МІЖНАРОДНЕ ПРАВО

УДК 343.1
DOI https://doi.org/10.32844/2618-1258.2024.4.55

ВАРЕНИК О.С.

МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ГЛОБАЛІЗАЦІЇ

INTERNATIONAL LEGAL REGULATION OF CYBERCRIME IN THE CONTEXT OF GLOBALIZATION

Актуальність дослідження обумовлена інтенсивним безперервним зростанням кіберзлочинності, яка перетворилася на одну з найсерйозніших загроз міжнародній безпеці, економічній стабільності та правам людини за останні десятиліття. Метою статті є теоретико-правовий аналіз міжнародно-правового регулювання кіберзлочинності в умовах глобалізації. У статті проаналізовано теоретико-правову сутність поняття кібербезпеки та кіберзлочинності. Розкрито роль кібербезпеки як ключового елемента в міжнародно-правовому регулюванні кіберзлочинності, що включає запобігання, виявлення та реагування на злочини у кіберпросторі. Досліджено наукові позиції щодо понятійно-категоріального апарату. Охарактеризовано специфіку кіберзлочинності як міжнародного явища. Детально розглянуто основні міжнародні нормативно-правові акти, що регулюють боротьбу з кіберзлочинністю. Автором почергово розкрито їх специфіку, наведено характеристику кожного з них. Аргументовано авторську позицію щодо їхньої ефективності у контексті глобалізаційних змін. Обґрунтовано позицію щодо необхідності розробки нових правових механізмів для масштабної протидії сучасним кіберзагрозам, включаючи кібершпигунство, фінансові шахрайства та атаки на критичну інфраструктуру задля забезпечення міжнародного правопорядку в умовах цифрової епохи. Зроблено висновок, що кібербезпека забезпечує правові, технічні та організаційні рамки, в межах яких можливе створення ефективних механізмів міжнародного співробітництва, захисту прав людини та підтримання глобальної стабільності в умовах цифрового світу. Кіберзлочинність є однією з найсерйозніших загроз сучасному міжнародному правопорядку, яка суттєво впливає на економічну, соціальну та інформаційну стабільність у глобальному масштабі. Транснаціональний характер цієї злочинності, а також її здатність швидко адаптуватися до новітніх технологій створює значні виклики для традиційних правових систем і потребує системного та скоординованого міжнародного реагування. Лише через ефективну координацію зусиль держав, міжнародних організацій, приватного сектору та громадянського суспільства можливо забезпечити стійкість глобального кіберпростору, захист прав людини та економічну стабільність у світі.

Ключові слова: *кіберзлочинність, міжнародне право, глобалізація, кібербезпека, транснаціональні злочини, правове регулювання.*

The relevance of the study is due to the intensive continuous growth of cybercrime, which has become one of the most serious threats to international security, economic stability and human rights in recent decades. The purpose of the article is a theoretical and legal analysis of the international legal regulation of cybercrime in the context of

© ВАРЕНИК О.С. – доктор юридичних наук, професор кафедри міжнародного та європейського права факультету міжнародних відносин (Національний авіаційний університет)

globalization. The article analyzes the theoretical and legal essence of the concepts of cybersecurity and cybercrime. The role of cybersecurity as a key element in the international legal regulation of cybercrime is revealed, which includes the prevention, detection and response to crimes in cyberspace. Scientific positions on the conceptual and categorical apparatus are studied. The specifics of cybercrime as an international phenomenon are characterized. The main international regulatory legal acts regulating the fight against cybercrime are considered in detail. The author reveals their specifics in turn, provides a characteristic of each of them. The author's position on their effectiveness in the context of globalization changes is argued. The position on the need to develop new legal mechanisms for large-scale counteraction to modern cyber threats, including cyber espionage, financial fraud and attacks on critical infrastructure in order to ensure international law and order in the digital age is substantiated. It is concluded that cybersecurity provides a legal, technical and organizational framework within which it is possible to create effective mechanisms for international cooperation, protect human rights and maintain global stability in the digital world. Cybercrime is one of the most serious threats to the modern international legal order, which significantly affects economic, social and informational stability on a global scale. The transnational nature of this crime, as well as its ability to quickly adapt to new technologies, creates significant challenges for traditional legal systems and requires a systematic and coordinated international response. Only through effective coordination of efforts of states, international organizations, the private sector and civil society can it be possible to ensure the stability of global cyberspace, the protection of human rights and economic stability in the world.

Key words: *cybercrime, international law, globalization, cybersecurity, transnational crimes, legal regulation.*

Постановка проблеми. У сучасних умовах глобалізації кіберзлочинність стала однією з найсерйозніших загроз міжнародній безпеці, економічній стабільності та правам людини. Сучасне міжнародне право має бути адаптоване до умов цифрової епохи, що вимагає створення нових підходів до правового регулювання, зокрема щодо транскордонного переслідування кіберзлочинців, екстрадиції та визначення юрисдикції. З розвитком цифрових технологій, що інтегруються у всі сфери суспільного життя, масштаби кіберзлочинності постійно зростають.

Так, кіберзлочинність та кібертероризм загрожують мирному існуванню людства та використанню кіберпростору у суспільно корисних цілях. У зв'язку з чим вкрай актуальним постає питання міжнародного співробітництва з метою забезпечення кібермиру та підтримання кіберстабільності на основі норм та принципів міжнародного права [1, с. 179]. Інтернет став невід'ємною та важливою частиною нашого суспільства та економіки. 80 % молоді в Європі підтримують зв'язок один з одним та світом завдяки соціальним онлайн мережам, а щорічний товарообіг електронної торгівлі становить 8 трлн. доларів. Проте із зростанням діяльності онлайн, зростає і кількість кримінальних злочинів – більш як один мільйон осіб по всьому світу стають щодня жертвами кіберзлочинності. Кримінальна діяльність онлайн включає цілу низку дій: від продажу викрадених кредитних карток за лише 1 євро, до викрадення особистих даних та сексуальної експлуатації дітей, включаючи серйозні кібератаки проти державних та європейських інститутів або інфраструктури [2, с. 144]. У 2023 році середня вартість витоку даних досягла рекордних 4,45 млн доларів США, а вартість інцидентів, пов'язаних із програмами-вимагачами, перевищила 5 млн доларів, що підтверджує високу економічну ціну недостатньої кібербезпеки. Прогнозовані збитки для світової економіки у 10,5 трильйонів доларів США на рік до 2025 року вказують на те, що кіберзлочинність перетворюється на одну з найзначущіших загроз глобальному економічному порядку [3]. Щоденне збільшення кількості жертв кіберзлочинності вимагає адекватної реакції з боку міжнародного співтовариства. Проблема полягає у тому, що традиційні правові механізми регулювання злочинів у фізичному світі не можуть ефективно застосовуватися в кіберпросторі через його транснаціональний характер, децентралізовану природу та відсутність фізичних кордонів. Кіберпростір надає злочинцям можливість діяти анонімно, здійснювати атаки з території однієї держави на інші юрисдикції та уникати відповідальності, використовуючи слабкі місця в законодавстві окремих країн.

Стан дослідження. У тій чи іншій мірі проблематики міжнародно-правового регулювання кіберзлочинності в умовах глобалізації стосувалися праці таких вчених: 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, М.В. Копійка, М.М. Кравчук, А.І. Марущак, Н.В. Савчук, Є.Д. Скулиш, Н.І. Хавронюк, Ю.С. Шемшученко та ін. Все ж, не применшуючи їх внеску у розвиток науки міжнародного права, доцільно відмітити, що дана проблематика є надзвичайно актуальною, оскільки досі не є усталеною та динамічно розвивається в умовах інтенсивного науково-технічного прогресу.

Метою статті є теоретико-правовий аналіз міжнародно-правового регулювання кіберзлочинності в умовах глобалізації.

Виклад основного матеріалу. У сучасному глобалізованому світі разом з інноваційними технологіями виникають і нові види злочинів, що, по суті є закономірним явищем. Використання та удосконалення сфери інформаційних технологій спричинило появу кіберзлочинності – характерного наслідку глобалізації інформаційних процесів. І тому, як вірно відмічає М.І. Саєнко, кіберзлочинність стала загрозою не лише для окремих осіб, а й для держав, оскільки передбачає руйнування економічної та інформаційної сфер. Характерні ознаки кіберзлочинності приваблюють людство, що означає, у свою чергу, збільшення кількості осіб, що чинять протиправну діяльність. Більшість методів соціальної інженерії не вимагають особливих технічних знань з боку зловмисників, а отже використовувати ці методи може будь-хто — від дрібних злодіїв до досвідчених кіберзлочинців [4, с. 387].

У рамках розгляду кіберзлочинності як міжнародно-правового феномену кібербезпека відіграє роль фундаментального елемента. Адже саме через забезпечення кібербезпеки можливо ефективно протидіяти таким явищам, як кібершпигунство, крадіжка інтелектуальної власності, фінансові шахрайства, поширення шкідливого програмного забезпечення та навіть кібератаки на критичну інфраструктуру. Ці злочини не лише завдають шкоди окремим особам чи компаніям, але й мають потенціал підривати стабільність цілих держав та регіонів. Так, кібербезпека є ключовим елементом міжнародно-правового регулювання кіберзлочинності, адже саме вона формує основу для попередження, виявлення та реагування на злочини в кіберпросторі. Західні науковці, визначаючи кібербезпеку як багатовимірне поняття, що охоплює захист інформації, технологій, користувачів та їхніх інтересів, пропонують підхід, який можна інтегрувати у контекст глобалізації та викликів міжнародного права [5, с. 101]. У контексті міжнародного права кібербезпека може слугувати інструментом забезпечення глобальної стабільності, оскільки будь-яка вразливість у кіберпросторі має потенціал перерости у транснаціональні загрози. Глобалізація створила умови для посилення залежності міждержавних відносин від цифрової інфраструктури, що, у свою чергу, посилює актуальність забезпечення кібербезпеки як превентивного заходу проти кіберзлочинності. Зокрема, інтеграція міжнародних стандартів з кібербезпеки у національні правові системи може забезпечити узгоджений підхід до розслідування кіберзлочинів, екстрадиції підозрюваних та захисту жертв. Під терміном кібербезпека в науці міжнародного права, як зазначає О.О. Грицун, часто розуміють «методи, технічні засоби та технології, що використовуються людьми з метою запобігання, виявлення і відновлення в разі нанесення шкоди конфіденційності, цілісності та доступності інформації в кіберпросторі. Кібербезпека стоїть на захисті критичної інфраструктури», або ж «запобігання пошкодженню, захист і відновлення комп'ютерів, електронних систем зв'язку, електронних послуг зв'язку, дротового зв'язку та електронних засобів зв'язку, в тому числі інформації, що там міститься з метою забезпечення її доступності, цілісності, автентичності, конфіденційність і непідробленості» [6, с. 17–18]. Досліджуючи кібербезпеку, важливо враховувати також її взаємозв'язок з правами людини та суверенітетом держав. З одного боку, держава повинна забезпечити кібербезпеку своїх громадян, захищаючи їхню приватність, персональні дані та свободу вираження поглядів. З іншого боку, надмірна регламентація з боку держави може спричинити ризики порушення цих прав. Таким чином, міжнародно-правове регулювання має спрямовуватися на створення балансу між безпекою та свободою, враховуючи глобальні виклики та національні особливості.

Загалом, науковці різних країн пропонують різноманітні підходи до визначення кібербезпеки, відображаючи специфіку національних стратегій та підходів до забезпечення інформаційної безпеки. У французькій документації кібербезпека трактується як «бажаний стан інформаційної системи, який дозволяє їй протистояти загрозам із кіберпростору, що можуть поставити під загрозу доступність, цілісність чи конфіденційність даних, які зберігаються, обробляються чи передаються, а також послуг, які забезпечуються цими системами або надаються ними в доступ». У німецькій стратегії цей термін охоплює «комплекс необхідних та відповідних заходів, що дозволяють мінімізувати ризики, пов'язані з використанням інформаційних і комунікаційних

технологій». Канадські дослідники, у свою чергу, акцентують увагу на кібербезпеці як «захисті кіберсистем від шкідливого використання чи деструктивних атак», що підкреслює важливість попередження злочинних дій. Турецькі вчені наголошують на тому, що кібербезпека полягає в «захисті інформаційних систем, які функціонують у межах кіберпростору, від атак, забезпеченні конфіденційності, цілісності та доступності інформації, а також у виявленні та протидії кіберінцидентам». Нідерландський підхід визначає кібербезпеку як "сукупність заходів, спрямованих на запобігання збиткам, що можуть виникнути через збої в роботі інформаційно-комунікаційних технологій або їх неналежне використання, а також на відновлення цих технологій після реалізації загроз» [7, с. 315].

Вищенаведені визначення ілюструють, що кібербезпека розглядається багатогранно: як стан системи, як комплекс заходів для мінімізації ризиків, як захист від атак або як відновлення після інцидентів. Відповідний різноманітний підхід вказує на складність і багатовимірність цього явища, а також про необхідність інтеграції політичних, технічних, правових та організаційних інструментів для забезпечення ефективного функціонування кіберпростору. Визначення з різних країн акцентують увагу на універсальних принципах конфіденційності, цілісності та доступності, що є фундаментальними для міжнародно-правового регулювання сфери кіберзлочинності.

Таким чином, аспект кібербезпеки при розгляді міжнародно-правового регулювання кіберзлочинності є критично важливим з кількох причин. По-перше, кібербезпека забезпечує технічну та правову базу для створення механізмів запобігання кіберзлочинам. По-друге, вона дозволяє формувати єдиний підхід до розслідування кіберзлочинів на міжнародному рівні. По-третє, вивчення кібербезпеки розширює можливості для запобігання ескалації конфліктів у кіберпросторі, зокрема шляхом встановлення «червоних ліній» у міжнародному праві.

У свою чергу, під поняттям «кіберзлочину», на думку Н.С. Никончук та О.О. Маслової доцільно розуміти соціальне явище, що являє собою навмисну мотивовану атаку з використанням мережі Інтернет на інформацію в комп'ютерній системі, програми або дані, що чиниться окремою особою або угрупуваннями, яке має суспільну небезпеку для суспільного ладу України, його політичної й економічної системи, власності, особі, політичним, трудовим, майновим та іншім правам і свободам громадян [8, с. 203]. Таким чином, можна констатувати, що використання Інтернету як засобу для вчинення злочинів, зокрема через доступ до персональних даних, поширення шкідливого програмного забезпечення або використання методів соціальної інженерії, ставить під загрозу право на приватність, інформаційну безпеку та свободу слова. Міжнародне право має передбачити створення механізмів правового захисту громадян, які стали жертвами таких злочинів, зокрема через обов'язкову імплементацію державами-членами міжнародних стандартів кібербезпеки. Також особливої уваги заслуговує визначення кіберзлочинності як явища, що охоплює як індивідуальні, так і організовані форми злочинної діяльності. У цьому контексті особливого значення набуває розробка механізмів притягнення до відповідальності не лише індивідів, але й організованих угруповань, які використовують кіберпростір для досягнення своїх злочинних цілей.

Але саме в міжнародному контексті варто зазначити, що поняття «кіберзлочинність» як правовий феномен зародилося в умовах стрімкого розвитку інформаційних технологій, що наприкінці XX століття трансформували глобальну правову реальність. Вперше з'явившись у середині 70-х років у США, кіберзлочинність вже на початкових етапах свого існування продемонструвала не лише нові можливості для зловмисників, але й суттєві виклики для традиційних правових систем. Історичний прецедент 1973 року, коли банківський касир використав комп'ютер для викрадення понад двох мільйонів доларів США, став своєрідною відправною точкою для усвідомлення суспільством небезпек, пов'язаних із використанням інформаційних технологій у протиправних цілях.

Поява першого правового визначення кіберзлочинів на Конференції Американської асоціації адвокатів у 1974 році та ухвалення у 1986 році «Закону про шахрайство з використанням комп'ютерів» у США свідчать про те, що національні правові системи почали реагувати на нові виклики. Однак, незважаючи на важливість таких нормативних актів, їх дія була обмежена територіальними межами, що створювало значні перешкоди для ефективної протидії кіберзлочинності, яка вже тоді набула транснаціонального характеру [9, с. 280].

Досвід США, Великобританії, Нідерландів та Німеччини демонструє різні підходи до правового регулювання кіберзлочинності. Наприклад, ухвалення «Акту про комп'ютерні зловживання» у Великобританії в 1990 році відображає прагнення забезпечити відповідальність за злочини, вчинені у кіберпросторі, встановлюючи широкий діапазон покарань, включаючи штрафи

та позбавлення волі. Водночас країни континентальної Європи, такі як Нідерланди та Німеччина, інтегрували нові положення про кіберзлочинність у чинні кримінальні кодекси, демонструючи прагнення адаптувати існуючі правові системи до сучасних реалій.

Таким чином, розглянемо детальніше основні нормативно-правові акти у контексті кіберзлочинності. У контексті міжнародно-правового регулювання варто погодитись з А.В. Пазюком, що міжнародні договори є головним інструментом регулювання охоронних інформаційних відносин (наприклад, Конвенція Ради Європи про кіберзлочинність, № ETS 185), оскільки боротьба із кіберзлочинністю належить до публічних функцій, що вимагає конкретизації зобов'язань держав та запровадження механізму міждержавного співробітництва на міжнародному універсальному і регіональному рівнях [10, с. 256]. Так, важливо зазначити, що Конвенція Конвенція Ради Європи про кіберзлочинність [11] вважається першим міжнародним документом, спрямованим на боротьбу з кіберзлочинністю. Конвенція (її часто називають Будапештською Конвенцією) встановлює мінімальні стандарти для криміналізації таких дій, як незаконний доступ до комп'ютерних систем, втручання в дані, розповсюдження шкідливих програм. Вона також передбачає механізми транскордонної співпраці, включаючи видачу, взаємну правову допомогу та оперативний обмін інформацією. Її головний недолік – обмежене географічне охоплення через невелике коло держав, що її ратифікували.

У доповнення даній Конвенції прийнято Додатковий протокол, міжнародно-правове регулювання якого спрямоване на криміналізацію актів расизму та ксенофобії, що вчиняються через комп'ютерні системи. Він підкреслює важливість боротьби з розпалюванням ненависті в кіберпросторі. Даний Документ передбачає обов'язковість включення таких правопорушень до національного законодавства держав-учасниць [12].

Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства спрямована на запобігання сексуальній експлуатації та насильству щодо дітей, включаючи злочини, вчинені з використанням інформаційно-комунікаційних технологій [13]. Вона встановлює заходи для захисту дітей та криміналізації відповідних діянь. Її значення в контексті кіберзлочинності полягає в тому, що вона враховує сучасні реалії, де злочини проти дітей дедалі частіше вчиняються за допомогою інформаційно-комунікаційних технологій. У документі підкреслюється необхідність захисту дітей від онлайн-грумінгу (зваблення), що є однією з найнебезпечніших форм кіберзлочинності. Конвенція вимагає від держав забезпечення права жертв на захист під час кримінального процесу, зокрема щодо збереження конфіденційності їхніх особистих даних. Лансаротська конвенція, як її ще називають, встановлює обов'язковість включення таких діянь до кримінальних кодексів держав-учасниць. Вона також підкреслює важливість міжнародного співробітництва у сфері розслідування таких злочинів, включаючи обмін інформацією між правоохоронними органами різних країн.

Конвенція Ради Європи про запобігання тероризму охоплює питання запобігання терористичним актам, включаючи використання Інтернету для терористичних цілей [14]. Вона передбачає заходи для запобігання та боротьби з тероризмом, а також механізми міжнародного співробітництва. Конвенція зобов'язує держави-учасниці криміналізувати такі дії, як заклики до терористичних актів або їхнє виправдання в онлайн-середовищі. Документ акцентує увагу на небезпеці кіберпростору, який використовується для вербування нових членів терористичних організацій. Конвенція закликає держави вжити заходів для контролю фінансових потоків, які можуть використовуватися для підтримки терористичних угруповань через різні Інтернет-платформи.

Також важливою є Конвенція ООН проти транснаціональної організованої злочинності [15]. Хоча вона не була створена спеціально для боротьби з кіберзлочинністю, її положення застосовуються до протидії кіберзлочинам, які мають транснаціональний характер. Конвенція визначає механізми міжнародного співробітництва, включаючи екстрадицію, взаємну правову допомогу та спільні розслідування.

Науковий інтерес також викликає Директива ЄС про мережеву та інформаційну безпеку [16]. Даний міжнародний нормативний акт встановлює обов'язкові вимоги для країн-членів ЄС щодо захисту критичної кіберінфраструктури, включаючи фінансовий сектор, енергетику та охорону здоров'я. Директива також передбачає обмін інформацією про кіберінциденти між державами ЄС.

Отже, на основі характеристики міжнародно-правового регулювання кіберзлочинності в умовах глобалізації, можемо стверджувати про такі особливості. Кіберзлочинність є транснаціональною, оскільки кіберзлочини не визнають державних кордонів, що створює значні труднощі для їхнього ефективного регулювання в межах національних правових систем. Наприклад, дії

кіберзлочинця можуть бути спрямовані на жертву, яка знаходиться в іншій країні, при цьому сам злочинець може використовувати інфраструктуру, розташовану в третій державі. Це вимагає гармонізації національних законодавств та створення дієвих механізмів міжнародного співробітництва, таких як передбачено в Будапештській конвенції.

Однією з основних ознак міжнародного регулювання кіберзлочинності є акцент на швидкому реагуванні та обміні інформацією між державами. Зважаючи на стрімкість кіберзагроз, традиційні процедури екстрадиції чи правової допомоги можуть бути недостатньо ефективними.

Однієї з особливостей міжнародно-правового регулювання кіберзлочинності в умовах глобалізації є різний рівень технологічного розвитку держав. Не всі країни мають рівний доступ до технологій чи ресурсів для забезпечення кібербезпеки. Ця нерівність ускладнює створення універсальної системи протидії кіберзлочинності. Наприклад, країни, що розвиваються, можуть мати обмежені технічні можливості для реалізації зобов'язань за міжнародними договорами, що вимагає підтримки з боку розвинених держав і міжнародних організацій.

Міжнародно-правове регулювання кіберзлочинності вказує на динамічність та адаптивність. Так, швидкий розвиток інформаційних технологій постійно змінює характер кіберзлочинів, що вимагає від міжнародного права високого рівня адаптивності. Наприклад, нові форми кіберзлочинності, такі як атаки на штучний інтелект чи використання криптовалют для відмивання грошей, потребують розробки нових правових інструментів. Тож, можна резюмувати, що у сучасних умовах міжнародно-правове регулювання кіберзлочинності є фрагментованим, незважаючи на наявність фундаментальних міжнародних документів.

Глобальний характер кіберзлочинності зумовлює необхідність уніфікації національних законодавств та запровадження узгоджених механізмів співробітництва між державами. Зокрема, Конвенція Ради Європи про кіберзлочинність встановлює мінімальні стандарти криміналізації таких злочинів, як незаконний доступ до інформаційних систем, втручання у дані та системи, а також використання шкідливого програмного забезпечення. Однак, незважаючи на її значення, цей договір має обмежений вплив через те, що чимало держав досі не приєдналися до нього. Це створює прогалини в глобальній системі протидії кіберзлочинності та підкреслює необхідність розробки більш універсального механізму, який враховував би інтереси різних правових систем та політичних реалій.

Одним із напрямів міжнародного співробітництва має стати створення уніфікованої системи реагування на кіберінциденти. Наприклад, міжнародні конвенції, подібні до Конвенції Ради Європи про кіберзлочинність, повинні передбачати обов'язкові механізми для негайного обміну інформацією про кіберзагрози між державами. Це дозволить оперативно ідентифікувати загрози та мінімізувати їхній вплив на глобальну економіку. Важливим аспектом також є створення глобального фонду кібербезпеки, який фінансуватиме заходи із запобігання кіберзлочинності, особливо у країнах із недостатньо розвиненою кіберінфраструктурою.

Додатково, кіберзлочинність потребує нових підходів до криміналізації. Зокрема, прогалини в міжнародному праві щодо програм-вимагачів, які вимагають викуп у криптовалюті, потребують чітких правових визначень та механізмів розслідування. Це передбачає, що міжнародні акти повинні включати положення про легалізацію механізмів відстеження криптовалютних транзакцій із гарантією дотримання прав людини.

Таким чином, як можна помітити, процес законодавчої боротьби з кіберзлочинами в зарубіжних країнах розпочався ще у XX столітті. Основні, фундаментальні нормативно-правові акти, що формують систему протидії, також були прийняті в той час, і більшість з них діють досі. Однак це зовсім не означає, що сучасна система протидії кіберзлочинам базується виключно на актах, прийнятих у минулому столітті. Сучасний світ змінюється швидко через такі фактори, як комп'ютеризація, глобалізація та інформатизація, перманентна війна. В цих умовах технології та техніка постійно оновлюються, що призводить до швидких змін і у злочинній сфері, особливо в галузі кіберзлочинів [17].

Україна повинна продовжувати участь у міжнародному діалозі з питань відповідальної поведінки держав у кіберпросторі на основі дотримання принципів міжнародного права, Статуту ООН, а також норм, правил та принципів відповідальної поведінки держави. Це потребуватиме більшої координації та консолідації заінтересованих сторін на міжнародних форумах, в яких Україна буде не лише учасником, але й ініціатором та організатором. Беручи до уваги вищевикладене, погоджуємось з О.М. Поляковим, що Україна повинна займати більш проактивну позицію на міжнародній арені з питань забезпечення кібербезпеки. Держава має розвивати міжнародне співробітництво у сфері кібербезпеки, спрямоване, передусім, на забезпечення незалежності

і державного суверенітету, відновлення територіальної цілісності України, підтримання ініціатив учасників системи колективної безпеки НАТО [18, с. 137].

Висновки. Отже, аналізуючи кіберзлочинність в умовах глобалізації, неможливо обійти увагою питання кібербезпеки, адже саме вона забезпечує правові, технічні та організаційні рамки, в межах яких можливе створення ефективних механізмів міжнародного співробітництва, захисту прав людини та підтримання глобальної стабільності в умовах цифрового світу.

Дослідження міжнародно-правового регулювання кіберзлочинності в умовах глобалізації дозволило визначити, що кіберзлочинність є однією з найсерйозніших загроз сучасному міжнародному правопорядку, яка суттєво впливає на економічну, соціальну та інформаційну стабільність у глобальному масштабі. Транснаціональний характер цієї злочинності, а також її здатність швидко адаптуватися до новітніх технологій створює значні виклики для традиційних правових систем і потребує системного та скоординованого міжнародного реагування. Лише через ефективну координацію зусиль держав, міжнародних організацій, приватного сектору та громадянського суспільства можливо забезпечити стійкість глобального кіберпростору, захист прав людини та економічну стабільність у світі.

Список використаних джерел:

1. Кирилюк О. В. Міжнародно-правове забезпечення розвитку глобального інформаційного суспільства : дис. ... канд. юрид. наук : 12.00.11 – Міжнародне право. Київ, 2017. 250 с.

2. Павленко А.В. Правове регулювання діяльності Європейського Союзу у сфері протидії транскордонним злочинам: дис. канд. юрид. наук : 12.00.01 / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2016. 244 с.

3. What is cybersecurity? *IBM*. URL: https://www.ibm.com/topics/cybersecurity

4. Саєнко М.І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського національного університету. Серія : Право.* 2021. Вип. 64. С. 386–391.

5. Von Solms R. From information security to cyber security. *Computers & security.* 2013. Vol. 38. P. 97–102

6. Грицун О.О. Міжнародно-правове забезпечення міжнародної інформаційної безпеки : дис. ... канд. юрид. наук : 12.00.11; Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2016. 244 с.

7. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки». *2024. № 1 (*41). С. 314–320.

8. Никончук Н.С., Маслова О.О. Кіберзлочинність в Україні: виклики сучасності. *Юридичний науковий електронний журнал.* 2021. № 9. С. 202–205.

9. Попко В. В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського Національного Університету. Серія право*. 2021. Вип. 66. С. 276-283

1 0. Пазюк А. В. Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти : дис…. д-ра юрид. наук: 12.00.11 / Київ. нац. ун-т ім. Тараса Шевченка. К., 2016. 467 с.

11. Конвенція про кіберзлочинність: Міжнародний документ Ради Європи від 23.11.2001.

12. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Міжнародний документ від 28.01.2003. URL https://zakon.rada.gov.ua/laws/show/994_687#Text

13. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства : Міжнародний документ від 25.10.2007. URL https://zakon.rada.gov.ua/laws/show/994_927#Text

14. Конвенція Ради Європи про запобігання тероризму : Міжнародний документ від 15.11.2000. URL https://zakon.rada.gov.ua/laws/show/995_789#Text

15. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності : Міжнародний документ від 15.11.2000. URL https://zakon.rada.gov.ua/laws/show/995_789#Text

16. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

17. Голін І.В. Боротьба з кіберзлочинами: досвід окремих зарубіжних країн. *Аналітично-порівняльне правознавство.* 2024. № 4. С. 497–501.

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