



УДК 341.9:343.7:004.056

[https://doi.org/10.52058/3041-1254-2026-5\(27\)-686-695](https://doi.org/10.52058/3041-1254-2026-5(27)-686-695)

Пипяк Микола Іванович кандидат юридичних наук, доцент, доцент кафедри права, Вінницький торговельно економічний інститут Державного торговельно-економічного університету, м. Вінниця, <https://orcid.org/0000-0001-9133-6762>

МІЖНАРОДНО-ПРАВОВА ДОПОМОГА ТА СПІВРОБІТНИЦТВО У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ: ВИКЛИКИ ЦИФРОВОЇ ЕПОХИ

Анотація. У статті здійснено комплексний теоретико-правовий аналіз становлення, сучасного стану та перспектив розвитку міжнародного співробітництва у сфері протидії кіберзлочинності. Визначено, що протиправні діяння в інформаційному просторі переросли рівень поодиноких правопорушень і трансформувалися у високотехнологічну транснаціональну індустрію. Ця кримінальна діяльність дедалі частіше функціонує як скоординований тіньовий бізнес, що надає протиправні послуги за замовленням, залучає інструменти штучного інтелекту для автоматизації атак і зливається з іншими небезпечними формами організованої злочинності, зокрема з торгівлею людьми, корупційними схемами та легалізацією брудних коштів.

У роботі детально досліджено еволюцію міжнародної нормативно-правової бази, яка пройшла шлях від регіональних ініціатив окремих держав до розробки та ухвалення універсального договору під егідою Організації Об'єднаних Націй. Проведено порівняльний аналіз правових інструментів, що заклали основи криміналізації комп'ютерних системних посягань та транскордонного збору доказів. Особливу увагу приділено новій всесвітній конвенції, яка покликана стати єдиною глобальною платформою для взаємної правової допомоги та обміну цифровими даними між країнами з різними правовими системами.

Систематизовано ключові правові виклики та системні перешкоди, які знижують ефективність чинних міжнародних механізмів. До них віднесено гострі юрисдикційні колізії, складність узгодження принципу подвійної кримінальності, технічні бар'єри при вилученні даних із хмарних сховищ, а також ризики порушення фундаментальних прав людини та використання розмитих юридичних формулювань авторитарними режимами для політичних переслідувань і цензури під виглядом боротьби з екстремізмом. Також виявлено суттєвий матеріально-технічний і регуляторний розрив між державами, що перешкоджає оперативному обміну інформацією.





Обґрунтовано, що для забезпечення безпеки цифрового простору міжнародне право має діяти проактивно. Сформульовано висновки про необхідність прискорення ратифікаційних процесів, створення дієвих моніторингових інституцій та розробки додаткових протоколів, які регулюватимуть використання штучного інтелекту в кримінальному процесі, обіг віртуальних активів і протидію синтетичному шахрайському контенту. Визначено перспективні напрями подальших наукових розвідок у контексті подолання геополітичної фрагментації та зміцнення міжнародної солідарності на засадах верховенства права.

Ключові слова: транснаціональна організована злочинність, електронні докази, взаємна правова допомога, юрисдикційні конфлікти, цифрові загрози, штучний інтелект у злочинності, публічно-приватне партнерство, глобальна кіберстійкість, універсальні правові стандарти.

Рупіак Mykola Ivanovych Candidate of Juridical Sciences, Associate Professor, Associate Professor of the Department of Law, Vinnytsia Institute of Trade and Economics of the State University of Trade and Economics, Vinnytsia, <https://orcid.org/0000-0001-9133-6762>

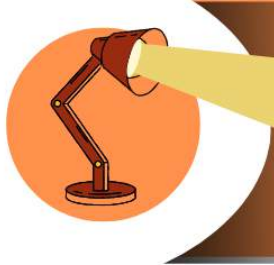
INTERNATIONAL LEGAL ASSISTANCE AND COOPERATION IN COUNTERING CYBERCRIME: CHALLENGES OF THE DIGITAL AGE

Abstract. The article provides a comprehensive theoretical and legal analysis of the formation, current state, and development prospects of international cooperation in the field of combating cybercrime. It is determined that unlawful acts in the information space have outgrown the level of isolated offenses and transformed into a high-tech transnational industry. This criminal activity increasingly functions as a coordinated shadow business that provides illicit services on demand, involves artificial intelligence tools for automating attacks, and merges with other dangerous forms of organized crime, including human trafficking, corruption schemes, and money laundering.

The paper examines in detail the evolution of the international regulatory and legal framework, which has progressed from regional initiatives of individual states to the development and adoption of a universal treaty under the auspices of the United Nations. A comparative analysis of legal instruments that laid the foundations for the criminalization of computer system encroachments and cross-border evidence collection is conducted. Special attention is paid to the new global convention, which is designed to become a single global platform for mutual legal assistance and digital data exchange between countries with different legal systems.

The key legal challenges and systemic obstacles that reduce the effectiveness of existing international mechanisms are systematized. These include acute jurisdictional





conflicts, the complexity of reconciling the principle of double criminality, technical barriers in extracting data from cloud storage, as well as the risks of violating fundamental human rights and the use of vague legal formulations by authoritarian regimes for political persecution and censorship under the guise of combating extremism. A significant material, technical, and regulatory gap between states that hinders the timely exchange of information is also identified.

It is substantiated that to ensure the security of the digital space, international law must act proactively. Conclusions are formulated on the need to accelerate ratification processes, create effective monitoring institutions, and develop additional protocols that will regulate the use of artificial intelligence in criminal proceedings, the circulation of virtual assets, and the counteraction to synthetic fraudulent content. Prospective directions for further scientific research are identified in the context of overcoming geopolitical fragmentation and strengthening international solidarity based on the rule of law.

Keywords: transnational organized crime, electronic evidence, mutual legal assistance, jurisdictional conflicts, digital threats, artificial intelligence in crime, public-private partnership, global cyber resilience, universal legal standards.

Постановка проблеми. Цифрова трансформація суспільних відносин кардинально змінила природу злочинності, надавши їй транснаціонального, високотехнологічного та комерціалізованого характеру. Кіберзлочинність сьогодні виступає не лише як окремий вид правопорушень, а й як каталізатор гібридних загроз, що поєднують кримінальні, економічні та геополітичні елементи. Актуальність теми зумовлена експоненційним зростанням масштабів кіберінцидентів, поширенням моделей «злочинність як послуга», інтеграцією штучного інтелекту в злочинні схеми та стрімким старінням традиційних правових інструментів.

Наукова новизна дослідження полягає в комплексному критичному аналізі еволюції міжнародно-правових механізмів після ухвалення Конвенції ООН проти кіберзлочинності 24 грудня 2024 р. у контексті балансу між ефективністю правоохоронної діяльності та захистом прав людини в умовах геополітичної фрагментації.

Мета статті виявити системні виклики міжнародно-правової допомоги у сфері протидії кіберзлочинності та науково обґрунтувати напрями її оптимізації у цифрову епоху.

Аналіз останніх досліджень і публікацій. Питання формування дієвих механізмів протидії правопорушенням в інформаційній сфері перебувають у центрі уваги багатьох сучасних науковців. Зокрема, у дослідженнях О. О. Кожушка, Л. М. Товпиги та В.О. Бабіної проаналізовано ключові інструменти протидії інформаційним злочинам на рівні міжнародного права. Процес пристосування





кримінального законодавства до викликів цифрової ери висвітлено у працях М. І. Краська та А. І. Цевух, а вагомий внесок у визначення загальних міжнародно-правових рамок безпеки віртуального простору зробили С. Б. Карвацька, А. З. Маник та М. І. Строїч. Праці цих учених заклали надійне теоретичне підґрунтя для розуміння природи сучасних загроз, проте поза увагою дослідників усе ще залишається комплексний аналіз системних суперечностей між прагненням до уніфікації транскордонного збору цифрових даних та ризиками порушення фундаментальних прав людини в умовах геополітичної фрагментації.

Виклад основного матеріалу дослідження. Дослідження міжнародно-правового виміру протидії протиправним діям у кіберпросторі вимагає переосмислення традиційних доктринальних підходів до розуміння суверенних повноважень держав та інституційного наповнення правової допомоги. Сучасний етап розвитку глобального інформаційного суспільства характеризується детериторіалізацією правопорушень, коли архітектура цифрових мереж нівелює класичне географічне та політичне зонування. Як наслідок, правова реальність зіштовхується із парадоксом: суверенна правоохоронна та судова юрисдикція залишається обмеженою державними кордонами, тоді як об'єктивна сторона кіберзлочинів розгортається у транскордонній віртуальній площині. Це зумовлює об'єктивну неможливість ефективного автономного реагування на цифрові загрози з боку окремо взятої національної правової системи та виводить інститути взаємної правової допомоги на рівень стратегічного елемента забезпечення міжнародної безпеки. Системний аналіз цієї проблематики потребує першочергового розмежування сутнісних характеристик об'єкта правового регулювання, його динамічної еволюції під впливом технологічного прогресу та вивчення ієрархії нормативних інструментів, що покликані регламентувати міжнародну взаємодію у цій специфічній сфері.

Кіберзлочинність являє собою складне соціально-правове явище, яке охоплює будь-які протиправні діяння, що вчиняються з використанням інформаційно-комунікаційних технологій або спрямовані проти них. На відміну від традиційної злочинності, вона не обмежується фізичним простором і не залежить від територіальних кордонів. Будапештська конвенція 2001 року визначає її через чотири основні групи діянь: злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; комп'ютерно-спрямовані злочини (наприклад, шахрайство); злочини, пов'язані зі змістом даних (дитяча порнографія, розпалювання ненависті); та порушення авторських прав. Сучасне розуміння, закріплене в Конвенції ООН 2024 року, є значно ширшим і включає як «кіберзалежні» злочини (вчинені виключно завдяки ІКТ), так і «кіберспрямовані» (традиційні злочини, вчинені за допомогою цифрових технологій, - відмова коштів, торгівля людьми, тероризм, відмивання грошей) [1].

Сьогодні кіберзлочинність характеризується високою латентністю, надзвичайною швидкістю вчинення та поширення, низьким рівнем ризику для злочинця

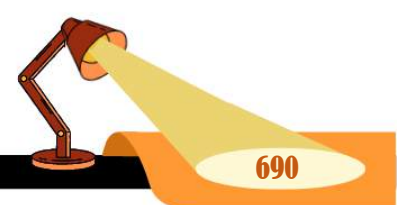




завдяки анонімізації, а також глобальним масштабом наслідків. Вона еволюціонувала від поодиноких актів хакерства до розвиненої транснаціональної індустрії, яка працює за бізнес-моделлю «злочинність як послуга» (Cybercrime-as-a-Service). На підпільних ринках доступні ransomware-пакети, фішингові набори, інструменти для створення deepfakes, ботнети та навіть «кібермерсепарії», що надають послуги з DDoS-атак, шпигунства чи зламу систем. Особливо небезпечним є злиття кіберзлочинності з іншими формами організованої злочинності — торгівлею людьми, наркоторгівлею та корупцією, що спостерігається, зокрема, у scam-центрах Південно-Східної Азії. Використання штучного інтелекту дозволяє автоматизувати атаки, створювати персоналізований шахрайський контент і обхід систем захисту, що значно підвищує їхню ефективність і знижує поріг входу для нових учасників. Отже, кіберзлочинність перетворилася на одну з найбільш динамічних і руйнівних загроз сучасності, яка підриває економічну стабільність держав, довіру до цифрових систем, захист персональних даних і національну безпеку в цілому.

Формування міжнародно-правової допомоги в сфері протидії кіберзлочинності пройшло тривалий і нерівномірний шлях від фрагментарних ініціатив окремих держав і регіональних організацій до спроб створення дійсно універсальної системи регулювання. Першим спеціалізованим багатостороннім договором, який заклав фундаментальні стандарти, стала Конвенція Ради Європи про кіберзлочинність, відома як Будапештська конвенція, ухвалена 2001 року. Цей документ запровадив уніфіковані підходи до криміналізації основних видів кіберправопорушень, таких як незаконний доступ до комп'ютерних систем, перехоплення даних, пошкодження або знищення інформації, а також передбачив комплекс процесуальних повноважень для слідчих органів і механізми взаємної правової допомоги, екстрадиції та збереження доказів. Станом на 2026 рік конвенцію ратифікували понад 80 держав, серед яких не лише європейські країни, а й низка держав з інших континентів, що свідчить про її значний глобальний вплив. Другий додатковий протокол 2022 року суттєво розширив практичні можливості доступу до електронних доказів, особливо в хмарних середовищах, запровадивши механізми прямої співпраці з провайдерами послуг і процедури швидкого збереження даних, що стало відповіддю на стрімкий розвиток технологій зберігання інформації за кордоном [2].

Важливим етапом універсалізації регулювання стало ухвалення Генеральною Асамблеєю ООН Конвенції проти кіберзлочинності 24 грудня 2024 року (резолюція 79/243). Цей документ, відкритий для підписання з жовтня 2025 року в Ханой, а згодом у Нью-Йорку, встановлює широкі стандарти криміналізації злочинів, скоєних із використанням інформаційно-комунікаційних технологій, і детально регламентує механізми обміну електронними доказами для тяжких злочинів. Станом на квітень 2026 року конвенцію підписали 74 держави,

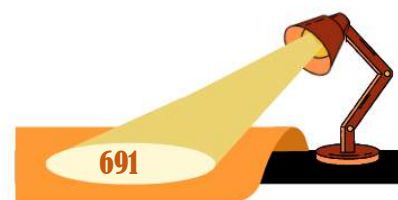




включаючи як традиційних лідерів у сфері кібербезпеки, так і країни, що розвиваються; ратифікували її Катар і В'єтнам. Хоча для набрання чинності ще необхідно досягти 40 ратифікацій, документ уже формує глобальну платформу, яка доповнює регіональні інструменти. Паралельно з формальними договірними механізмами активно розвивається оперативна координація через структури Європолу, зокрема Європейський центр з кіберзлочинності, та Інтерпол, які реалізують масштабні спільні операції, спрямовані на вимкнення інфраструктури злочинних сервісів як послуги. Ці ініціативи демонструють, як нормативна база поєднується з практичними діями, створюючи багаторівневу систему міжнародної допомоги, здатну реагувати на динамічні загрози цифрового середовища [3].

Сучасна кіберзлочинність еволюціонувала в потужну транснаціональну індустрію, яка функціонує за чіткою бізнес-моделлю і генерує прибутки, співставні з ВВП окремих держав. Звіти UNODC та Європолу за 2025–2026 роки фіксують стрімке поширення моделі «злочинність як послуга», коли на підпільних ринках пропонуються готові інструменти для здійснення ransomware-атак, фішингових кампаній, створення deepfake-контенту та автоматизованих інструментів на базі штучного інтелекту. Особливо небезпечним явищем стало злиття кіберзлочинності з іншими формами транснаціональної організованої злочинності, зокрема торгівлею людьми в так званих scam-центрах Південно-Східної Азії, де примусова праця тисяч осіб генерує мільярдні прибутки через масові шахрайські схеми. Така структурна трансформація радикально ускладнює традиційні методи кримінального розслідування, оскільки елементи одного злочину можуть бути розподілені між численними юрисдикціями на різних континентах, а анонімізація через криптовалюти, мережі Tor і численні проксі-сервери суттєво знижує ефективність національних правоохоронних органів. Унаслідок цього кіберзлочинність все частіше набуває ознак гібридної загрози, що поєднує кримінальні дії з елементами економічного шантажу, політичного впливу та дестабілізації суспільства, вимагаючи не лише суто кримінально-правової, але й комплексної політико-правової та дипломатичної відповіді на міжнародному рівні [4].

Однією з центральних і найбільш складних проблем, що суттєво обмежує ефективність міжнародно-правової допомоги, залишається подолання юрисдикційних конфліктів і колізій. Кіберзлочин, скоєний у віртуальному просторі, часто зачіпає інтереси кількох держав одночасно, причому національні законодавства по-різному кваліфікують одні й ті самі діяння та встановлюють відмінні вимоги до допустимості доказів. Принцип подвійної кримінальності, який традиційно лежить в основі взаємної правової допомоги, у багатьох випадках стає перешкодою, оскільки запитувана держава може відмовити у співпраці, якщо діяння не є злочином за її законодавством. Обмін електронними доказами ускладнюється не





лише величезним обсягом даних, їхньою швидкою втратою або видаленням, але й особливостями зберігання в хмарних сервісах, розташованих у третіх країнах. Конвенція ООН намагається врегулювати ці питання через спеціальні механізми, проте відсутність повністю уніфікованих стандартів допустимості доказів у різних правових сім'ях - континентальній та англо-саксонській - суттєво знижує практичну ефективність. Додаткові труднощі створюють технології end-to-end шифрування та перспективні квантові загрози, які можуть повністю знецінити традиційні методи отримання доказів, змушуючи правоохоронні органи шукати нові технічні та правові рішення.

Забезпечення балансу між ефективністю боротьби зі злочинністю та захистом фундаментальних прав людини виступає одним із найбільш критичних імперативів сучасного міжнародного кіберспівробітництва. Широке формулювання положень Конвенції ООН, особливо щодо визначення «серйозних злочинів», викликають обґрунтовані занепокоєння правозахисних організацій щодо потенційного зловживання авторитарними режимами. Такі держави можуть використовувати нові механізми обміну даними для політичних переслідувань інакомислення, цензури чи моніторингу опозиції під виглядом боротьби з екстремізмом або дезінформацією. Відсутність чітких і обов'язкових механізмів судового контролю, принципу пропорційності та прозорості доступу до даних посилює ці ризики. У цьому контексті особливо важливим стає посилення ролі регіональних правозахисних стандартів, таких як Європейська конвенція з прав людини, а також активна участь незалежного громадянського суспільства в моніторингу імплементації міжнародних зобов'язань, щоб запобігти перетворенню інструментів боротьби зі злочинністю на інструменти обмеження свобод [5].

Значна частина кіберінцидентів виявляється саме приватним сектором - технологічними компаніями, фінансовими установами та провайдерами послуг, що робить публічно-приватне партнерство стратегічно важливим елементом ефективної протидії. Однак регуляторні розбіжності між різними регіонами, зокрема жорсткі вимоги GDPR в Європейському Союзі порівняно з більш ліберальними підходами в інших частинах світу, створюють суттєві бар'єри для оперативного обміну даними. Країни Глобального Півдня стикаються з хронічним дефіцитом фінансових ресурсів, технічної експертизи та сучасної інфраструктури, що значно посилює глобальну асиметрію кіберстійкості та робить їх особливо вразливими до транснаціональних злочинних мереж. Програми розбудови потенціалу (capacity building), які реалізують UNODC та Інтерпол, безумовно корисні, проте їхній поточний масштаб і охоплення ще недостатні для подолання цифрового розриву між державами [4].

Перспективи подальшого розвитку міжнародно-правової допомоги у сфері протидії кіберзлочинності мають комплексний і багатовимірний характер,





зумовлений динамікою технологічного прогресу та зростанням глобальної взаємозалежності держав. Насамперед вони пов'язані з необхідністю прискорення процесу ратифікації Конвенції ООН проти кіберзлочинності, що дозволить трансформувати її з декларативного інструменту у повноцінний універсальний правовий механізм. Важливим інституційним кроком у цьому контексті є створення ефективного, постійно діючого механізму Конференції держав-учасниць, яка повинна виконувати не лише координаційну, а й моніторингову, інтерпретаційну та нормотворчу функції, забезпечуючи уніфіковане застосування положень Конвенції [6].

Особливого значення набуває розробка та ухвалення додаткових протоколів, спрямованих на врегулювання новітніх технологічних феноменів. Йдеться, зокрема, про використання штучного інтелекту у злочинній діяльності та кримінальному процесі, обіг криптоактивів як інструменту фінансування кіберзлочинності, а також технології створення синтетичного контенту (deepfake), що породжують нові форми правопорушень і суттєво ускладнюють процес доказування. У цьому аспекті міжнародне право має діяти проактивно, випереджаючи появу нових загроз, а не лише реагуючи на них постфактум [7, с. 146].

Отже, комплексний аналіз сучасних міжнародно-правових механізмів засвідчує, що архітектура глобальної протидії кіберзлочинності перебуває у стані глибокої трансформації, зумовленої необхідністю адаптації до викликів цифрової епохи. Ухвалення Конвенції ООН проти кіберзлочинності у грудні 2024 року заклало підвалини для формування універсальних правових стандартів, проте її реальний потенціал залишається заручником геополітичної фрагментації та техніко-юридичних розбіжностей між державами. Накладення новітніх технологічних ризиків, таких як автоматизація атак за допомогою штучного інтелекту та анонімізація фінансових потоків через віртуальні активи, на класичні правові проблеми – юрисдикційні конфлікти й дотримання принципу подвійної кримінальності – вимагає від міжнародного співтовариства переходу до проактивної та гнучкої моделі правотворчості. Ефективність взаємної правової допомоги у довгостроковій перспективі залежатиме не лише від формальної кількості ратифікацій нових договорів, а й від спроможності держав збалансувати інтереси національної безпеки із неухильним дотриманням фундаментальних прав людини.

Висновки. Проведене дослідження дозволяє сформулювати такі основні висновки. По-перше, міжнародно-правова допомога та співробітництво є необхідною, але недостатньою умовою ефективної протидії кіберзлочинності в цифрову епоху, оскільки без постійної адаптації до нових технологій навіть найпрогресивніші договори швидко втрачають актуальність. По-друге, Конвенція ООН 2024 року створює важливу універсальну основу для глобальної координації, проте її практична ефективність залежатиме від швидкості ратифікації, якості





національної імплементації та наявності дієвих гарантій захисту прав людини. По-третє, ключовими системними перешкодами залишаються юрисдикційні колізії, проблеми трансграничного доказування, технологічний розрив між державами та ризики зловживань владними повноваженнями.

Перспективи подальших наукових досліджень пов'язані з емпіричним моніторингом практики застосування нової Конвенції після набрання нею чинності, розробкою рекомендацій щодо інтеграції штучного інтелекту в кримінально-процесуальну діяльність, аналізом впливу геополітичної фрагментації на рівень довіри між державами та оцінкою ефективності програм розбудови потенціалу для країн, що розвиваються. Лише через постійну адаптацію правових інструментів, зміцнення міжнародної солідарності та дотримання принципів верховенства права можливо забезпечити відносну безпеку цифрового простору в умовах швидких технологічних змін.

Література:

1. Конвенція Організації Об'єднаних Націй проти кіберзлочинності: резолюція Генеральної Асамблеї ООН від 24 грудня 2024 р. № 79/243. URL: <https://www.unodc.org/unodc/en/cybercrime/convention/home.html> (дата звернення: 15.04.2026).
2. Конвенція про кіберзлочинність: підписана в Будапешті 23 листопада 2001 р. (ETS № 185). URL: <https://rm.coe.int/1680081561> (дата звернення: 17.04.2026).
3. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2025. Luxembourg: Publications Office of the European Union, 2025. 112 p.
4. United Nations Office on Drugs and Crime. What to know about cybercrime in 2026. Vienna: UNODC, 2025. 48 p. URL: <https://www.unodc.org/unodc/frontpage/2025/October/what-to-know-about-cybercrime-in-2025.html> (дата звернення: 15.04.2026).
5. World Economic Forum. Global Cybersecurity Outlook 2026. Geneva: WEF, 2026. 84 p.
6. Hakmeh J. The UN convention on cybercrime: a milestone or a missed opportunity? Journal of Cyber Policy. 2024. Vol. 9, No. 3. P. 245–262. DOI: <https://doi.org/10.1080/23738871.2024.2441549> (дата звернення: 21.04.2026).
7. Саєнко М. І. Міжнародно-правове регулювання протидії кіберзлочинності: сучасні виклики та перспективи. *Вісник Національної академії правових наук України*. 2024. Т. 31, № 4. С. 145–162.
8. Кожушко, О. О., Товпи́га, Л. М., Ба́біна, В. О. Механізми протидії інформаційним злочинам у цифрову епоху на рівні міжнародного права. *Український політико-правовий дискурс*. 2026. № 19. URL: <https://ppdnz.com.ua/index.php/home/article/view/511/409> (дата звернення: 25.04.2026).

References:

1. United Nations General Assembly. (2024, December 24). *Konventsiiia Orhanizatsii Obiednanykh Natsii proty kiberzlochynnosti: rezoliutsiia Heneralnoi Asamblei OON № 79/243* [United Nations Convention Against Cybercrime: UN General Assembly resolution No. 79/243]. Retrieved from <https://www.unodc.org/unodc/en/cybercrime/convention/home.html> [in Ukrainian].





2. Council of Europe. (2001, November 23). *Konventsiiia pro kiberzlochynnist* [Convention on Cybercrime] (ETS No. 185). Retrieved from <https://rm.coe.int/1680081561> [in Ukrainian].
3. Europol. (2025). *Internet Organised Crime Threat Assessment (IOCTA) 2025*. Luxembourg: Publications Office of the European Union.
4. United Nations Office on Drugs and Crime. (2025). *What to know about cybercrime in 2026*. Vienna: UNODC. Retrieved from <https://www.unodc.org/unodc/frontpage/2025/October/what-to-know-about-cybercrime-in-2025.html>.
5. World Economic Forum. (2026). *Global Cybersecurity Outlook 2026*. Geneva: WEF.
6. Hakmeh, J. (2024). The UN convention on cybercrime: a milestone or a missed opportunity? *Journal of Cyber Policy*, 9(3), 245–262. <https://doi.org/10.1080/23738871.2024.2441549>.
7. Saienko, M. I. (2024). Mizhnarodno-pravove rehuliuвання protydii kiberzlochynnosti: suchasni vyklyky ta perspektyvy [International legal regulation of combating cybercrime: current challenges and prospects]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy – Journal of the National Academy of Legal Sciences of Ukraine*, 31(4), 145–162 [in Ukrainian].
8. Kozhushko, O. O., Tovpyha, L. M., & Babina, V. O. (2026). Mekhanizmy protydii informatsiynym zločynam u tsyfrovu epokhu na rivni mizhnarodnoho prava [Mechanisms of countering information crimes in the digital era at the level of international law]. *Ukrainskyi polityko-pravovyi dyskurs – Ukrainian Political and Legal Discourse*, 19. Retrieved from <https://ppdnz.com.ua/index.php/home/article/view/511/409> [in Ukrainian].

Дата першого надходження статті до видання: 02.05.2026

Дата прийняття статті до друку після рецензування: 17.05.2026

