз сучасних тенденцій міжнародного співробітництва у сфері кібербезпеки, що набуває стратегічного значення в умовах глобальної цифровізації та загострення кіберзагроз. Здійснено загальнотеоретичну характеристику кожної з них. Наведено позиції науковців у досліджуваній царині та деталізовано специфіку кожної із них. У результаті проведеного дослідження підсумовано, що міжнародне співробітництво у сфері кібербезпеки є критично важливим елементом сучасної системи глобальної безпеки, оскільки кіберзагрози мають транснаціональний характер і можуть безпосередньо впливати на політичну, економічну та соціальну стабільність держав. Відсутність єдиної міжнародно-правової бази у цій сфері, фрагментарність регулювання та різні підходи до кіберзахисту в різних країнах світу суттєво ускладнюють координацію зусиль для ефективного протистояння кіберзлочинності, державним кіберзагрозам та використанню кібератак у гібридних війнах. Наголошено на наявності системних проблем, зокрема фрагментарності політики кіберзахисту, відсутності належної координації між державами-партнерами, а також неефективного використання міжнародної технічної допомоги. Україна, як держава, що активно інтегрується в європейський та євроатлантичний безпековий простір, отримує значну технічну підтримку від міжнародних партнерів, зокрема НАТО, Європейського Союзу, США, Великобританії та Канади, спрямовану на посилення її кіберстійкості. Однак, проблемою залишається питання нераціонального використання програмних та апаратних засобів кіберзахисту, що надаються в межах міжнародної технічної допомоги. Зроблено висновок, що міжнародне співробітництво у сфері кібербезпеки є критично важливим елементом сучасної системи глобальної безпеки, оскільки кіберзагрози мають транснаціональний характер і можуть безпосередньо впливати на політичну, економічну та соціальну стабільність держав. Відсутність єдиної міжнародно-правової бази у цій сфері, фрагментарність регулювання та різні підходи до кіберзахисту в різних країнах світу суттєво ускладнюють координацію зусиль для ефективного протистояння кіберзлочинності, державним кіберзагрозам та використанню кібератак у гібридних війнах.

Ключові слова: тенденції, кібербезпека, міжнародна безпека, кіберзлочинність, міжнародне співробітництво, правове регулювання.

The article provides a comprehensive analysis of current trends in international cooperation in the field of cybersecurity, which is gaining strategic importance in the context of global digitalization and the aggravation of cyber threats. A general theoretical description of each of them is provided. The positions of scientists in the field under study are presented and the specifics of each of them are detailed. As a result of the study, it is concluded that international cooperation in the field of cybersecurity is a critically important element of the modern global security system, since cyber threats are transnational in nature and can directly affect the political, economic and social stability of states. The lack of a single international legal framework in this area, the fragmentation of regulation and different approaches to cyber protection in different countries of the world significantly complicate the coordination of efforts to effectively combat cybercrime, state cyber threats and the use of cyber attacks in hybrid wars. The authors emphasize the existence of systemic problems, in particular, the fragmentation of cyber defense policy, the lack of proper coordination between partner states, as well as the ineffective use of international technical assistance. Ukraine, as a state actively integrating into the European and Euro-Atlantic security space, receives significant technical support from international partners, in particular NATO, the European Union, the United States, the United Kingdom and Canada, aimed at strengthening its cyber resilience. However, the issue of irrational use of cyber defense software and hardware provided within the framework of international technical assistance remains a problem. It is concluded that international cooperation in the field of cybersecurity is a critically important element of the modern global security system, since cyber threats are transnational in nature and can directly affect the political, economic and social stability of states. The lack of a unified international legal framework in this area, fragmented regulation, and different approaches to cyber defense in different countries of the world significantly complicate the coordination of efforts to effectively combat cybercrime, state cyber threats, and the use of cyberattacks in hybrid wars.

Key words: trends, cybersecurity, international security, cybercrime, international cooperation, legal regulation.

Постановка проблеми. Україна, як повноправний суб'єкт міжнародного права, бере активну участь у глобальній системі кібербезпеки, що є невід'ємним компонентом архітектури міжнародної безпеки в сучасному світі. У сучасних умовах, коли кібератаки стають одним із ключових інструментів гібридної війни, особливо з боку держав-агресорів, таких як російська федерація, критично важливим є розширення міжнародного партнерства у сфері забезпечення кіберстійкості.

У сучасних умовах глобальної цифрової трансформації кібербезпека набула стратегічного значення, ставши одним із ключових аспектів забезпечення міжнародної та національної безпеки. Інформаційні технології, штучний інтелект, великі дані, квантові обчислення та інші цифрові інновації кардинально змінюють структуру економічних, соціальних та політичних процесів, сприяючи підвищенню ефективності управління, міжнародного співробітництва та економічного розвитку. У зв'язку з тим, що терористичні організації дедалі частіше використовують кіберпростір для здійснення атак на державні інституції, фінансові системи та стратегічні об'єкти, міжнародна спільнота активізує заходи для протидії кібертероризму.

Україна, як держава, що систематично зазнає цілеспрямованих кібератак у межах гібридної війни, посідає важливе місце у глобальній архітектурі кібербезпеки. Масштабні та комплексні атаки на критично важливу інфраструктуру, фінансовий сектор, державні реєстри та комунікаційні системи обумовили необхідність посилення національного кіберзахисту та активного залучення України до міжнародних механізмів співробітництва. У відповідь на ці виклики було здійснено стратегічні кроки щодо інтеграції у глобальні ініціативи з кібербезпеки, зокрема шляхом участі у Трастовому фонді НАТО з кібербезпеки, залучення до програм Європейського Союзу з цифрової безпеки, а також налагодження тісної взаємодії з провідними міжнародними суб'єктами у цій сфері, зокрема США, Великобританією, Канадою та іншими стратегічними партнерами. У цьому контексті дослідження тенденцій міжнародного співробітництва у сфері кібербезпеки є особливо актуальним не лише для забезпечення кіберстійкості нашої держави, але й для розвитку ефективних глобальних механізмів цифрової безпеки, що сприятиме зміцненню міжнародного кіберпростору.

Стан дослідження. У тій чи іншій мірі проблематики тенденцій міжнародного співробітництва у сфері

кібербезпеки розглядали ряд вчених серед яких доцільно назвати таких: О.Є. Архіпова, П.Д. Біленчук, М.В. Бєлова, В.В. Бут, С.А. Буяджи, М.В. Гребенюк, О.О. Грицун, С.В. Демедюк, Н.А. Зелінська, Н.В. Карчевський, А.А. Коваленко, М.В. Копійка, М.М. Кравчук, В. А. Ліпкан, Р. В. Лук'янчук, А.І. Марущак, Н.В. Савчук, Є.Д. Скулиш, М.С. Тєтєвін, Ю.С. Шемшученко та ін. Тим не менш, не применшуючи наукового доробку вказаних авторів, доцільно відзначити, що проблема деталізації тенденцій міжнародного співробітництва у сфері кібербезпеки набуває все більшої актуальності у зв'язку з інтенсивним науково-технічним прогресом та політичною дестабілізацією у світі загалом.

Метою статті є загальнотеоретична характеристика тенденцій міжнародного співробітництва у сфері кібербезпеки.

Виклад основного матеріалу. У сучасному цифровому світі кібербезпека стала однією з найбільш актуальних проблем, оскільки зростання кількості підключених пристроїв призвело до збільшення кіберзагроз, які становлять серйозний ризик для національної та міжнародної безпеки. У цьому контексті співпраця між країнами стає надзвичайно важливою для захисту суверенітету та забезпечення кібербезпеки на глобальному рівні. Україна, яка має багатий досвід у протистоянні з кіберзагрозами, активно приймає участь у міжнародних ініціативах та співпраці в цій галузі [1, с. 263]. Україна виступає не лише як об'єкт кібератак, а й як активний суб'єкт міжнародної кіберспільноти, що розробляє та впроваджує сучасні механізми колективної безпеки.

Так, Україна є повноцінним членом глобальної системи безпеки, пріоритетами для якої залишаються розвиток міжнародного партнерства й співробітництва у сфері забезпечення кібербезпеки, підтримка міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглиблення тісної співпраці України з НАТО з метою підвищення спроможностей України у сфері забезпечення кібербезпеки, участь у заходах зі зміцнення довіри в кіберпросторі тощо. Україна відповідно до укладених нею міжнародних договорів проводить виважену державну політику у сфері вдосконалення співробітництва у сфері кібербезпеки. Враховуючи глобальну цифровізацію, зростання обсягів транснаціональної кіберзлочинності, загрозливі тенденції динамічного поширення кіберзагроз у світовому масштабі для України актуальним вбачається уточнення напрямків подальшого міжнародного співробітництва щодо посилення спроможностей України у сфері забезпечення кібербезпеки [2, с. 130].

Важливим аспектом міжнародного співробітництва у сфері кібербезпеки є формування ефективної системи колективного стримування кіберзагроз, що передбачає не лише оперативне реагування на атаки, а й запровадження механізмів запобігання кіберагресії на основі міжнародного права. В умовах гібридних війн, що дедалі частіше включають кібернетичні операції, особливої актуальності набуває розробка універсальних міжнародно-правових стандартів, які б регулювали питання відповідальності за використання кіберпростору у воєнних, інформаційних та економічних конфліктах.

Як відмічає Т. В. Станіславський, сьогоднішній стан міжнародного співробітництва у сфері кібербезпеки характеризує відсутність дієвої державної політики в організації міжнародної взаємодії у сфері забезпеченні кібербезпеки; неефективне, некоординоване, неконтрольоване та не обліковане використання отриманих в рамках міжнародної, в тому числі, технічної допомоги в програмного та апаратного забезпечення для підвищення рівня їх кіберзахисту; недостатньо відповідальне ставлення з боку бенефіціарів до отриманих у рамках технічної допомоги програмних та апаратних засобів кіберзахисту, негативно впливає на її міжнародний імідж та інвестиційну привабливості, а також втрати спроможностей України у динамічному впровадженні цифрових технологій [3, с. 65].

Сучасні інформаційні загрози підкреслюють нагальну потребу у співпраці між державами для попередження постійних загроз в інтернеті, забезпечення кращого розслідування, затримання і переслідування зловмисних агентів, подолання проблем кібербезпеки, адже сучасні суспільства глобально взаємопов'язані, а кібератаки можуть призвести до значних економічних і соціальних збитків. Саме тому, як вдало зазначає О.Г. Трофименко, міжнародні зусилля у посиленні кібербезпеки та захисту критично важливих інформаційних інфраструктур мають бути узгоджені та діяти у відповідь на ці нові тенденції в глобальному русі до цифрової економіки та інформаційного суспільства [4, с. 154].

Відсутність єдиного правового підходу до протидії кіберзлочинності, розбіжності у визначеннях правопорушень у кіберпросторі та відмінності в законодавчих підходах різних держав значно ускладнюють процес гармонізації правозастосовної практики [5, с. 491]. Зокрема, у зв'язку з інтенсивним науково-технічним прогресом за останні два десятиліття, на міжнародному рівні триває дискусія щодо необхідності розробки нової універсальної правової рамки для боротьби з кіберзагрозами, яка могла б ефективно доповнити положення Будапештської конвенції про кіберзлочинність 2001 року [6], що є основним міжнародним договором у цій сфері. Тож, тому перша тенденція полягає у поступовому посиленні міжнародно-правового регулювання кіберпростору. Через те, що чинні міжнародні норми ще не повною мірою охоплюють питання юридичної відповідальності за сучасні види кіберзлочинів, кібератаки державного рівня та гібридні загрози, держави та міжнародні організації активно працюють над оновленням та доповненням наявного міжнародного права.

Зважаючи на зростання гібридних загроз, зокрема кібернетичних атак як елемента інформаційної війни, особливого значення набуває розвиток механізмів оперативного міжнародного обміну інформацією між урядовими структурами, правоохоронними органами та приватним сектором. Одним із перспективних напрямів є створення багатосторонніх ініціатив із формування спільних стандартів кіберзахисту, розробка комплексних механізмів реагування на масштабні кібератаки, а також посилення відповідальності суб'єктів, які надають цифрові послуги, за безпеку інформаційних систем.

Ще однією з тенденцій міжнародного співробітництва у сфері кібербезпеки є спільна боротьба у сфері дезінформації рф. У 2022 році НАТО оприлюднила нову програму швидкого реагування на кібератаки, в рамках якої пообіцяла посилити кіберзахист України перед обличчям російських кібератак, які тривають. Оновлено Комплексний пакет допомоги НАТО Україні, ключовим компонентом є Трастовий фонд кібербезпеки. НАТО зосередилося на розвитку можливостей України, забезпеченні необхідним обладнанням і навчанні персоналу у сфері кібербезпеки. Ця підтримка спрямована на те, щоб допомогти Україні захистити свою інфраструктуру від сучасних кіберзагроз [7, с. 78]. Міжнародне співробітництво у сфері кібербезпеки дедалі більше набуває геополітичного значення, особливо в контексті протидії дезінформаційним кампаніям та кібератакам з боку російської федерації. Також це стосується всіх війн і тому актуальним є в глобальному значенні. Кібербезпека стає ключовим компонентом національної та міжнародної безпеки, оскільки сучасні гібридні загрози використовують кіберпростір як ефективний інструмент для досягнення політичних, військових та економічних цілей.

На думку О. М. Полякова, подальше співробітництво доцільно зосередити на наступних напрямках: використання передового досвіду НАТО у цій площині, погли-

блювати державно-приватне партнерство; ініціювати приєднання України до Центру передового досвіду НАТО з кібероборони, що допоможе Україні імплементувати кращі практики і поглибити співпрацю з Альянсом у цій сфері; нарощувати оборонний технічний потенціал України у сфері кібербезпеки за сприяння Трастового фонду НАТО з кібербезпеки та у співпраці із Румунією; розробити механізми розподілення ризиків через використання захищених Хмарних сервісів задля мінімізації можливих втрат у разі кібернападу на інформаційні бази органів державної влади; залучати кращі практики задля посилення міжвідомчого співробітництва з виробленням конкретного дієвого механізму його практичного застосування; спільними зусиллями розробити систему мотивації для фахівців, зайнятих у сфері кібербезпеки тощо [2, с. 136]

Тому, дана тенденція також обумовлена рядом факторів, а саме: 1) зростанням рівня кіберагресії з боку рф, включаючи атаки на критичну інфраструктуру, банківську систему, державні реєстри та об'єкти військового управління; 2) транскордонним характером кіберзагроз, що ускладнює їх нейтралізацію без міжнародної координації; 3) необхідністю залучення інвестицій та технологій для модернізації систем кіберзахисту.

Участь України в ініціативах НАТО у сфері кібербезпеки дозволяє не лише посилити власний захист, а й сприяти формуванню глобальної стратегії протидії кіберагресії. В подальшому важливе інституційне посилення кібербезпеки України шляхом створення інтегрованих механізмів моніторингу та реагування на кіберзагрози. Також вагомим є поглиблення міжнародного співробітництва через участь у нових кібербезпекових ініціативах ЄС, G7 та НАТО. На доповнення цьому доцільним вважаємо створення міжнародного трибуналу для розслідування кіберзлочинів, зокрема тих, що мають системний характер і є частиною військової агресії. Тому дана тенденція характеризується розширенням колективних механізмів кіберзахисту, що проявляється у розвитку міжнародних ініціатив та багатосторонніх платформ для обміну даними про кіберзагрози.

На завершення спостерігається ще одна тенденція, а саме розвиток кібердипломатії та посилення кіберсанкцій як механізму міжнародного тиску. У зв'язку зі зростанням кількості державних кібератак, що стають елементом гібридної війни, міжнародна спільнота активно впроваджує дипломатичні механізми для попередження та нейтралізації загроз у кіберпросторі. Основним інструментом кібердипломатії є розробка міжнародних норм поведінки держав у кіберсередовищі, що включають принципи невтручання у цифрові системи інших країн, заборону на кібератаки проти цивільної інфраструктури та дотримання міжнародного гуманітарного права під час кіберконфліктів. У цьому контексті Європейський Союз та НАТО активно просувають ініціативу щодо розробки Кодексу, який би стосувався відповідальності держав у кіберпросторі задля забезпечення глобальної кібербезпеки.

Висновки. Отже, ефективне забезпечення кібербезпеки неможливе без транскордонної взаємодії та координації дій між державами, міжнародними організаціями та приватним сектором. Оскільки кіберзагрози мають глобальний характер, жодна держава не здатна ефективно протидіяти їм самостійно. У цьому контексті роль України як активного учасника міжнародних ініціатив у сфері кібербезпеки є фундаментальною, особливо з огляду на її унікальний досвід боротьби з масштабними кібератаками в тому числі під час війни з рф.

Аналіз існуючих тенденцій міжнародної співпраці у сфері кібербезпеки вказує на наявність системних проблем, зокрема фрагментарності політики кіберзахисту, відсутності належної координації між державами-партнерами, а також неефективного використання міжнародної технічної допомоги. Україна, як держава, що активно інтегрується в європейський та євроатлантичний безпековий простір, отримує значну технічну підтримку від міжнародних партнерів, зокрема НАТО, Європейського Союзу, США, Великобританії та Канади, спрямовану на посилення її кіберстійкості. Однак, проблемою залишається питання нераціонального використання програмних та апаратних засобів кіберзахисту, що надаються в межах міжнародної технічної допомоги.

Тому, можемо резюмувати, що міжнародне співробітництво у сфері кібербезпеки є критично важливим елементом сучасної системи глобальної безпеки, оскільки кіберзагрози мають транснаціональний характер і можуть безпосередньо впливати на політичну, економічну та соціальну стабільність держав. Відсутність єдиної міжнародно-правової бази у цій сфері, фрагментарність регулювання та різні підходи до кіберзахисту в різних країнах світу суттєво ускладнюють координацію зусиль для ефективного протистояння кіберзлочинності, державним кіберзагрозам та використанню кібератак у гібридних війнах.

ЛІТЕРАТУРА

1. Тєтєвін М. С. Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки. *Науковий вісник Ужгородського Національного Університету.* Серія ПРАВО. 2024.Вип. 82. Ч. 3. С. 263-266.

2. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. Інформація і право. 2021. № 2 (37). С. 129-138.

3. Станіславський Т. В. Розвиток міжнародного співробітництва України у сфері кібербезпеки. Актуальні проблеми державного управління. 2019. № 3 (79). С. 58-67.

4. Трофименко О. Г. Кібербезпека України: аналіз сучасного стану. *Захист інформації.* 2019. № 3. Том 21. С. 150-157.

5. Сливка М.М. Міжнародне співробітництво у сфері забезпечення кібербезпеки України. *Юридичний науковий електронний журнал*. 2022. № 10. С. 489-491.

6. Конвенція про кіберзлочинність: Міжнародний документ Ради Європи від 23.11.2001. URL (дата звернення 22.08.24)

7. Максимець В. Є., Вівсяна В. І. Співробітництво України та НАТО у протидії деструктивним інформаційним впливам російської федерації (2022–2023 рр.). *ВІСНИК НТУУ «КПІ».* Політологія. Соціологія. Право. 2023. Випуск 2(58). С. 74-80.