DOI: https://doi.org/10.37634/efp.2026.1.9
УДК 004.056.5:341.24

Людмила ***БУДНИК***
к.е.н., доцент, Західноукраїнський національний університет
ORCID: https://orcid.org/0009-0004-7762-5882
e-mail: l.budnyk@wunu.edu.ua

Ольга ***РОНСЬКА***
к.е.н., доцент, Західноукраїнський національний університет
ORCID: https://orcid.org/0000-0002-9856-3105
e-mail: o.ronska@wunu.edu.ua

БЕЗПЕКОВІ АСПЕКТИ МІЖНАРОДНОЇ СПІВПРАЦІ У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

У статті досліджено безпекові аспекти міжнародної співпраці у протидії кіберзлочинності в умовах зростання глобальних цифрових загроз. Проаналізовано сучасний стан кіберзлочинів, основні виклики транскордонної взаємодії та проблеми гармонізації правових підходів. Розкрито роль міжнародних організацій і механізмів інформаційного обміну у забезпеченні ефективного реагування на кіберінциденти. Визначено ключові ризики, пов'язані з політизацією співпраці, нерівномірністю технічного розвитку та відсутністю стандартизованих процедур. Запропоновано рекомендації із вдосконалення глобальних механізмів кібербезпеки та підвищення результативності міжнародної взаємодії.

Ключові слова: *кіберзлочинність, міжнародна співпраця, кібербезпека, обмін інформацією, нормативно-правове регулювання*

ВСТУП

Глобалізація інформаційного простору, швидкий розвиток цифрових технологій та інтеграція держав у світову кіберінфраструктуру створили нові виклики для національних систем безпеки. Кіберзлочини стали однією з найбільш загрозливих форм злочинності, що не визнає державних кордонів та здійснюється із застосуванням інноваційних технологічних засобів. Сучасні кіберзагрози характеризуються високим рівнем анонімності, складністю технічної реалізації та глобальністю наслідків впливу, що унеможливлює повноцінну протидію їм в межах однієї держави. Саме тому питання міжнародної співпраці у сфері протидії кіберзлочинності набуває визначального значення.

МАТЕРІАЛИ ТА МЕТОДИ

У дослідженні застосовано міжнародні нормативно-правові акти, аналітичні звіти провідних організацій з кібербезпеки та наукові публікації, що стосуються транснаціональної кіберзлочинності. Методологічною основою стала системно-аналітична оцінка механізмів міжнародної співпраці та безпекових підходів до протидії кіберзагрозам. Для порівняння ефективності різних моделей міжнародної взаємодії застосовано компаративний метод. Крім того, проведено контент-аналіз практик обміну інформацією між державами та міжнародними інституціями.

МЕТА статті – аналіз безпекових аспектів міжнародної співпраці у боротьбі з кіберзлочинністю та визначення ключових механізмів підвищення ефективності такої взаємодії.

РЕЗУЛЬТАТИ

Сучасний стан кіберзагроз визначено стрімким ускладненням технічних методів атак, високим рівнем автоматизації та здатністю шкідливих програм адаптуватися до механізмів захисту. Fortinet у своєму звіті вказав на ключові тенденції кіберзагроз 2025 [1]. Кіберпростір став середовищем, в якому злочинці активно застосовують фішингові кампанії, програми-вимагачі, шкідливе програмне забезпечення, DDoS-атаки, компрометацію ланцюгів поставок, фінансові шахрайські схеми, викрадення персональних даних і промислове шпигунство. Все це перетворило кіберзлочинність на складний багатокомпонентний феномен, що не обмежується національними кордонами та характеризується значним потенціалом завдання шкоди державним інституціям, бізнесу та приватним особам. Особливе занепокоєння викликає той факт, що значна частина масштабних кібератак здійснюється транснаціональними злочинними угрупованнями, які часто мають приховану підтримку або толерантність з боку окремих державних структур. Це формує додатковий безпековий вимір і ускладнює процес атрибуції, адже визначення реального джерела атаки потребує не лише технічного аналізу, а й комплексного розгляду політичного контексту. Водночас технологічний ландшафт розвивається настільки швидко, що навіть найпідготовленіші правоохоронні органи багатьох країн не встигають адаптувати методики розслідування, а обмеження в ресурсах і відсутність висококваліфікованих фахівців лише поглиблюють проблему.

У межах міжнародної співпраці виникає низка викликів, які суттєво впливають на ефективність колективної протидії кіберзлочинності. Насамперед це різні правові стандарти, що визначають склад кіберзлочинів і встановлюють відповідальність за них, причому в окремих юрисдикціях такі злочини досі не виділено в окрему категорію кримінального права. До цього додається проблема атрибуції: встановити джерело атаки та зібрати доказову базу, достатню для судового переслідування, часто майже неможливо через застосування анонімізуючих технологій, багаторівневих проксі та кібератак «під чужим прапором». Значною перешкодою залишається нерівномірний рівень кіберзахисту різних держав: одні країни мають розвинені національні CERT- і CSIRT-структури, інші – відчувають дефіцит технічних ресурсів, що робить їх «слабкими ланками» глобальної цифрової безпеки. Політичні інтереси окремих держав також накладають свій відбиток, оскільки вони нерідко стримують обмін інформацією або ухиляються від співпраці, побоюючись розкриття власних внутрішніх кіберможливостей чи стратегічних вразливостей. У сукупності ці чинники свідчать про те, що боротьба з кібер-

© Л. БУДНИК, О. РОНСЬКА, 2026

злочинністю вимагає глобально скоординованих зусиль, заснованих на довірі, стандартизованих технічних підходах і ефективних каналах міжнародної комунікації.

Нормативно-правове регулювання міжнародної боротьби з кіберзлочинністю залишається фрагментарним, хоча наявні окремі важливі документи та інституційні платформи. Центральне місце серед них займає Будапештська конвенція 2001 р., що стала першим універсальним міжнародним актом, спрямованим на уніфікацію криміналізації кіберзлочинів і створення механізмів міжнародної взаємодії [2]. Водночас глобальна дієвість конвенції обмежується тим, що низка ключових держав з високим кіберпотенціалом відмовилися її підтримати, що створює значні прогалини у міжнародному правовому полі. У 2022 р. прийнято Другий додатковий протокол до Конвенції, який розширив можливості транскордонного доступу до електронних доказів і передбачив прямий обмін даними між компетентними органами та провайдерами, що суттєво пришвидшує реагування на кіберінциденти та підвищує ефективність розслідувань [3].

На глобальному рівні ООН продовжує пошук консенсусу з формування нової універсальної конвенції про кіберзлочинність, однак цей процес ускладнено суттєвими розбіжностями між країнами із трактування інформаційної безпеки, свободи слова, цифрових прав людини та меж міжнародного впливу в кіберпросторі. Регіональні ініціативи, хоч і демонструють вищий рівень практичності, також не забезпечують повного глобального охоплення. В Європі активно функціонують мережі кіберінформаційних центрів, Європол та ENISA, які координують розслідування, забезпечують технічну підтримку та організовують обмін аналітикою [4]. У межах G7 реалізуються проекти з обміну інформацією та вироблення колективних механізмів реагування. США зі свого боку укладають двосторонні угоди, що дають змогу підвищити рівень координації з окремими державами. Проте навіть за наявності такої кількості інструментів фрагментарність і відсутність уніфікації залишаються головною проблемою міжнародної взаємодії.

Одним з найважливіших аспектів боротьби з кіберзлочинністю є ефективний обмін інформацією та організація міжнародних механізмів реагування. Держави повинні швидко отримувати, аналізувати та передавати дані про інциденти, щоб мінімізувати їхній масштаб і запобігати повторним атакам. Однак сучасна практика демонструє суттєві обмеження. Технічні бар'єри зумовлено тим, що не всі країни мають розвинені центри аналізу кіберзагроз, здатні працювати в режимі реального часу та застосовувати сучасні інструменти автоматизованого виявлення атак. Правові бар'єри виникають через розбіжності в підходах до захисту персональних даних, регулювання доступу до метаданих і вимог до збереження інформації у провайдерів [5].

Міжнародна координація супроводжується низкою безпекових ризиків, які потрібно враховувати у формуванні сучасної інфраструктури кіберспівпраці. Одним з головних ризиків є загроза витоку конфіденційної інформації, адже обмін оперативними даними часто включає елементи державної таємниці або інформацію, що стосується критичної інфраструктури. Якщо держава-партнер має недостатній рівень кіберзахисту, навіть одноразовий витік може завдати значної шкоди. Інший ризик пов'язаний з можливістю використання співпраці у політичних цілях, коли окремі країни маніпулюють даними або застосовують їх для тиску на партнерів. Додаткову небезпеку становить подвійне застосування технологій, створених в межах співпраці, адже інструменти захисту може бути застосовано й для наступальних кібероперацій.

На основі проведеного аналізу можна окреслити ключові напрями вдосконалення міжнародної співпраці. Першочерговим завданням є гармонізація законодавства у сфері кібербезпеки, розширення застосування Будапештської конвенції та її протоколів, а також розроблення нових універсальних норм до цифрових доказів і процедур збереження даних. Наступним стратегічним кроком має стати створення глобальної системи швидкого реагування на кіберінциденти – міжнародного центру або платформи, яка забезпечувала б координацію у разі масштабних атак і дозволяла оперативно мобілізувати ресурси. Важливим напрямом є підвищення рівня довіри між державами, що може бути досягнуто шляхом прозорих політик у сфері кібероперацій, регулярних спільних навчань, симуляційних вправ і механізмів підтвердження доброчесності партнерів. Значну увагу потрібно приділяти технічній сумісності, стимулюючи застосування однакових форматів обміну інформацією, відкритих стандартів та спільних платформ аналізу загроз. Окрему роль відіграє зміцнення партнерства між державою та приватним сектором, адже більшість цифрових ресурсів і критичної інфраструктури перебувають у руках приватних компаній, які мають власні інструменти виявлення та реагування на атаки. Поєднання державних та приватних можливостей здатне створити більш стійку систему глобальної кібербезпеки та підвищити готовність до протидії найскладнішим сучасним загрозам.

ВИСНОВКИ

Міжнародна співпраця в боротьбі з кіберзлочинністю є стратегічним елементом глобальної безпеки, оскільки жодна країна не здатна самостійно протистояти високотехнологічним загрозам у цифровому середовищі. Аналіз показав, що сучасні механізми координації мають значний потенціал, але залишаються фрагментованими та обмеженими низкою політичних, правових і технічних бар'єрів. Найбільш перспективними напрямами вдосконалення міжнародної взаємодії є гармонізація законодавства, розбудова спільних інструментів технічного реагування, підвищення рівня довіри між державами та посилення приватно-публічного партнерства. Впровадження рекомендацій, визначених у статті, сприятиме формуванню більш стійкої та ефективної системи глобальної кібербезпеки. Тільки узгоджені дії держав на основі спільних стандартів і відповідальності здатні забезпечити належний рівень захисту в умовах зростання кіберзагроз та комплексності інформаційного простору.

Список використаних джерел

1. Загрози-2025: звіт Fortinet про майбутні тренди, ризики та рішення у галузі кібербезпеки. URL: https://my-

itspecialist.com/zvit-fortinet-zagrozy-2025-kiberbezpeka

2. Конвенція про кіберзлочинність. Ратифікація від 07.09.2005. № 994_575 URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

3. Посилена співпраця та розкриття електронних доказів: 22 країни підписали новий Протокол до Конвенції про кіберзлочинність. URL: https://www.coe.int/uk/web/kyiv/-/enhanced-co-operation-and-disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention

4. Кривенко П. Зміцнення кіберзахисту Європи: найновіший арсенал у боротьбі з кіберзагрозами. URL: https://cacds.org.ua/зміцнення-кіберзахисту-європи-найно/

5. Попко В.В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського національного університету*. 2021. № 66. С. 276–283.

References

1. Zahrozy-2025: report of Fortinet on future trends, risks and solutions in the field of cybersecurity. URL: https://my-itspecialist.com/zvit-fortinet-zagrozy-2025-kiberbezpeka (In Ukrainian).

2. Convention on Cybercrime. Ratification of 07.09.2005 No. 994_575. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (In Ukrainian).

3. Enhanced cooperation and disclosure of electronic evidence: 22 countries signed a new Protocol to the Convention on Cybercrime. URL: https://www.coe.int/uk/web/kyiv/-/enhanced-co-operation-and-disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention (In Ukrainian).

4. Kryvenko P. Strengthening Europe's cyber defense: the latest arsenal in combating cyber threats. URL: https://cacds.org.ua/зміцнення-кіберзахисту-європи-найно/ (In Ukrainian).

5. Popko V.V. International legal regulation of transnational cybercrime in cyberspace. *Scientific Bulletin of Uzhhorod National University*. 2021. No. 66. pp. 276–283. (In Ukrainian).

Liudmyla BUDNYK
PhD in Economics, Associate Professor, West Ukrainian National University
ORCID: https://orcid.org/0009-0004-7762-5882
e-mail: l.budnyk@wunu.edu.ua

Olha RONSKA
PhD in Economics, Associate Professor, West Ukrainian National University
ORCID: https://orcid.org/0000-0002-9856-3105
e-mail: o.ronska@wunu.edu.ua

SECURITY ASPECTS OF INTERNATIONAL COOPERATION IN FIGHTING CYBERCRIME

The paper examines the security aspects of international cooperation in combating cybercrime, emphasizing the growing complexity and transnational nature of digital threats. The introductory section outlines how global digitalization and the rapid evolution of cyberattacks create challenges that no state can address independently. The materials and methods of the study are based on international legal instruments, analytical reports, and comparative and content analysis, enabling an assessment of existing cooperation mechanisms. The purpose of the paper is to analyze security-oriented approaches to international interaction and identify effective tools for strengthening collective resilience. The results demonstrate that cybercrime has evolved into a multilayered global phenomenon marked by advanced attack techniques, difficulties in attribution, uneven cybersecurity capacities, and political constraints that hinder information exchange. The study reviews key legal frameworks, including the Budapest Convention and its protocols, UN initiatives, and regional mechanisms of the EU, NATO, and G7, highlighting their fragmented implementation. It further analyzes technical, legal, and trust-related barriers to information sharing, alongside security risks such as data leaks, political misuse of shared intelligence, and the dual-use nature of cyber tools. Based on this assessment, the paper proposes harmonization of legislation, establishment of rapid-response mechanisms, enhancement of trust-building practices, improvement of technical interoperability, and expanded public–private partnerships as essential components of effective cooperation. The conclusions emphasize that only coordinated international action, grounded in shared standards and mutual responsibility, can ensure sustainable global cybersecurity in the face of escalating digital threats.

Keywords: *cybercrime, international cooperation, cybersecurity, information, exchange, legal frameworks*