УДК 343.9: 341.1/8
DOI https://doi.org/10.32782/2524-0374/2024-9/72

АТРИБУЦІЯ ЗЛОЧИНУ ЯК КРИТИЧНО ВАЖЛИВА ПРОБЛЕМА КІБЕРБЕЗПЕКИ

CRIME ATTRIBUTION AS A CRITICAL CYBERSECURITY ISSUE

Павлюх О.А., к.ю.н., доцент,
доцент кафедри кримінального права та процесу
Навчально-науковий інститут права Державного податкового університету

Санжарова Г.Ф., старший викладач кафедри
романської філології та порівняльно-типологічного мовознавства
Київський столичний університет імені Бориса Грінченка

Стаття присвячена дослідженню та оцінці основних норм і правових шляхів реагування в існуючому міжнародному праві, які пропонуються для боротьби з кібератаками, зокрема проблемі атрибуції кіберзлочину. Проаналізовано особливості атрибуції кіберзлочинної діяльності та наявну практику технічної, публічної та юридичної атрибуції.

Констатовано, що спеціальні правила щодо атрибуції кібератак відсутні в міжнародному праві. Відзначено, що підстави присвоєння поведінки державі містяться в «Статтях про відповідальність за міжнародно-протиправні діяння» 2001 року. «Статті про відповідальність» не мають юридично обов'язкового характеру, оскільки є доктриною, але більшість норм набула звичаєвого характеру, що виправдовує їх застосування до кібератак. Можна стверджувати, що необхідність надійної протидії викликам динамічного середовища кіберзагроз актуалізувала розробку націлених на наступальні дії проти ворожих акторів у кіберпросторі доктрин, що припускають можливість превентивних, випереджальних дій.

Автори вважають безперечним, що в контексті міжнародної безпеки існує нагальна необхідність об'єднання глобальних зусиль по реалізації ефективного контролю за кіберінцидентами і забезпеченню відповідальної поведінки особливо державних акторів у кіберпросторі. Функція контрзаходів – спонукати державу-порушницю виконати свої міжнародні зобов'язання. Відзначено, що згідно сучасного звичаєвого міжнародного права і судової практики Міжнародного Суду випереджувальна самооборона, як частина наступальної стратегії боротьби з кіберзагрозами, не визнається контрзаходом. Держава, контрзахід якої на кібератаку згодом не проходить перевірку на законність, нестиме відповідальність за протиправність своїх дій. Зроблено висновок, що саме юридична атрибуція сприятиме загальновизнаному застосуванню норм і правил міжнародного права до кібероперацій.

Ключові слова: кіберпростір, кібербезпека, кіберзлочин, атрибуція, публічна атрибуція, юридична атрибуція кібератак.

The article is devoted to the study and evaluation of the main norms and legal ways of response in the existing international law, which are proposed to combat cyberattacks, in particular, the problem of cybercrime attribution. The peculiarities of the attribution of cybercriminal activity and the existing practice of technical, public and legal attribution are analyzed.

It was established that there are no special rules regarding the attribution of cyber attacks in international law. It was noted that the grounds for assigning conduct to the state are contained in the 2001 'Articles on Responsibility for Internationally Illegal Acts'. The 'Articles' are not legally binding as they are doctrine, but most of the norms have acquired a customary character, justifying their application to cyber attacks. It can be argued that the need for a reliable response to the challenges of the dynamic environment of cyber threats actualized the development of doctrines aimed at offensive actions against hostile actors in cyberspace, which assume the possibility of preventive, anticipatory actions.

The authors consider it indisputable that in the context of international security there is an urgent need to unite global efforts to implement effective control over cyber incidents and ensure responsible behavior, especially of state actors in cyberspace. The function of countermeasures is to induce the offending state to fulfill its international obligations. It was noted that according to modern customary international law and the judicial practice of the International Court of Justice, anticipatory self-defense, as part of an offensive strategy to combat cyber threats, is not recognized as a countermeasure. A state whose countermeasure against a cyber attack does not subsequently pass a legality check will bear responsibility for the illegality of its actions. It was concluded that it is legal attribution that will contribute to the generally recognized application of norms and rules of international law to cyber operations.

Key words: Cyberspace, Cybersecurity, Cybercrime, Attribution, Public Attribution, Legal Attribution of Cyber Attacks.

Актуальність. В останні десятиліття кіберзлочинність стає чутливим викликом міжнародному співтовариству у кіберпросторі. Кібератаки стають постійно зростаючою проблемою [1, с. 857–860; 2]. За оцінками фахівців, у 2024 році кіберзлочинність коштує світу близько 9,22 трильйона доларів, а у 2028 році очікується, що цей показник зросте до 13,82 трильйона доларів [2]. Згідно щорічному звіту Європейської агенції мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA) у вересні 2024 р. основними групами загроз кібербезпеці є програми-вимагачі та зловмисне програмне забезпечення, соціальна інженерія, загрози щодо даних і доступності (відмова в обслуговуванні), маніпулювання інформацією та втручання, а також атаки на ланцюги поставок. Найбільш зареєстрованими формами атак, на які припадає більше половини спостережуваних подій (ENISA Threat Landscape, ETL2024 базується на аналізі понад 11000 інцидентів), залишились DDoS-атаки та атаки програм-вимагачів. Галузевий аналіз показав найбільшу націленість атак на державне управління (19%) та транспорт (11%) [3]. В останні роки кіберзагрози (кібератаки ворожих держав і широкомасштабної організованої кіберзлочинності) все частіше визнаються «першим рівнем» ризику поряд із тероризмом, міждержавними війнами, пандемією та стихійними лихами. Деякі держави та групи, які мають державну підтримку, більш-менш регулярно намагаються отримати політичні, дипломатичні, технологічні, комерційні та стратегічні переваги в кіберпросторі, насамперед завдяки несанкціонованому проникненню у мережу державного, оборонного, фінансового, енергетичного та телекомунікаційного секторів інших держав [4, с. 18; 5, с. 28]. Консенсус у розумінні загрози сприяє міжнародній співпраці у виробленні стратегії протидії та виробленні дієвих механізмів відповідальності і їх закріпленню в міжнародному праві. На міжнародному форумі з кібербезпеки, що відбувся у Києві 7–8 лютого 2024 р. за ініціативи Національного координаційного центру кібербезпеки (НКЦК) при РНБО України і Фонду цивільних досліджень та розвитку США (CRDF Global) за участі представників Державного департаменту США, країн НАТО та ЄС, було наголошено на міжнародно-правовій відповідальності держави-агресора за кібератаки під час кібервійни, а також відзначалося, що найбільшою проблемою буде атрибуція і було запропоновано кваліфікувати кібератаки проти цивільної інфраструктури, які є частиною більшого за масштабом нападу як воєнні злочини.

Аналіз останніх досліджень і публікацій. Проблематика міжнародної відповідальності держави та атрибуції протиправних дій у міжнародному праві є надактуальною для сьогодення як з академічної, так і з практичної точок зору. Внесок сучасних вітчизняних учених в розробку понять, ознак, принципів, функцій та підстав юридичної відповідальності у міжнародному праві на загальнотеоретичному рівні підсумовано в монографії С. С. Андрейченко [6]. Кібербезпекові проблеми стають дедалі актуальнішими для будь-якої з країн світу і, безумовно, потребують правового визначення. Правознаці все частіше звертаються до вивчення досвіду протидії кіберзлочинності як на національному інституційно-законодавчому рівні окремих країн (М. Карпюк, К. Качмарек, М. Мацелик, О. Павлюх, В. Пизло, В. Санжаров та інші) [5; 7, с. 219–227; 8; 10; 11, с. 234–245; 12, с. 645–663], так і на міжнародному (О. Бодунова, А. Салій, В. Топчій та інші) [13, с. 187–194; 14, с. 330–334]. Проблема атрибуції кіберзлочинів розглянута серед іншого в статті М. Мацелика, Г. Санжарової, В. Санжарова, присвяченій національній стратегії кібербезпеки Великої Британії [5, с. 28–30]. На формування цієї стратегії, за визначенням її авторів, вплинули кібер-атаки на енергосистему України в 2015 р. [4, с. 18]. Комплексний аналіз кібератак проти систем електроенергетики України у 2015 та 2016 рр. здійснено в дослідженні В. Музики [15]. Автор довів необхідність технічної та політичної атрибуції кіберзлочинної діяльності в контексті збройного конфлікту на сході України [15, с. 116–125], визначив основні практичні кроки для ефективної атрибуції кібератак проти об'єктів критичної інфраструктури [15, с. 131–144], теоретичні та практичні проблеми щодо застосування звичаєвих норм атрибуції до кібератак [15, с. 85–95], перспективи розгляду міждержавних спорів щодо атрибуції кібератак в межах Міжнародного Суду ООН [15, с. 153–168]. Статті Ф.Дж. Еглоффа присвячені переважно проблематиці політичної атрибуції [16, с. 1–12]. Ф. Еглофф та М. Сміт описують основні етапи та наводять структуру публічної атрибуції, автори зазначають, що публічне приписування авторства є складним процесом і несе значні ризики [17, с. 1–32]. В статті «Оспорювані публічні приписи кіберінцидентів і роль наукових кіл» Ф. Еглофф розглядає проблему атрибуції на прикладі трьох кіберінцидентів (Sony Pictures в 2014, DNC в 2016 и NotPetya в 2017 р.) [18, с. 55–81]. Атрибуція займає центральне місце в політиці кібербезпеки. Вона встановлює зв'язок між технічними подіями та політичними наслідками, зменшуючи невизначеність щодо того, хто стоїть за вторгненням і якими були ймовірні наміри, зрештою створюючи «правду» про кібербезпеку з політичними наслідками [16; 19, с. 4–37; 20, с. 209–216]. Атрибуція як елемент міжнародно-протиправного діяння посідає ключове місце у категоріальному апараті права міжнародної відповідальності. Сучасні політико-правові реалії вимагають перегляду та модифікації концепції «атрибуції».

Мета статті полягає в дослідженні та оцінці основних норм і правових шляхів реагування в існуючому міжнародному праві, які пропонуються для боротьби з кібератаками, зокрема проблеми атрибуції («attribution») кіберзлочину.

Виклад основного матеріалу. Правова природа кіберпростору наразі є предметом дискусій. Безумовно, кіберпростір є частиною глобального спільного міжнародного простору, однак через те інфраструктура Інтернету є одночасно як публічною, так і приватною, його функціонування підпорядковане як національним, так і міжнародному законодавству. Міжнародний правовий режим для основних ресурсів кіберпростору поки що залишається справою майбутнього. Міжнародна відповідальність в кіберпросторі через поширеність анонімності в Мережі – за допомогою віртуальних приватних мереж (VPN), проксі-серверів, цибулевої маршрутизації тощо – та різноманітність присутніх у кіберпросторі акторів стикається з проблемою атрибуції, визначення авторства кіберзлочинів. Набула поширення практика окремих держав використовувати посередників для здійснення таємних дій в Інтернеті; заборони міжнародних інстанцій на використання державами третіх сторін для вчинення міжнародно-протиправних дій за допомогою інформаційно-комунікаційних технологій не дієві.

Атрибуція займає центральне місце в політиці кібербезпеки. Процес атрибуції включає кілька етапів і встановлює зв'язок між технічними подіями та їх політичними наслідками. Юридичній атрибуції передують технічна і публічна атрибуція. Технічна атрибуція має пов'язати кібератаку з конкретним місцем (комп'ютером) і конкретним виконавцем (особою) [19, с. 10–11; 21, с. 6–8]. Технічні можливості тривалий час були доволі обмеженими, що унеможливлювало процес встановлення виконавців кібератак та держав, що за ними стоять. Наразі обмежені ресурси держави компенсує співпраця з приватним сектором: технічні звіти компаній CrowdStrike щодо Putter Panda [19, с. 13], або Symantec відносно вірусу Stuxnet [19, с. 10; 21, с. 3]. Європейська агенція мережевої та інформаційної безпеки забезпечує виконання функції виявлення і блокування кібератак, а також локалізації їх наслідків незалежно від походження стосовно цивільних об'єктів усіх форм власності. CERT-EU (Computer Emergency Response Team) – це структура, яка виявляє кібератаки за допомогою спеціалізованої технологічної системи датчиків, встановлених на абонентських лініях доступу до серверів. У разі здійснення кібератаки спрацьовує датчик, про що оперативно сповіщається CERT-EU. Якщо CERT-EU виявляє кібератаки з ознаками злочинних дій, то відповідна інформація передається до Європейського центру з розслідування кіберзлочинів (European Cybercrime Centre, ECC), який, у свою чергу, може поінформувати про них Європейську агенцію оборони (European Defence Agency) для організації кібероперацій або Європейську службу зовнішніх справ (European External Action Service) [3; 14, с. 333]. Європейський Союз розробив та прийняв так звані Рамки для спільного дипломатичного реагування на шкідливу кібердіяльність, що наразі представляють унікальний підхід до реагування на кібератаки. Разом з тим особливості високотехнологічних рішень вимагають переробки існуючих режимів правового регулювання.

Публічна атрибуція має на меті присвоїти кібератаку конкретній державі, на яку вказують технічні та певні політичні індикатори [16, с. 1–12]. Приклад кібератаки Wannacry у 2017 році: приватні фірми протягом кількох днів атрибували Північну Корею, за кілька місяців США та Великобританія офіційно визнали атрибуцію Північної Кореї, але публічних санкцій не було. Кібератака в Грузії в 2019 році: через чотири місяці понад 20 держав публічно офіційно приписали кібератаку росії, але не вказали конкретні правила міжнародного права, які були порушені цією кібератакою. У Звіті GGE ООН за 2015 р. зазначено, що визначення того, що кіберактивність почалася на території чи інфраструктурі держави, недостатньо для атрибуції їй такої діяльності. Досить розповсюдженими є взяття під контроль та незаконне використання кіберінфраструктури, урядової чи приватної, іншої держави для здійснення зловмисних операцій. Випадки спуфінгу за допомогою видавання себе за інші організації або використання їхніх IP-адрес, дуже важко ідентифікувати. У цьому пункті юридичну визначеність важко підтвердити заздалегідь, і кінцевий результат є небажаним з юридичної точки зору. Окремі держави все ще балансують між застосуванням міжнародного права та стратегічними і політичними міркуваннями [22, с. 195–201]. Труднощі, пов'язані з атрибуцією (приписуванням), спонукають держави до стратегії обережності, згідно з якою, через неможливість встановити атрибуцію з упевненістю, краще не посилатися на

незаконність певної кібер-діяльності, що, у свою чергу, сприяє безкарності [20, с. 209–216]. Важливим складником атрибуції кіберзлочину з точки зору міжнародного права є оприлюднення доказів, на яких ґрунтується приписування кібероперації іншій державі. Сполучені Штати стверджували через юридичного радника Державного департаменту, що не існує міжнародного зобов'язання розкривати докази до вжиття відповідних дій, схожу позицію висловлювали Велика Британія, Франція та Нідерланди. За спостереженнями Ф. Еглоффа, останнім часом деякі держави змінили свою політику реагування з боротьби з окремими кібервторгненнями на реагування в ширшому політичному контексті відносин із конкретним супротивником, що призвело до відповідей, схожих на кампанію стримування потенційних супротивників [21, с. 5]. Урядова політика відносно кіберпростору стала більш інтервенціоністською, націленою на наступальні дії проти «ворожих акторів» у кіберпросторі [4, с. 25, 51; 5, с. 30]. Інциденти кіберсаботажу чи кібершпигунства прискорили кіберозброєння. Деякі країни оголосили «кібер» п'ятою військовою сферою (після землі, моря, повітря та космосу), виділяють значні бюджети на розвиток військового кіберпотенціалу [7, с. 222–223; 5, с. 30]. Загальнодоступні документи (національні стратегії, військові доктрини, офіційні заяви) надають докази існування наступальних кіберпотенціалів майже в 50 країнах.

Першим випадком масштабної, приписуваної кібератаки на об'єкт критичної інфраструктури України під час російської війни проти України 2022 року були відсутність сигналу та збій в роботі модемів каліфорнійської фірми Viasat, яка надає послуги Інтернету через супутник. Руйнівна шкідлива програма AcidRain заразила модеми клієнтів Viasat, в тому числі модеми українських збройних сил, які частково покладалися на технологію Viasat для доступу до Інтернету у віддалених районах із незначним покриттям. Це програмне забезпечення видаляло файлові системи модемів і викликало перезавантаження пристрою, модеми не могли відновити підключення. Через три місяці, після вичерпного розслідування збою Viasat, Європейський Союз, уряди Сполученого Королівства, Сполучених Штатів, Канади та Австралії, публічно приписали збій Viasat нападу російської військової розвідки (ГРУ). На сьогоднішній день не було жодних нових російських кібератак на підключену до України критичну інфраструктуру, які можна порівняти за масштабом, складністю та успіхом інциденту з Viasat [23, с. 96–121].

Підстави атрибуції (присвоєння злочинної поведінки) державі містяться в «Статтях про відповідальність за міжнародно-протиправні діяння» 2001 року [24]. У 2013 році Центр передового досвіду спільної кібероборони НАТО (Cooperative Cyber Defence Centre of Excellence, CCDCOE) підготував Талліннський посібник, у якому докладно розроблено імплементацію чинного міжнародного гуманітарного права щодо вступу та ведення війни (jus ad bellum та jus in bello) у кіберпросторі. У 2017 році була опублікована доповнена версія Tallinn Manual 2.0 [25]. Правила 14–18 Талліннського посібника дублюють положення «Статей», адаптуючи їх зміст до кібероперацій. Талліннський посібник розділяє позицію США та Сполученого Великої Британії щодо односторонньої реакції держави на кіберзлочин: вона має відповідати критерію розумності, відповідно до контексту в кожному конкретному випадку. Однак, вживання однією державою контрзаходів проти кіберактивності іншої держави завжди має певний ризик: якщо згодом буде виявлено помилку в атрибуції (приписуванні), держава своєю відповіддю вчинить міжнародне протиправне діяння. «Талліннський посібник» визначив, що кібервійна регулюється тими ж міжнародними правовими рамками, які формують і обмежують інші види використання військової сили. Висновки М. В. Грушко про достатність правил «Таллінського керівництва» для атрибуції поведінки державі і відсутність необхідності подальшої розробки юридичного інструментарію атрибуції є хибними [22, с. 198]. В 2021 році CCDCOE запустив проект Tallinn Manual 3.0 – п'ятирічний процес перегляду існуючих норм визначення та реагування на кіберзагрози, щоб не відставати від існуючої практики застосування міжнародного права в кіберпросторі [26]. Заплановано створення міжнародного органу під назвою Агентство із захисту інформаційної інфраструктури (Agency for Information Infrastructure Protection, AIIP).

Міжнародна відповідальність держав є одним із найдавніших інститутів міжнародного права, при цьому його правові норми досі не кодифіковані і ґрунтуються, як правило, на застосуванні звичаєвих норм, що склалися на базі прецедентів і судових рішень. Виходячи з цього, на думку М. В. Грушко, юридична атрибуція кіберзлочину державі можлива «відповідно до звичаєвих форм відповідальності держави» [22, с. 196], звичаєвого міжнародного права і судової практики Міжнародного Суду. Група експертів ООН у своєму останньому звіті за 2021 рік, а також усі держави-члени ООН при ухваленні звіту відкритої робочої групи ООН (OEWG) за 2021 рік підтвердили, що існуюче міжнародне право та міжнародне гуманітарне право застосовуються до кіберпростору, необхідність заохочування міжнародної спільноти до просування міжнародних норм відповідальної поведінки держав у кіберпросторі і скоординованих відповідей на кіберінциденти в існуючих міжнародних правових рамках.

Висновки. На підставі аналізу особливостей атрибуції кіберзлочинної діяльності та наявної практики технічної, публічної та юридичної атрибуції основні висновки можна сформулювати наступним чином: 1) спеціальні правила щодо атрибуції кібератак відсутні в міжнародному праві; 2) підстави присвоєння поведінки державі містяться в «Статтях про відповідальність за міжнародно-протиправні діяння» 2001 року. «Статті про відповідальність» не мають юридичного обов'язкового характеру, оскільки є доктриною, але більшість норм набула звичаєвого характеру, що виправдовує їх застосування до кібератак; 3) в контексті міжнародної безпеки існує нагальна необхідність об'єднання глобальних зусиль по реалізації ефективного контролю за кіберінцидентами і забезпеченню відповідальної поведінки особливо державних акторів у кіберпросторі; 4) функція контрзаходів – спонукати державу-порушницю виконати свої міжнародні зобов'язання; 5) згідно сучасного звичаєвого міжнародного права і судової практики Міжнародного Суду випереджувальна самооборона, як частина наступальної стратегії боротьби з кіберзагрозами, не визнається контрзаходом; 6) держава, контрзахід якої на кібератаку згодом не проходить перевірку на законність, нестиме відповідальність за протиправність своїх дій; 7) саме юридична атрибуція сприятиме загальновизнаному застосуванню норм і правил міжнародного права до кібероперацій.

ЛІТЕРАТУРА

1. Павлюх О.А., Санжарова Г.Ф. Кіберзлочинність: проблеми дослідження та методи правового реагування. *Актуальні питання юридичної науки в дослідженнях молодих вчених:* збірник матеріалів Всеукраїнської науково-практичної конференції (м. Київ, 18 травня 2023 р.). Одеса: вид. «Юридика», 2023. С. 857–860.

2. World Cybercrime Index. URL: https://www.ox.ac.uk/news/2024-04-10-world -first-cybercrime-index-ranks-countries-cybercrime-threat-level (дата звернення: 28. 09.2024).

3. ENISA Threat Landscape 2024. [130 p.]. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 28.09.2024).

4. National cyber security strategy, 2016–2021. URL:https://assets.publishing. service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (дата звернення: 26.09.2024).
5. Мацелик М.О., Санжарова Г.Ф., Санжаров В.А. Третя національна стратегія кібербезпеки Великої Британії: політика «на майбутнє» в динамічному технічному середовищі. *Юридичний науковий електронний журнал*. 2023. № 9. С. 28–30.
6. Андрейченко С.С. Концепція атрибуції поведінки державі в міжнародному праві : монографія. Одеса : Фенікс, 2015. 578 с.
7. Павлюх О.А., Санжарова Г.Ф., Санжаров В.А. Виклики сучасної кібербезпеки: інституційні і правові відповіді Німеччини. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 3 (12). С. 219–227.
8. Санжарова Г.Ф., Мацелик М.О., Санжаров В.А. Еволюція стратегії кібербезпеки Німеччини протягом останніх трьох десятиліть: інституційний та правничий виміри. *Наукові тренди постіндустріального суспільства:* матеріали IV Міжнародної наукової конференції, м. Суми, 31 березня 2023 р. Вінниця: Європейська наукова платформа, 2023. С. 71–73.
9. Shevchenko A.E., Pavliukh O.A., Sanzharova G F. Germany's National Legal Framework in the Field of Cyber Security. *International scientific conference «Topical issues of modern jurisprudence»: conference proceedings (April 5–6, 2023. Częstochowa, Republic of Poland)*. Riga, Latvia: Baltija Publishing, 2023. P. 38–41.
10. Шевченко А.Є., Павлюх О.А., Санжаров В.А. Питання кібербезпеки в сучасному італійському законодавстві: національний безпековий периметр. *Наукові тренди постіндустріального суспільства:* матеріали IV Міжнародної наукової конференції, м.Суми, 31 березня 2023 р. Вінниця, 2023. С. 80–82.
11. Karpiuk M. The Cybersecurity Strategy of the Republic of Poland as a Source of Internal Law. *Cybersecurity and Law*. 2024. Vol.12 (2). P. 234–245.
12. Karpiuk M., Pizło W., Kaczmarek K. Cybersecurity Management – Current State and Directions of Change. *International Journal of Legal Studies*. 2023. Vol. 14 (2). P. 645–663.
13. Топчій В.В., Бодунова О.М. Система кримінальних правопорушень у сфері інформаційних технологій: міжнародно-правовий вимір. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 1 (10). С. 187–194.
14. Салій А.Я. Особливості відповідальності за кібератаки в країнах ЄС. *Науковий вісник УжНУ. Серія Право*. 2024. Вип. 81 (2). С. 330–334.
15. Музика В.В. Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення: дис. … д-ра філософії: за спеціальністю 081 «Право». Одеса, 2021. 219 с.
16. Egloff F.J. Public attribution of cyber intrusions. *Journal of Cybersecurity*. 2020. Vol. 6 (1). P. 1–12.
17. Egloff F.J., Smeets M. Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*. 2021. Vol. 46 (4). P. 1–32.
18. Egloff F.J. Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy*. 2020. Vol. 41 (1). P. 55–81.
19. Rid T, Buchanan B. Attributing cyber attacks. *Journal of Strategic Studies*. 2015. Vol. 38 (1–2). P. 4–37.
20. Сурілова О.О. Публічна атрибуція кібератак державами-членами ЄС та застосування кіберсанкцій союзом щодо кібератак, які становлять загрозу ЄС та його членам. *Правова держава*. 2021. № 43. С. 209–216.
21. Egloff F., Cavelty M. Attribution and Knowledge Creation Assemblages in Cybersecurity Politics. *Journal of Cybersecurity*. 2021. Vol. 7 (1). P. 1–12.
22. Грушко М.В. Атрибуція кібератак як передумова забезпечення відповідальної поведінки в кіберпросторі. *Правова держава*. 2021. № 43. С.195–201.
23. Givens A.D., Gorbachevsky M., Biernat A.How Putin's Cyberwar Failed in Ukraine. *Journal of Strategic Security*. 2023. Vol. 16 (2). P. 96–121.
24. Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No.10 (A/56/10), chp.IV.E.1. (114 p.) URL: http:// legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
25. Tallinn manual 2.0 on the international law applicable to cyber operations / ed. M.N. Schmitt. Cambridge: Cambridge University Press, 2017.
26. Responsible state behaviour in cyberspace and cyber conflicts: open issues. https://dig.watch/topics/cyberconflict.