УДК 343.9

Цюприк Ігор Володимирович
доктор юридичних наук,
професор кафедри кримінального процесу та криміналістики
Національна академія СБУ
Tsiupryk Igor
Doctor of Law,
Professor of the Department of Criminal Procedure and Forensics
National Academy of the Security Service of Ukraine
ORCID: 0009-0007-4460-9968

DOI: 10.25313/2520-2308-2025-7-11180

ПРОБЛЕМИ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРАГРЕСІЇ В УМОВАХ ЦИФРОВОЇ ЕПОХИ

PROBLEMS OF INTERNATIONAL LEGAL REGULATION OF CYBER AGGRESSION IN THE DIGITAL AGE

Анотація. *Вступ. У XXI столітті феномен війни зазнав суттєвих змін від класичних форм застосування збройної сили до новітніх, гібридних методів впливу, серед яких особливе місце посідають кібератаки, що дедалі частіше застосовуються державами як інструмент реалізації геополітичних інтересів, дестабілізації політичних систем, підриву національної безпеки та впливу на внутрішньодержавні процеси. При цьому міжнародно-правові механізми кваліфікації таких дій залишаються застарілими та фрагментарними, що створює суттєві виклики для ефективного реагування світової спільноти на нові форми агресії.*

Особливу актуальність дана проблематика набула в контексті збройної агресії Російської Федерації (далі – РФ) проти України, яка супроводжується безпрецедентними за масштабами і складністю кібератаками проти органів державної влади, критичної інфраструктури, систем зв'язку та інформаційного середовища, що загрожує суверенітету, політичній незалежності, а відтак і національній безпеці держави.

Попри наявність базових положень щодо заборони агресії у Статуті Організації Об'єднаних Націй (далі – ООН), Резолюції № 3314 Генеральної Асамблеї ООН та Римському статуті Міжнародного кримінального суду, чинне міжнародне право залишається концептуально неготовим до повноцінної правової оцінки кібератак як форми акту агресії. Водночас, на тлі збройної агресії РФ проти України постає потреба перегляду підходів до визначення та змістовного наповнення терміну «акт агресії» з урахуванням нових викликів цифрової епохи.

Метою цієї наукової статті є комплексне дослідження правових підстав для визнання міждержавних кібератак формою акту агресії у розумінні сучасного міжнародного права у світлі окремих прикладів кібератак проти України у 2022–2024 роках.

Матеріали і методи. Матеріалами дослідження є: нормативно-правові акти міжнародного права, які регулюють питання агресії, зокрема Статут Організації Об'єднаних Націй, Резолюція Генеральної Асамблеї ООН № 3314 (XXIX) від 14 грудня 1974 року, Римський статут Міжнародного кримінального суду та Поправки до нього; Закон України «Про основні засади забезпечення кібербезпеки України», Стратегія кібербезпеки України від 2021 року та інші національні нормативно-правові акти України, що стосуються сфери кібербезпеки, цифрової інфраструктури та оборонної політики в умовах воєнного стану; доктринальні джерела – наукові праці українських і зарубіжних дослідників у сфері міжнародного гуманітарного права, кіберправа, гібридних загроз і сучасних збройних конфліктів; аналітичні матеріали та офіційні звіти, підготовлені державними органами України, спеціалізованими центрами кібербезпеки, а також публікації міжнародних організацій щодо кібератак; окремі публікації у засобах масової інформації, висновки IT-експертів та дані з відкритих джерел, що документують факти кібератак проти України та їх наслідки.

У процесі здійснення дослідження було використано такі наукові методи, як метод теоретичного узагальнення та систематизації для формування загальної картини впливу кіберзагроз на міжнародну безпеку та правовий порядок;

метод аналізу і синтезу для розкладання окремих елементів кіберзагроз на складові агресії; порівняльно-правовий метод для порівняння положень чинних міжнародних правових актів щодо агресії з сучасними потребами в регулюванні її гібридних форм; метод правової інтерпретації для тлумачення норм міжнародного права з позицій функціонального підходу до кваліфікації акту агресії; історико-правовий метод для простеження еволюції змісту поняття «агресія» в міжнародному праві; метод логічного узагальнення результатів для формулювання пропозицій щодо удосконалення міжнародно-правових механізмів реагування на кібератаки як акту агресії.

Результати. У науковій статті наведено системний аналіз чинного міжнародного нормативно-правового регулювання понять «акт агресії» та «злочин агресії» у контексті сучасних викликів цифрової доби, зокрема кібератак. Підкреслено, що історично сформовані міжнародно-правові підходи орієнтовані виключно на класичні форми застосування збройної сили, що не дозволяє повною мірою охопити нові гібридні форми міждержавної агресії.

У статті узагальнено практику кібератак проти України у 2022–2024 роках, визначено їхні спільні риси, масштаби та наслідки, що дозволяє кваліфікувати їх як акт міжнародної агресії, яка в ряді випадків має наслідки традиційного воєнного вторгнення. Зроблено висновок про необхідність перегляду та актуалізації міжнародно-правової доктрини та розширення поняття акту агресії з урахуванням новітніх викликів, загроз та їх змістовних елементів, що були виокремлені та досліджені у статті, а також запропоновано конкретні напрями оновлення міжнародно-правових механізмів.

Перспективи. У подальших наукових дослідженнях варто зосередити увагу на: аналізі міжнародного досвіду протидії цифровим формам агресії та ефективності вже існуючих правових і технічних механізмів реагування в різних правових системах; удосконаленні національного законодавства України у сфері кібербезпеки, цифрового суверенітету та відповідальності за вчинення міжнародних кіберзлочинів; формуванні нової доктрини міжнародного гуманітарного та кримінального права, яка би враховувала кіберпростір як повноцінну площину ведення кібервійни та агресії.

Ключові слова: *кібербезпека, кібератака, акт агресії, міжнародне право, гібридна війна, міжнародний злочин, критична інфраструктура, відповідальність.*

Summary. *Introduction. In the 21st century, the nature of warfare has undergone substantial transformation – from traditional armed conflicts to hybrid methods of influence. Among these, cyberattacks play an increasingly prominent role, actively employed by states as tools for achieving geopolitical goals, destabilizing political systems, undermining national security, and interfering in internal affairs. At the same time, international legal frameworks remain outdated and fragmented in addressing the classification and legal response to such acts, creating significant challenges for effective reaction by the global community to new forms of aggression.*

This issue has gained particular relevance in the context of the armed aggression of the Russian Federation against Ukraine, accompanied by unprecedented cyberattacks targeting government bodies, critical infrastructure, communication systems, and the information domain. These actions violate fundamental principles of sovereignty, political independence, and state security.

Despite the existing foundational norms on the prohibition of aggression in the UN Charter, UN General Assembly Resolution № 3314, and the Rome Statute of the International Criminal Court, current international law is conceptually unprepared to provide a comprehensive legal assessment of cyberattacks as a form of act of aggression. In light of Russia's ongoing aggression against Ukraine, there is an urgent need to reconsider the approaches to defining and interpreting the term "act of aggression" within the realities of the digital age.

The purpose of this scientific article is to conduct a comprehensive legal study on the qualification of inter-state cyberattacks as an act of aggression under modern international law, as well as to analyze key examples of cyberattacks against Ukraine between 2022 and 2024.

Materials and methods. The materials used for this study include: international legal instruments governing the issue of aggression, such as the Charter of the United Nations, UN General Assembly Resolution № 3314 (XXIX) of 14 December 1974, the Rome Statute of the International Criminal Court and its Kampala Amendments adopted in 2010; national legal acts of Ukraine in the field of cybersecurity, digital infrastructure, and defense policy under martial law; doctrinal sources – academic writings by Ukrainian and international scholars on international humanitarian law, cyber law, hybrid threats, and modern armed conflicts; analytical materials and official reports by Ukrainian government agencies, specialized cybersecurity centers, and international organizations (EU, NATO, UN) on cyberattacks; selected media publications, expert opinions, and open-source intelligence documenting cyber incidents and their consequences in Ukraine.

The research employed the following scientific methods: theoretical generalization and systematization to form a comprehensive view of cyberthreats and their impact on international security and legal order; analysis and synthesis to deconstruct cyberthreats into elements of aggression; comparative legal method to assess the adequacy of existing international norms regarding aggression in regulating its modern hybrid manifestations; legal interpretation method for interpreting international law provisions from a functional perspective; historical-legal method to trace the evolution of the legal concept of "aggression"; and the method of logical generalization for the development of proposals to enhance international legal mechanisms for responding to cyberattacks as a form of aggression.

Results. The article presents a systematic analysis of current international legal frameworks regulating the concepts of "act of aggression" and "crime of aggression" in the context of digital-era threats, particularly cyberattacks. It emphasizes that historically formed approaches remain centered on classical uses of armed force and do not adequately reflect modern hybrid forms of interstate aggression.

The study consolidates the practice of cyberattacks against Ukraine in 2022–2024, identifying their common features, scope, and consequences, which justify classifying them as acts of international aggression – in many cases comparable to traditional armed incursions. The article concludes that there is an urgent need to update and expand international legal doctrine, especially regarding the definition and interpretation of aggression, in light of new digital threats. It also proposes concrete directions for the modernization of international legal mechanisms.

Discussion. Further research should focus on: analyzing international practices in countering digital aggression and evaluating the effectiveness of existing legal and technical mechanisms across jurisdictions; enhancing Ukraine's national legislation in the fields of cybersecurity, digital sovereignty, and accountability for committing international cybercrimes; and developing a new doctrinal foundation of international humanitarian and criminal law that fully incorporates cyberspace as a legitimate theater of war and aggression.

Key words: *cybersecurity, cyberattack, act of aggression, international law, hybrid warfare, international crime, critical infrastructure, accountability.*

Постановка проблеми. На тлі стрімкої цифровізації всіх сфер суспільного життя та ескалації міжнародних конфліктів із застосуванням новітніх гібридних інструментів постає необхідність переосмислення базових категорій міжнародного кримінального та гуманітарного права. Однією з ключових теоретико-практичних проблем є неврегульованість питання правової кваліфікації кібератак як акту агресії, попри те, що такі дії можуть завдавати шкоди, співмірної з класичними формами збройного вторгнення.

Існуючі міжнародно-правові акти, зокрема Статут ООН, Резолюція № 3314 (XXIX) Генеральної Асамблеї ООН, а також Римський статут Міжнародного кримінального суду, формувалися в епоху, коли війна розумілася винятково як фізичне застосування сили. Унаслідок цього чинна міжнародно-правова доктрина не охоплює цифрові форми протистояння між державами, що супроводжують або заміщують традиційні бойові дії і не забезпечують адекватного механізму притягнення до відповідальності за такі дії.

Проблема загострюється в умовах повномасштабної збройної агресії рф проти України, яка супроводжується безпрецедентною за масштабами та інтенсивністю кібератак, спрямованих на критичну інфраструктуру, цифрову комунікацію, державне управління та інформаційний простір. Такі атаки демонструють зміну природи агресії, її прихований та технологічно витончений характер, що вимагає нових правових підходів і перегляду існуючих міжнародних норм.

Аналіз останніх досліджень і публікацій. У сучасній українській та зарубіжній науковій літературі проблема кібератак як елементу гібридної агресії, а також пов'язана з нею проблематика кібербезпеки, цифрового суверенітету та міжнародної відповідальності, перебувають у фокусі міждисциплінарних досліджень. В останні роки національна правнича наука значною мірою активізувала вивчення кіберзагроз у контексті збройного конфлікту, однак, водночас, залишається обмежено розробленим підхід до їхньої кваліфікації саме як акту агресії у міжнародно-правовому розумінні.

В аспекті аналізу кібератак як новітньої форми міжнародної агресії доцільно спиратися на наукові доробки окремих національних дослідників, які вивчали як кримінально-правові, так і міжнародно-правові аспекти кіберзагроз. Зокрема, К.В. Юртаєва, В. та Б. Горлинські, О.О. Дудоров, М.І. Хавронюк, Є.В. Лащук і Р.О. Мовчан досліджували питання криміналізації кіберзлочинів і специфіку їх кваліфікації в умовах збройного конфлікту[15]. Суттєвий внесок у дослідження кібербезпеки на національному рівні зробили В.Л. Бурячок, Р.В. Бараненко, В. та Н. Калетніки, Н.П. Бортник, С.С. Єсімов, Д.В. Дубов і М.А. Погорецький, що у своїх працях акцентували увагу на гібридному характері сучасних кіберзагроз та необхідності формування комплексної системи кібернетичної безпеки держави[12]. Питання механізму здійснення кібератак, а також способів протидії їм, знайшли відображення в працях С. Федонюка, С.А. Буяджи, Р.В. Грищука та О.О. Сурілової, а питання міжнародної відповідальності за кібератаки піднімали В.В. Кондратьєв та Л.В. Рибальченко[11; 13; 14].

Незважаючи на наявність широкого кола наукових публікацій, більшість із них акцентують увагу переважно на загальних питаннях забезпечення кібербезпеки, окремих аспектах кримінально-правової кваліфікації або інформаційно-технічному вимірі проблеми. У той же час у сучасному правничому дискурсі досі не сформовано цілісного, концептуально обґрунтованого підходу до правової оцінки масштабних міждержавних кібератак як акту агресії у розумінні міжнародного права. Така відсутність доктринального узагальнення щодо правового статусу кібератак як форми агресивного застосування сили в немілітарному форматі, зокрема в умовах сучасних гібридних конфліктів, створює суттєві правові прогалини.

Тож, попри значну кількість досліджень у сфері кібербезпеки та протидії кіберзлочинності, в академічному середовищі зберігається суттєвий дефіцит комплексних міждисциплінарних праць, які б одночасно охоплювали міжнародно-правовий, кримінально-правовий, інформаційно-аналітичний і технічний компоненти феномену кібератак. Саме ця наукова прогалина зумовлює як актуальність,

так і новизну даного дослідження, яке спрямоване на розкриття кібератак як форми акту агресії, що потребує оновлення міжнародно-правового інструментарію в контексті цифрової трансформації конфліктів XXI століття.

Виклад основного матеріалу. З огляду на стрімке зростання рівня цифровізації сучасного глобального суспільства, розвиток інформаційних технологій, а також трансформацію форм і методів збройного протистояння, включно з появою нових гібридних форм агресії, виникає обґрунтована та нагальна потреба в концептуальному переосмисленні підходів до кваліфікації кібератак у міжнародному праві. Особливої актуальності це питання набуває в умовах триваючої збройної агресії Російської Федерації проти України, які демонструють, що кібератаки вже є не лише супутнім явищем сучасних конфліктів, а самостійним, стратегічним інструментом ведення війни, який здатен паралізувати державне управління, зруйнувати економічні зв'язки, дестабілізувати суспільство та підірвати фундаментальні засади державності.

У вказаному контексті надзвичайно важливо акцентувати увагу на застарілому характері чинної міжнародно-правової бази, зокрема в частині тлумачення й застосування таких ключових категорій, як «злочин агресії» та «акт агресії». Норми, які формували фундамент післявоєнного міжнародного правопорядку були створені у відповідь на виклики середини XX століття та відображали у своїй конструкції переважно класичне розуміння війни як фізичного, збройного конфлікту між державами з використанням конвенційних військових засобів, оскільки на момент їх ухвалення не існувало практичного уявлення про можливість використання цифрових технологій як самостійного засобу ведення міжнародного конфлікту.

Так, пункт 4 статті 2 Статуту Організації Об'єднаних Націй встановлює зобов'язання всіх держав-членів утримуватися у своїх міжнародних відносинах від погрози силою або її застосування проти територіальної недоторканності чи політичної незалежності будь-якої держави, або у будь-який інший спосіб, несумісний із Цілями ООН[2]. Норма, яка досі залишається фундаментальною у системі сучасного міжнародного правопорядку, сформувалась у середині XX століття та відображає традиційне розуміння війни як конфлікту з безпосереднім застосуванням фізичної сили, збройних засобів та людського ресурсу.

Аналогічним чином, Резолюція Генеральної Асамблеї ООН № 3314 (XXIX) від 14 грудня 1974 року, яка надає визначення поняттю «агресія», базується на парадигмі прямої фізичної силової атаки держави на державу. Відповідно до статті 1 зазначеної Резолюції, агресією визнається застосування збройної сили державою проти суверенітету, територіальної цілісності або політичної незалежності іншої держави, що є несумісним із положеннями Статуту ООН [3].

У статті 3 цього ж документа наведено перелік форм актів агресії, серед яких: вторгнення або напад збройних сил держави на територію іншої держави або будь-яка військова окупація, який би тимчасовий характер вона не мала, бомбардування території іншої держави, блокада портів, тощо. Попри наявність застереження про невичерпний характер переліку, аналіз положень Резолюції свідчить про її орієнтацію виключно на силові засоби ведення війни. Водночас, розвиток сучасних технологій, зокрема в сфері інформаційної безпеки, відкрив новий вимір загроз, які можуть нести масштаби не менші, а подекуди й більш значні, ніж традиційне збройне вторгнення. Саме тому існуюче міжнародне право не в повній мірі відповідає викликам XXI століття щодо наявності правових механізмів протидії кіберзагрозам.

Відповідно до статті 5 Римського Статуту юрисдикція Міжнародного кримінального суду обмежується найбільш тяжкими злочинами, які викликають занепокоєння всього міжнародного співтовариства, серед яких і злочини агресії [4].

Однак, сам Римський Статут прийнятий у 1998 році та ратифікований Україною 21 серпня 2024 року не містить фактичного визначення злочину чи акту агресії. Лише після прийняття 11 червня 2010 року в Кампалі відповідних Поправок до Римського статуту Міжнародного кримінального суду було запропоновано конкретизацію термінів «злочин агресії» та «акт агресії».

Україна ратифікувала зазначені Поправки 21 серпня 2024 року, що є надзвичайно важливим кроком у контексті адаптації міжнародного кримінального права до сучасних умов. Очікується, що вони наберуть чинності для України у жовтні 2025 року. Відповідно до положень статті 8 bis Поправок:

– **злочин агресії** означає планування, підготовку, ініціювання або вчинення особою, яка спроможна фактично здійснювати контроль за політичними чи військовими діями держави або керувати ними, акту агресії, який за своїм характером, тяжкістю та масштабами є грубим порушенням Статуту Організації Об'єднаних Націй [1];
– **акт агресії** означає застосування збройної сили державою проти суверенітету, територіальної цілісності або політичної незалежності іншої держави чи в будь-який інший спосіб, несумісний зі Статутом Організації Об'єднаних Націй [1].

Хоча визначення формально залишає акцент на збройному компоненті, важливим є той факт, що в юридичному обігу з'являється потенційна можливість тлумачення поняття «агресія» у ширшому, функціональному ключі, включно із сучасними формами гібридного впливу, зокрема через кібератаки чи інформаційні операції, які є не менш небезпечними ніж фізичне збройне втручання.

Таким чином, аналіз чинної міжнародно-правової бази засвідчує її обмеженість у контексті реагування на кіберзагрози, що змушує правозастосовні органи,

наукову спільноту та держави-учасниці ініціювати оновлення та переосмислення підходів до поняття агресії, враховуючи новітні технології як повноцінні засоби міжнародної агресії. У цьому контексті саме Україна, як держава, що фактично стала полігоном для випробування всіх сучасних немілітаризованих форм гібридної агресії, має виправдану можливість ініціювати глобальний перегляд існуючих норм, шляхом: ініціювання розроблення Поправок до Римського статуту, що прямо передбачатимуть кібератаки як форму агресії; розроблення критеріїв та ознак кібератак для їх кваліфікації як актів агресії; розробки міжнародних стандартів доказування всесвітнього механізму превенції кіберагресії, зокрема через систему санкцій за державне ведення чи фінансування кібертероризму; ініціювання створення міжнародного кібертрибуналу, компетентного розглядати кіберзлочини міжнародного характеру;

У контексті збройної агресії РФ проти України особливої уваги заслуговують масштабні та системно реалізовані кібератаки, що супроводжували або передували широкомасштабним бойовим діям. Аналіз окремих кейсів дає підстави розглядати такі дії не лише як інструмент гібридної війни, а як самостійні форми акту агресії, що мають усі притаманні цьому поняттю юридичні ознаки відповідно до положень Статуту ООН, Резолюції Генеральної Асамблеї № 3314 (XXIX) та поправок до Римського Статуту Міжнародного кримінального суду.

14 січня 2022 року Україна зазнала масштабної кібератаки, що охопила близько 70 державних веб-ресурсів, створених на CMS October компанією Kitsoft. У результаті було здійснено так звану дефейс-атаку, зловмисники розмістили на урядових сайтах деструктивні повідомлення трьома мовами — українською, російською та спотвореною польською[7]. Контент таких повідомлень містив елементи історичної пропаганди, маніпуляцій і погроз, спрямованих на психологічний тиск на українське суспільство. Висвітлена кібератака є показовим прикладом використання інформаційної зброї з політично мотивованою метою, що, з урахуванням масштабності та доведеного зв'язку із зовнішнім суб'єктом, можна розцінювати як початковий елемент акту агресії. Атака була спрямована на підрив інформаційної безпеки, дестабілізацію довіри до органів державної влади та розпалювання міжнаціональної ворожнечі — тобто мала всі ознаки умисної діяльності, спрямованої на підрив суверенітету України.

Одна з найбільших у новітній історії України DDoS-атак, що відбулася 15–16 лютого 2022 року була спрямована на державні ресурси та провідні банківські установи — зокрема, ПриватБанк, Ощадбанк, сайти Міністерства оборони, Збройних Сил України та інших ключових органів[5]. Атака призвела до тимчасового порушення доступу до цифрових сервісів, мобільних додатків та фінансових операцій, створивши ефект дестабілізації інформаційно-економічного середовища країни. На момент її реалізації така атака розцінювалася фахівцями як цілеспрямована кампанія з елементами інформаційно-психологічної операції, спрямована на дискредитацію державних інституцій України, створення атмосфери паніки серед населення та формування зовнішньополітичного тиску. За своїм характером, масштабами та впливом ця дія відповідає критеріям, зазначеним у статті 8 bis Римського Статуту щодо злочину агресії, насамперед у контексті цілеспрямованого впливу на цивільне населення шляхом порушення функціонування об'єктів критичної інфраструктури.

23 лютого 2022 року, за день до повномасштабного вторгнення російських військ на територію України, було здійснено нову серію координованих кібератак на урядові портали — зокрема, на сайти Верховної Ради України, Кабінету Міністрів, Міністерства закордонних справ, Служби безпеки України та інших установ з метою знищення баз даних та цифрової інформації, що, в умовах наближення збройного конфлікту, мало на меті паралізувати здатність держави до оперативного реагування[9]. А вже 24 лютого 2022 року, буквально за годину до вторгнення військ РФ, відбулася атака на супутникову мережу зв'язку Viasat, яка забезпечувала комунікацію Збройних Сил України, а також комерційних користувачів у Центральній Європі. Унаслідок атаки з використанням шкідливого коду було порушено зв'язок на значній території Європи. Згідно з офіційними заявами ЄС, Великої Британії та США, відповідальність за цю атаку несе РФ, що яскраво ілюструє приклад цілеспрямованого паралічу військової цифрової інфраструктури[10].

Впродовж 2023–2024 років Україна продовжила зазнавати масштабних кібератак, що потенційно варто кваліфікувати як акт агресії у цифровому вимірі.

12 грудня 2023 року об'єктом потужної кібератаки став найбільший оператор зв'язку в Україні — компанія «Київстар». Унаслідок втручання було виведено з ладу мобільний зв'язок і інтернет на всій території України, паралізовано домашній зв'язок, а також заблоковано доступ до роумінгу інших операторів. Президент компанії Олександр Комаров заявив про «часткове руйнування ІТ-інфраструктури», а представник з кібербезпеки зазначив, що знищено «майже все», включно з тисячами віртуальних серверів та персональних комп'ютерів[8]. За своєю суттю це не лише порушення зв'язку — це системний цифровий удар по критично важливій цивільній інфраструктурі держави, яка забезпечує базову життєдіяльність населення. Метою атаки, як зазначають джерела, було не лише технічне знищення систем, а й психологічний ефект, а також можливе здобуття розвідувальної інформації. У збитках компанія оцінила втрати у понад 3,6 мільярди гривень.

19 грудня 2024 року відбулася одна з найсерйозніших атак на цифрову суверенність України — цілеспрямоване втручання в інформаційні ресурси

Міністерства юстиції України, Національних інформаційних систем та порталу «Дія». Внаслідок дій держави-агресора було паралізовано роботу понад 60 державних реєстрів, включно з Державним реєстром актів цивільного стану громадян та Державним реєстром речових прав на нерухоме майно. Як наслідок було зупинено функціонування держави у ключових сферах суспільних відносин, зокрема, було заблоковано можливість вчинення будь-яких реєстраційних, нотаріальних дій, ускладнено можливість перетину кордону і тому подібне. Віцепрем'єрка Ольга Стефанішина прямо заявила, що атака мала російське походження та метою було порушення функціонування критичної інфраструктури держави[6]. Вже 25 січня 2024 року зазнав втручання й один із ключових українських дата-центрів — «Парковий», користувачем якого є низка стратегічно важливих державних і комунальних підприємств, зокрема «Укрпошта», «Укрзалізниця», «Нафтогаз України» та система перетину кордону «Шлях». Внаслідок атаки тимчасово було зупинено видачу поштових послуг, блоковано прикордонне оформлення водіїв, припинено доступ до сервісів перевезень і обслуговування споживачів у енергетичній сфері, що є прикладом цілеспрямованого паралічу логістичних, енергетичних, поштових і транспортних систем. Атака мала явний ефект примусу, створення критичних незручностей для держави, бізнесу й громадян з метою дестабілізації управлінських і економічних процесів.

Аналогічно, в світлі кібератак не можна залишити поза увагою такий потужний інструмент гібридного впливу, як інформаційно-психологічні операції (далі — ІПсО), що часто супроводжують або й передують технічним формам кібератак. ІПсО становлять системну форму впливу на масову свідомість громадян, спрямовану на зміну поведінкових моделей, маніпулювання емоційними реакціями та нав'язування вигідних агресору наративів, і тому мають розглядатися не лише як частина інформаційної війни, а як повноцінний елемент цифрової агресії, що посягає на інформаційний суверенітет держави.

За своїм значенням наведені приклади кібератак проти України становлять не одиничні інциденти, а системну, багатоетапну спробу виведення з ладу основ функціонування української держави, що має всі характерні ознаки свідомого акту цифрової агресії вчиненого з боку іноземного державного суб'єкта або під його прямим контролем і сприянням.

Такий комплекс дій, з урахуванням їх масштабів, спрямованості, державного походження та стратегічних цілей, повністю відповідає юридичному змісту поняття «акту агресії». Аналіз наведених кібератак проти України дозволяє виокремити низку узагальнених ознак, які об'єднують ці інциденти в єдиний феномен, серед яких:

1. Державне походження або підтримка державного суб'єкта, що вказує на політичну вмотивованість таких дій.

2. Високий рівень координації, синхронізації та складності кібератак, що засвідчує їх реалізацію на високотехнологічному рівні.

3. Відсутність військової необхідності, що прямо порушує принципи міжнародного гуманітарного права.

4. Масштабність і тяжкість наслідків, які є співмірним з ефектом від традиційних збройних атак. А саме:

– виведення з ладу державних інформаційних систем, що призводить до підриву державного управління та суверенітету
– підрив економічної стабільності та знищення функціональних ланцюгів критичної інфраструктури, яка забезпечує базову життєдіяльність держави та взаємодію з громадянами, зокрема телекомунікаційних мереж, енергетичних систем, транспортних сервісів, банківського сектору, що призвело до фінансових втрат, призупинення договірних відносин, зупинення господарської діяльності і тд.
– цілеспрямована дискредитація органів державної влади, створення інформаційного хаосу, психологічний тиск на громадян з метою викликати дезорієнтацію, паніку та формувати образ «нездатної до управління держави» як у внутрішньому, так і у міжнародному вимірі.

Висновки та перспективи подальших досліджень. Як простежується, сучасна агресія у цифровому вимірі може мати наслідки, не менш серйозні, ніж класичне збройне втручання. Більше того, її невидимість і прихований характер лише підсилюють її руйнівний потенціал, адже завдана шкода проявляється не миттєво, а у вигляді затяжного ослаблення державних функцій, зниження довіри громадян до державних інституцій, а в окремих випадках — навіть політичної дестабілізації.

Тож, питання правової кваліфікації масштабних кібератак як акту агресії є не лише академічним, а й практичним завданням для міжнародної спільноти, що потребує оновлення існуючих міжнародно-правових механізмів реагування, притягнення до відповідальності та превенції. Відсутність у чинному міжнародному праві чіткої, імперативної норми, що визнає кібератаку формою акту агресії, створює критичний правовий вакуум і дестабілізує міжнародний правопорядок та підриває ефективність системи міжнародної безпеки.

В аспекті наведеного, не менш важливим є й адаптація національного законодавства, зокрема щодо подальшого розвитку криміналізації міждержавних форм цифрового впливу, зокрема таких як кібердиверсія, кібертероризм, кібершпигунство та інших кіберзлочинів під юрисдикційним контролем іноземної держави. Формування відповідного правового інструментарію має спиратися як на загальновизнані міжнародні стандарти, так і на унікальний досвід України як держави, яка перебуває на фронті цифрової війни нового покоління.

Література

1. Поправки до Римського статуту Міжнародного кримінального суду щодо злочину агресії від 11.06.2010. URL: https://zakon.rada.gov.ua/laws/show/995_004-10#Text (дата звернення: 20.06.2025).

2. Статуту Організації Об'єднаних Націй від 26.06.1945. URL: https://uk.wikisource.org/wiki/%D0%A1%D1%82%D0%B0%D1%82%D1%83%D1%82_%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%97_%D0%9E%D0%B1%27%D1%94%D0%B4%D0%BD%D0%B0%D0%BD%D0%B8%D1%85_%D0%9D%D0%B0%D1%86%D1%96%D0%B9 (дата звернення: 20.06.2025).,

3. Резолюція Генеральної Асамблеї ООН № 3314 (XXIX) від 14.12.1974. URL: https://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml (дата звернення: 20.06.2025).

4. Римський Статут Міжнародного Кримінального Суду від 17.07.1998. URL: https://zakon.rada.gov.ua/laws/show/995_588#Text (дата звернення: 20.06.2025).

5. BBC News Україна. Нова кібератака на банки була «найбільшою в історії України» й досі триває. URL: https://www.bbc.com/ukrainian/news-60401775 (дата звернення: 24.06.2025).

6. DOU.ua. Кібератака на реєстри Мін'юсту. URL: https://dou.ua/lenta/articles/cyberattacks-on-registries-and-vendor-locks/ (дата звернення: 25.06.2025).

7. DOU.ua. Україну накрили хакерські атаки: постраждали урядові сайти, портал «Дія» недоступний. URL: https://dou.ua/lenta/news/ukraine-was-covered-by-hacker-attacks/ (дата звернення: 25.06.2025).

8. Forbes.ua. Кібератака на «Київстар». URL: https://forbes.ua/news/kiberataka-na-kiivstar-gendirektor-kompanii-rozpoviv-pro-chastkove-ruynuvannya-it-infrastrukturi-12122023-17845 (дата звернення: 26.06.2025).

9. Інформаційне агентство УНІАН. Рік руйнівних кібератак в Україні: як загрози атакували користувачів та організації. URL: https://www.unian.ua/techno/communications/rik-ruynivnih-kiberatak-v-ukrajini-yak-zagrozi-atakuvali-koristuvachiv-ta-organizaciji-12158007.html (дата звернення: 26.06.2025).

10. ПрАТ «Телерадіокомпанія «Люкс»», 24 Канал. Китайські хакери зламали головну супутникову компанію світу Viasat. URL: https://24tv.ua/tech/kitayski-hakeri-zlamali-suputnikovu-kompaniyu-viasat-yaka-obslugovuye_n2851354 (дата звернення: 25.06.2025).

11. Актуальні проблеми міжнародного та європейського права. Погляд молодих вчених (19 жовтня 2023 року, м. Львів). Л. : Львівський національний університет імені Івана Франка, Факультет міжнародних відносин, Студентська спілка Української асоціації міжнародного права, 2023. ст. 139.

12. Бараненко Р.В. Кібератака як одна з форм кібертероризму. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2021, № 1. Том 32. URL: https://www.tech.vernadskyjournals.in.ua/journals/2021/1_2021/part_1/9.pdf (дата звернення: 21.06.2025).

13. Буяджи С.А. Перспективи правового регулювання боротьби з кіберзлочинністю в Україні. *Право України*. 2017. № 9. С. 245. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001432159 (дата звернення: 22.06.2025).

14. Міжнародні аспекти безпеки кіберпростору : монографія / С.В. Федонюк. Луцьк : Вежа-Друк, 2022. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/20718/1/Mizhnar_asp_bezp_kiberprostoru.pdf (дата звернення: 23.06.2025).

15. Юртаєва К.В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. *Юридичний науковий електронний журнал*. URL: http://www.lsej.org.ua/12_2022/96.pdf (дата звернення: 23.06.2025).

References

1. Amendments to the Rome Statute of the International Criminal Court on the Crime of Aggression, adopted on 11 June 2010. URL: https://zakon.rada.gov.ua/laws/show/995_004-10#Text (date of access: 20.06.2025).

2. Charter of the United Nations, signed on 26 June 1945. URL: https://uk.wikisource.org/wiki/Статут_Організації_Об%27єднаних_Націй (date of access: 20.06.2025).

3. UN General Assembly Resolution № 3314 (XXIX) on the Definition of Aggression, adopted on 14 December 1974. URL: https://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml (date of access: 20.06.2025).

4. Rome Statute of the International Criminal Court, adopted on 17 July 1998. URL: https://zakon.rada.gov.ua/laws/show/995_588#Text (date of access: 20.06.2025).

5. BBC News Ukraine. "New Cyberattack on Banks Is 'The Largest in Ukraine's History' and Still Ongoing". URL: https://www.bbc.com/ukrainian/news-60401775 (date of access: 24.06.2025).

6. DOU.ua. "Cyberattack on the Ministry of Justice Registers". URL: https://dou.ua/lenta/articles/cyberattacks-on-registries-and-vendor-locks/ (date of access: 25.06.2025).

7. DOU.ua. "Ukraine Hit by Cyberattacks: Government Websites and the 'Diia' Portal Unavailable". URL: https://dou.ua/lenta/news/ukraine-was-covered-by-hacker-attacks/ (date of access: 25.06.2025).

8. Forbes Ukraine. "Cyberattack on Kyivstar: The Company's CEO Reports Partial Destruction of IT Infrastructure". URL: https://forbes.ua/news/kiberataka-na-kiivstar-gendirektor-kompanii-rozpoviv-pro-chastkove-ruynuvannya-it-infrastrukturi-12122023-17845 (date of access: 26.06.2025).

9. UNIAN Information Agency. "A Year of Destructive Cyberattacks in Ukraine: How Threats Targeted Users and Organizations". URL: https://www.unian.ua/techno/communications/rik-ruynivnih-kiberatak-v-ukrajini-yak-zagrozi-atakuvali-koristuvachiv-ta-organizaciji-12158007.html (date of access: 26.06.2025).

10. TRC Lux, Channel 24. "Chinese Hackers Breach the World's Leading Satellite Company Viasat". URL: https://24tv.ua/tech/kitayski-hakeri-zlamali-suputnikovu-kompaniyu-viasat-yaka-obslugovuye_n2851354 (date of access: 25.06.2025).

11. Topical Issues of International and European Law. Perspective of Young Scholars (October 19, 2023, Lviv). Lviv: Ivan Franko National University of Lviv, Faculty of International Relations, Student Union of the Ukrainian Association of International Law, 2023, p. 139.

12. Baranenko, R.V. Cyberattack as One of the Forms of Cyberterrorism. *Scientific Notes of V.I. Vernadsky Taurida National University. Series: Technical Sciences.* 2021. № 1, Vol. 32. URL: https://www.tech.vernadskyjournals.in.ua/journals/2021/1_2021/part_1/9.pdf (date of access:21.06.2025).

13. Buyadzhi, S.A. Prospects of Legal Regulation of Combating Cybercrime in Ukraine. *Law of Ukraine.* 2017. № 9. p. 245. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001432159 (date of access:22.06.2025).

14. Fedoniuk, S.V. International Aspects of Cybersecurity: Monograph. Lutsk: Vezha-Druk, 2022. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/20718/1/Mizhnar_asp_bezp_kiberprostoru.pdf (date of access: 23.06.2025).

15. Yurtayeva, K.V. Criminal Liability for Cybercrimes Committed During Armed Conflict: International Trends and Ukrainian Realities. *Legal Scientific Electronic Journal.* URL: http://www.lsej.org.ua/12_2022/96.pdf (date of access: 23.06.2025).