УДК 343.9
DOI https://doi.org/10.32782/klj-2026-9.16

КІБЕРЗЛОЧИННІСТЬ ЯК ТРАНСНАЦІОНАЛЬНЕ ЯВИЩЕ: КРИМІНОЛОГІЧНІ ДЕТЕРМІНАНТИ ТА МІЖНАРОДНО-ПРАВОВІ МЕХАНІЗМИ ПРОТИДІЇ В УКРАЇНІ

Телесніцький Геннадій Никонович,
кандидат юридичних наук,
завідувач кафедри загально юридичних дисциплін
Приватного вищого навчального закладу «Фінансово-правовий коледж»
ORCID ID: 0000-0002-5427-1821

У статті аргументовано, що притаманна кіберзлочинності транснаціональність обумовлює потребу в комплексному поєднанні кримінологічного та міжнародно-правового підходів як у її науковому осмисленні, так і в практиці протидії. Проаналізовано ключові детермінанти цього явища в умовах цифровізації, зокрема соціально-економічні, технологічні та нормативно-правові чинники. Особливий акцент зроблено на міжнародно-правових інструментах боротьби з кіберзлочинністю та особливостях їх впровадження в Україні. Розглянуто положення Будапештської конвенції про кіберзлочинність і окреслено роль міжнародних організацій у відповідній сфері. Запропоновано напрями вдосконалення національного механізму запобігання та протидії кіберзлочинності.

Обґрунтовано, що міжнародно-правові інструменти, зокрема положення Будапештської конвенції, мають визначальне значення для формування дієвої системи протидії кіберзлочинності, оскільки сприяють гармонізації криміналізації відповідних діянь, регулюють процедури збирання цифрових доказів та посилюють міжнародне співробітництво. Підкреслено доцільність активнішого впровадження міжнародних стандартів у національну кримінологічну політику, а також адаптації механізмів міжнародної взаємодії до умов гібридних загроз.

Доведено, що ефективна протидія кіберзлочинності можлива лише за умови системного підходу, який поєднує національні та міжнародні зусилля, використання сучасних технологічних рішень і неухильне дотримання стандартів прав людини. Саме це забезпечує належний рівень безпеки в цифровому середовищі та гарантує захист прав і свобод особи.

У висновках наголошено, що для України пріоритетними завданнями залишаються подальше впровадження міжнародних стандартів, модернізація національного законодавства та підвищення результативності діяльності правоохоронних органів. Важливим є також зміцнення інституційної спроможності, розвиток технічного потенціалу та вдосконалення професійної підготовки фахівців у сфері кібербезпеки. Перспективи подальших досліджень доцільно пов'язати з аналізом окремих форм кіберзлочинів (зокрема ransomware, phishing, кібершпигунство), а також із розробленням кримінологічних моделей прогнозування та оцінювання ризиків у цифровому середовищі.

Ключові слова: *кіберзлочинність, транснаціональна злочинність, кримінологічні детермінанти протидії кіберзлочинності, міжнародно-правові механізми протидії кіберзлочинності, цифрові докази, Будапештська конвенція про кіберзлочинність, технічне забезпечення та професійної підготовки кадрів у сфері кібербезпеки.*

Telesnitsky Gennadiy. Cybercrime as a transnational phenomenon: criminological determinants and international legal mechanisms for countering it in Ukraine

The article argues that the transnational nature of cybercrime necessitates a comprehensive integration of criminological and international legal approaches, both in its academic analysis and in practical countermeasures. The key determinants of this phenomenon in the context of digitalisation are analysed, in particular socio-economic, technological and regulatory factors. Particular emphasis is placed on international legal instruments for combating cybercrime and the specifics of their implementation in Ukraine. The provisions of the Budapest Convention on Cybercrime are examined, and the role of international organisations in this field is outlined.

Directions for improving the national mechanism for preventing and combating cybercrime are proposed.

It is argued that international legal instruments, in particular the provisions of the Budapest Convention, are of decisive importance for the formation of an effective system to counter cybercrime, as they contribute to the harmonisation of the criminalisation of relevant acts, regulate procedures for the collection of digital evidence, and strengthen international cooperation. The paper emphasises the desirability of more actively incorporating international standards into national criminal policy, as well as adapting mechanisms for international cooperation to the conditions of hybrid threats.

It has been demonstrated that cybercrime can only be effectively combated through a systematic approach that combines national and international efforts, the use of modern technological solutions, and strict adherence to human rights standards. It is precisely this approach that ensures an adequate level of security in the digital environment and guarantees the protection of individual rights and freedoms.

The conclusions emphasise that Ukraine's priority tasks remain the further implementation of international standards, the modernisation of national legislation, and the improvement of the effectiveness of law enforcement agencies. It is also important to strengthen institutional capacity, develop technical capabilities, and improve the professional training of specialists in the field of cybersecurity. Future research should focus on analysing specific forms of cybercrime (in particular ransomware, phishing and cyber espionage), as well as on developing criminological models for forecasting and assessing risks in the digital environment.

Key words: *cybercrime, transnational crime, criminological determinants of combating cybercrime, international legal mechanisms for combating cybercrime, digital evidence, the Budapest Convention on Cybercrime, technical support and professional training in the field of cybersecurity.*

Постановка проблеми. Інтенсивне зростання інформаційно-комунікаційних технологій і цифрова трансформація суспільних відносин спричинили виникнення новітніх форм протиправної діяльності, які не обмежуються межами окремих держав. У цих умовах кіберзлочинність перетворилася на транснаціональне явище. І. Д. Бондаренко вважає, що «реальні кейси масштабних кібератак рф на Україну, розуміння у світі значення фактичних наслідків таких атак, їх здатності до масштабування та впливу на критичні для функціонування держави і життя соціуму сервіси – все це сприяло посиленню позиції щодо необхідності переосмислення міжнародно-правового змісту кібератак крізь призму міжнародного гуманітарного та міжнародного кримінального права» [1]. Варто погодитися, що «в умовах ескалації кіберзагроз, зокрема, у контексті збройних конфліктів, нагальною є потреба у створенні гармонізованої міжнародно-правової бази для ефективної кібербезпеки та захисту даних» [2].

У контексті збройного конфлікту та посилення гібридних викликів для України проблема кіберзлочинності загострюється. Відзначається тенденція до збільшення кількості кібератак, націлених на державні органи, об'єкти критичної інфраструктури, а також установи приватного сектору. Як наголошують фахівці, «системні та масштабні кібератаки рф на Україну та їх вплив на критичні для функціонування держави сервіси зумовлює необхідність переосмислення застосування практики міжнародного урегулювання відносин кібербезпеки» [2]. Це зумовлює необхідність застосування комплексного підходу, який інтегрує кримінологічне дослідження з дієвими механізмами міжнародно-правового співробітництва.

Аналіз останніх досліджень і публікацій. Проблематика криміналістичної типологізації правопорушень у кіберпросторі протягом останніх років залишається актуальною та привертає увагу численних науковців таких як: Бондаренко І. Д., Діденко О. В., Думчиков М. О., Карвацька С.Б., Маник А.З., Строїч М. І. Водночас, попри активність наукових досліджень і опрацювання цього дискусійного напряму, варто підкреслити потребу в його всебічному, системному й багаторівневому осмисленні.

Метою цієї статті є з'ясування кримінологічних чинників, що зумовлюють кіберзлочинність як транснаціональне явище, а також дослідження міжнародно-правових інструментів протидії їй і особливостей їх впровадження в Україні.

Виклад основного матеріалу дослідження. Кіберзлочинність становить багатовимірне соціально-правове явище, яке виникає та розвивається під впливом сукупності взаємопов'язаних чинників [3]. Серед ключових кримінологічних детермінант слід виокремити низку взаємопов'язаних чинників. По-перше, йдеться про технологічні фактори: масштабне впровадження цифрових рішень, розвиток інтернету речей, технологій штучного інтелекту та хмарних сервісів відкривають додаткові можливості для вчинення протиправних дій [4]. Практика Інтерполу демонструє, що забезпечена в мережі Інтернет анонімність, а також використання криптовалют істотно ускладнюють процес встановлення особи правопорушників [5]. По-друге, до соціально-економічних детермінант належать, зокрема, рівень безробіття, соціальна диференціація, а також недостатній рівень цифрової обізнаності населення, що в сукупності сприяють поширенню кіберзлочинності [3]. Водночас значний попит на нелегальні послуги у цифровому середовищі сприяє активізації та розширенню кіберкримінальних ринків. По-третє, до вагомих детермінант належать правові чинники: асинхронність розвитку законодавства в різних державах, відсутність єдиних уніфікованих стандартів, а також ускладненість процедур міжнародної правової допомоги формують сприятливе середовище для функціонування кіберзлочинності [6].

Окрему групу становлять організаційні та інституційні детермінанти. Кіберзлочинність дедалі частіше набуває ознак організованої злочинної діяльності: формуються стійкі злочинні угруповання, які діють за моделями, подібними до бізнес-структур, із чітким розподілом функцій між учасниками (розробники шкідливого програмного забезпечення, виконавці атак, посередники з легалізації незаконних доходів тощо). Це засвідчує поступову трансформацію кіберзлочинності у високодохідну кримінальну індустрію.

У сучасних умовах кіберзлочинність є складним, багатовимірним і динамічним явищем, яке виходить за межі класичних уявлень про злочинність. Вона характеризується чітко вираженою транснаціональною природою [4; 5]. Транснаціональний характер цього явища обумовлює потребу у формуванні комплексної системи протидії, що інтегрує кримінологічні, кримінально-правові та міжнародно-правові інструменти. Кіберзлочини можуть плануватися на території однієї держави, реалізовуватися з іншої, а їхні наслідки проявлятися в третіх країнах. Така багаторівнева організація ускладнює визначення юрисдикції, спричиняє колізії у правозастосуванні та потребує дієвих механізмів міжнародної координації.

М.О. Думчиков виділяє за способами вчинення такі кримінальні правопорушення у кіберпросторі «1) неправомірне підключення до інформаційно – телекомунікаційних систем та мереж; 2) створення, використання, розповсюдження та збут мережевого шкідливого програмного забезпечення; 3) протиправне створення, використання, розповсюдження або збут, матеріалів заборонених до публічного і вільного обороту, вчиненого шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж; 4) порушення авторських та суміжних прав в мережі Інтернет; 5) шахрайство вчинене з використанням цифрових пристроїв; 6) крадіжка вчинена в кібернетичному просторі; 7) надання комерційних послуг в мережі Інтернет без оформлення фізичної особи підприємця; 8) вимагання у кіберпросторі; 9) кібертероризм» [7].

Окремої уваги потребують найбільш поширені види кіберзлочинності в сучасних умовах. Серед них варто виокремити несанкціоноване втручання у роботу інформаційних систем, поширення шкідливого програмного забезпечення, фішин-

гові атаки, онлайн-шахрайство, незаконне заволодіння персональними даними, а також атаки із застосуванням програм-вимагачів (ransomware). В останні роки спостерігається тенденція до ускладнення таких посягань, їх автоматизації та дедалі активнішого використання технологій штучного інтелекту [4; 5]. На сьогодні «цифрова криміналістика займається збором, аналізом, збереженням і представленням цифрових доказів, отриманих з електронних пристроїв, мереж або цифрових середовищ, з метою розслідування злочинів, зокрема кіберзлочинів» [8, с. 190]. Вона охоплює методи виявлення, фіксації, вилучення та аналізу даних із комп'ютерів, смартфонів, серверів і хмарних сховищ, забезпечуючи їх належну доказову силу в судових провадженнях. Водночас важливим є дотримання вимог щодо захисту прав людини та забезпечення конфіденційності інформації.

В умовах збройного конфлікту кіберзлочинність часто перетинається з кіберопераціями, які можуть містити як ознаки кримінальних правопорушень, так і елементи кібервоєнного впливу. Це ускладнює правову кваліфікацію таких діянь і визначення належних механізмів притягнення до відповідальності. Міжнародно-правові засади протидії кіберзлочинності формуються через систему багатосторонніх договорів, регіональних ініціатив, а також практику діяльності міжнародних організацій [2]. Ключове місце серед таких інструментів займає Будапештська конвенція про кіберзлочинність, яка закріплює базові стандарти криміналізації відповідних діянь і визначає механізми міжнародного співробітництва у протидії кіберзлочинам [6]. Важливе значення мають також інструменти взаємної правової допомоги, екстрадиційні процедури, діяльність спільних слідчих груп, а також обмін оперативними даними через канали Інтерполу та Європолу. У сучасних умовах одним із ключових механізмів оперативного реагування на кіберінциденти виступає функціонування мережі цілодобових (24/7) контактних пунктів.

Україна активно інтегрується у міжнародну систему протидії кіберзлочинності [9; 10]. На національному рівні функціонують спеціалізовані підрозділи кіберполіції, прийнято нормативно-правові акти у сфері кібербезпеки, а також активно розвивається співпраця з міжнародними партнерами. Водночас аналіз практики виявляє низку проблемних аспектів. Зокрема, йдеться про недостатню оперативність обміну інформацією між державами, ускладненість процедур отримання електронних доказів з-за кордону, а також неоднаковий рівень технічного забезпечення правоохоронних органів [2]. Окремий напрям становить питання допустимості та належності цифрових доказів. У вітчизняній практиці досі відсутні повністю уніфіковані підходи до їх збирання, фіксації та оцінювання. Це, у свою чергу, може спричиняти втрату доказової сили отриманої інформації або її успішне оскарження в судовому порядку.

У контексті протидії кіберзлочинності особливого значення набуває практика ЄСПЛ, яка визначає баланс між ефективністю розслідувань та захистом прав людини в цифровому середовищі. Зокрема, у справі «Benedik v. Slovenia» Суд наголосив, що встановлення особи користувача Інтернету за IP-адресою є втручанням у право на повагу до приватного життя, гарантоване статтею 8 Конвенції [12]. Відтак, доступ правоохоронних органів до подібних даних має бути чітко врегульований на законодавчому рівні та забезпечений належними гарантіями від можливих зловживань. У справі «Big Brother Watch and Others v. the United Kingdom» ЄСПЛ визначив стандарти щодо масового перехоплення комунікацій, підкресливши необхідність забезпечення ефективного незалежного нагляду та дотримання принципу пропорційності втручання у права людини [13].

Зазначені підходи мають безпосереднє значення для України, оскільки окреслюють межі допустимого використання цифрових доказів і проведення кіберрозслідувань відповідно до європейських

стандартів захисту прав людини. З метою підвищення ефективності протидії кіберзлочинності доцільним є вдосконалення законодавчого регулювання цифрових доказів, гармонізація процесуальних процедур із міжнародними стандартами, посилення міжнародного співробітництва, підвищення рівня професійної підготовки фахівців, а також впровадження сучасних технологічних рішень для аналізу кіберзагроз.

Висновки і перспективи подальших розвідок у даному напрямі. Отже, кіберзлочинність у сучасних умовах постає як одна з найдинамічніших і водночас найнебезпечніших форм злочинної діяльності, що характеризується виразною транснаціональністю. Її детермінаційний комплекс охоплює технологічні, соціально-економічні та правові чинники, які перебувають у тісній взаємодії та посилюють свій вплив у процесі цифровізації суспільства і в умовах збройних конфліктів. Проведений аналіз дає підстави стверджувати, що ключову роль серед таких чинників відіграють стрімкий розвиток технологій, глобалізаційні тенденції, наявність соціально-економічних диспропорцій, а також прогалини й недосконаліть правового регулювання. Сукупний вплив зазначених факторів формує сприятливе підґрунтя для виникнення та еволюції новітніх форм злочинної поведінки у кіберпросторі.

Ефективна протидія кіберзлочинності можлива лише за умови реалізації комплексного підходу, що передбачає консолідацію національних і міжнародних зусиль, активне застосування інноваційних технологічних рішень та неухильне дотримання міжнародних стандартів у сфері прав людини. Такий підхід є необхідною передумовою забезпечення належного рівня кібербезпеки та гарантування захисту прав і свобод особи у цифровому середовищі. Важливе значення у формуванні дієвої системи протидії кіберзлочинності мають міжнародно-правові інструменти, передусім положення Будапештської конвенції про кіберзлочинність. Вони сприяють гармонізації кримінально-правових підходів до визначення протиправних діянь, регламентують процедури збору й використання електронних доказів, а також створюють нормативну основу для розвитку ефективного міжнародного співробітництва.

Для України пріоритетними залишаються завдання подальшого впровадження міжнародно-правових стандартів у національну правову систему, вдосконалення законодавчого регулювання та підвищення результативності діяльності правоохоронних органів у цій сфері. Особливого значення набуває зміцнення інституційної спроможності, модернізація технічної бази та підвищення рівня професійної підготовки фахівців із кібербезпеки.

Перспективи подальших наукових розвідок пов’язані з поглибленим вивченням окремих різновидів кіберзлочинів (зокрема програм-вимагачів, фішингових атак і кіберрозвідки), а також із розробленням сучасних кримінологічних моделей прогнозування динаміки кіберзлочинності та оцінювання ризиків у цифровому середовищі.

ЛІТЕРАТУРА:

1. Бондаренко І. Д. Концепт «втрати функціональності» в контексті визнання кібератак воєнним злочином. *Юридичний науковий електронний журнал.* 2024. № 10. С. 500–503. DOI: https://doi.org/10.32782/2524-0374/2024-10/115

2. Карвацька С. Б., Маник А. З., Строїч М. І. Кібербезпека: сучасні виклики та міжнародно-правові рамки щодо захисту даних. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2025. Вип. 87, ч. 4. DOI: https://doi.org/10.24144/2307-3322.2025.87.4.39

3. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems : Protocol of the Council of Europe (28.01.2003). URL: https://ccdcoe.org/uploads/2018/11/CoE-030128-AdditionalProtocol-1.pdf (дата звернення: 01.04.2026).

4. Comprehensive study on cybercrime / United Nations Office on Drugs and Crime. 2013. URL: https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html (дата звернення: 01.04.2026).

5. Internet Organised Crime Threat Assessment (IOCTA) 2024 / Europol. 2024. URL: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 (дата звернення: 01.04.2026).

6. Convention on Cybercrime : Convention of the Council of Europe від 23 листоп. 2001 р. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата звернення: 01.04.2026).

7. Думчиков М. О. Криміналістична типологізація кримінальних правопорушень у кіберпросторі. *Аналітично-порівняльне правознавство.* 2023. № 2. С. 287–290. DOI: https://doi.org/10.24144/2788-6018.2023.02.49

8. Діденко О. В. Цифрова криміналістика та міжнародна протидія кіберзлочинності (на прикладі електронної торгівлі). *Аналітично-порівняльне правознавство.* 2025. № 4 (3). С. 184–192. DOI: https://doi.org/10.24144/2788-6018.2025.04.3.26

9. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 01.04.2026).

10. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text и(дата звернення: 01.04.2026).

11. Global cybercrime strategy 2022–2025 / INTERPOL. 2022. URL: https://www.interpol.int/content/download/19846/file/Cybercrime%20Global%20Strategy_EN.pdf (дата звернення: 01.04.2026).

12. Benedik v. Slovenia (Application no. 62357/14): judgment of the European Court of Human Rights від 24 Apr. 2018. URL: https://hudoc.echr.coe.int/eng?i=002-11930 (дата звернення: 01.04.2026).

13. Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15): judgment of the European Court of Human Rights від 25 May 2021. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-140713%22]} (дата звернення: 01.04.2026).

REFERENCES:

1. Bondarenko, I. D. (2024). Kontsept «vtraty funktsionalnosti» v konteksti vyznannia kiberatak voiennym zlochynomи [The concept of 'loss of functionality' in the contexof recognising cyberattacks as war crimes.]. *Yurydychnyi naukovyi elektronnyi zhurnal*, 10, 500–503. https://doi.org/10.32782/2524-0374/2024-10/115 [in Ukrainian].

2. Karvatska, S. B., Manyk, A. Z., & Stroich, M. I. (2025). Kiberbezpeka: suchasni vyklyky ta mizhnarodno-pravovi ramky shchodo zakhystu danykh. [Cybersecurity: current challenges and the international legal framework for data protection]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo*, 4(87). https://doi.org/10.24144/2307-3322.2025.87.4.39 [in Ukrainian].

3. Council of Europe. (2003, January 28). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. https://ccdcoe.org/uploads/2018/11/CoE-030128-AdditionalProtocol-1.pdf

4. United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime. https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html

5. Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

6. Council of Europe. (2001, November 23). Convention on Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention

7. Dumchykov, M. O. (2023). Kryminalistychna typolohizatsiia kryminalnykh pravoporushen u kiberprostori. [Criminal typology of criminal offences in cyberspace]. *Analitychno-porivnialne pravoznavstvo*, 2, 287–290. https://doi.org/10.24144/2788-6018.2023.02.49 [in Ukrainian].

8. Didenko, O. V. (2025). Tsyfrova kryminalistyka ta mizhnarodna protydiia kiberzlochynnosti (na prykladi elektronnoi torhivli). [Digital forensics and international efforts to combat cybercrime (with reference to e-commerce).]. *Analitychno-porivnialne pravoznavstvo*, 4(3), 184–192. https://doi.org/10.24144/2788-6018.2025.04.3.26 [in Ukrainian].

9. Verkhovna Rada Ukrainy. (2001, April 5). Kryminalnyi kodeks Ukrainy No. 2341-III. https://zakon.rada.gov.ua/laws/show/2341-14#Text [in Ukrainian].

10. Verkhovna Rada Ukrainy. (2017, October 5). Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» No. 2163-VIII. [On the Basic Principles of Ensuring Ukraine's Cybersecurity' No. 2163-VIII.]. https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

11. INTERPOL. (2022). Global cybercrime strategy 2022–2025. https://www.interpol.int/content/download/19846/file/Cybercrime%20Global%20Strategy_EN.pdf

12. European Court of Human Rights. (2018, April 24). Benedik v. Slovenia (Application no. 62357/14). https://hudoc.echr.coe.int/eng?i=002-11930

13. European Court of Human Rights. (2021, May 25). Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15). https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-140713%22]}

Дата першого надходження статті до видання: 14.04.2026
Дата прийняття статті до друку після рецензування: 12.05.2026
Дата публікації (оприлюднення) статті: 20.05.2026