УДК 341
DOI https://doi.org/10.32782/2524-0374/2024-2/124

МІЖНАРОДНЕ ПРАВО І КІБЕРБЕЗПЕКА: ВИЗНАЧЕННЯ ПРАВОВОГО СТАТУСУ КІБЕРАТАК ТА КІБЕРВІЙСЬКОВИХ ОПЕРАЦІЙ

INTERNATIONAL LAW AND CYBER SECURITY: DETERMINING THE LEGAL STATUS OF CYBER ATTACKS AND CYBER MILITARY OPERATIONS

Поліщук В.П., аспірант
Міжрегіональна Академія управління персоналом

Панасевич Л.А., капітан юстиції,
старший науковий співробітник науково-дослідної лабораторії проблем правового забезпечення сектору безпеки і оборони науково-дослідного відділу проблем розвитку та впровадження стратегічних комунікацій
Інститут стратегічних комунікацій Національного університету оборони України

Стаття присвячена дослідженню визначення правового статусу кібератак та кібервійськових операцій крізь призму міжнародного права та забезпечення глобальної кібербезпеки. До основних характерних ознак кіберконфліктів, які відмежовують їх від інших загроз національної безпеки віднесено: просторові межі, можливість глобального розвитку в найкоротші терміни, відсутність суб'єктної прив'язки до конкретних дій в кіберпросторі.

Акцентовано увагу на тому, що трансформація конфліктної активності в кіберпростір провокує швидку глобалізацію конфронтації з можливістю залуження міжнародних акторів, які мають вплив на міжнародні процеси.

Враховуючи специфіку кіберпростору, зроблено висновок, що кібератака потенційно може спровокувати міжнародний конфлікт, в тому числі в просторі територіально визначеному, оскільки: а) в умовах глобальної взаємодії інформаційних інфраструктур окремих країн украй важко розрахувати межі й наслідки такої атаки; б) деякі заходи, що вживаються постраждалою стороною, можуть бути непропорційними через складність ідентифікації джерела або можливість помилок у судженнях.

Встановлено, що в інформаційному суспільстві сформовано уявлення про кіберконфлікт як спосіб впливу на масову свідомість, за допомогою спотворення реальності щодо наслідків конфронтації сторін. Результатом кіберконфлікту можуть бути політичні рішення глобального значення, які мають вагомий вплив на процес прийняття найважливіших політичних рішень. Політична еліта використовує результати конфронтації, як площину для легітимації персональних рішень та реалізації цілей геополітичного рівня.

Зазначено, що трансформація у військових атак у кібервійськові є проявом осучаснення ведення військових дій та реалізації глобалізаційних змін. Тому, кібервійськові атаки стають невід'ємною формою існуваннядемократичного устрою, у зв'язку з цим, виникає потреба у формуванні системи реагування органами управління, на небезпеку, яку вони можуть нести суспільству. Проаналізовано досвід Сполучених штатів Америки та Китайської народної республіки щодо впорядкування відносин з приводу забезпечення кібербезпеки.

Ключові слова: кібербезпека, кібератака, кібервійськова операція, глобалізація, конфронтація, міжнародне право.

The article is devoted to the study of determining the legal status of cyber attacks and cyber military operations through the prism of international law and ensuring global cyber security. The article is devoted to the study of determining the legal status of cyber attacks and cyber military operations through the prism of international law and ensuring global cyber security. The main characteristic features of cyber conflicts, which distinguish them from other threats to national security, include: spatial boundaries, the possibility of global development in the shortest possible time, the lack of subject attachment to specific actions in cyberspace.

Attention is focused on the fact that the transformation of conflict activity into cyberspace provokes a rapid globalization of confrontation with the possibility of involving international actors who have an influence on international processes.

Taking into account the specifics of cyberspace, it is concluded that a cyberattack can potentially provoke an international conflict, including in a territorially defined space, because: a) in the conditions of global interaction of the information infrastructures of individual countries, it is extremely difficult to calculate the limits and consequences of such an attack; b) individual measures of the affected party may be disproportionate due to the difficulty of determining the source and the probability of an erroneous assessment of the situation.

It has been established that the information society has formed an idea of cyber conflict as a way of influencing the mass consciousness by distorting reality regarding the consequences of the confrontation between the parties. The result of a cyber conflict can be political decisions of global importance, which have a significant impact on the process of making the most important political decisions. The political elite uses the results of the confrontation as a platform for legitimizing personal decisions and realizing goals at the geopolitical level.

It is noted that the transformation from military attacks to cyber attacks is a manifestation of the modernization of military operations and the implementation of globalization changes. Therefore, cyber military attacks become an integral form of the existence of a democratic system, in connection with this, there is a need for the formation of a system of response by management bodies to the danger that they can bring to society. The experience of the United States of America and the People's Republic of China in regulating relations regarding the provision of cyber security is analyzed.

Key words: cyber security, cyber attack, cyber military operation, globalization, confrontation, international law.

Актуальність дослідження. Станом на теперішній час, все почастішали кібератаки як в Україні, так і в інших державах. Розвиток впорядкування суспільних відносин в напрямку цифровізації є притаманним для багатьох розвинутих країн світу. Однак, для українського суспільства процес нормативної та інституціональної форми трансформації триває в умовах російсько-української війни, яка однозначно встановила єдиний напрямок суспільних інтересів та консолідацію українського суспільства. В умовах формування державних інститутів кібербезпеки та становлення норм права, щодо стабілізації політичних процесів, формується система поглядів на позитивні та негативні стилі поведінки учасників політичного процесу у кіберпросторі, можливі допустимі межі їхньої активності та створення інформаційної публічної бази, яка не шкодить інтересам країни.

Аналіз останніх досліджень та публікацій. Для створення комплексного уявлення про забезпечення кібербезпеки, заслуговують на увагу й праці щодо співробітництва в секторі інформаційної безпеки, яких здійснено такими вченими, як: Д. В. Дубов, В. О. Жадько, Ю. В. Завгородня, Л. І. Кормич, О. І. Харитоненко, Ю. С. Полтавець та іншими. Зарубіжний досвід щодо реакції на кіберконфлікти, кібератаки досліджується й у працях зарубіжних вчених, а саме: Ю. Тор, Р. Горва, М. Смеетс, Т. Рід, Д. Пуйвельде, А. Брантлі тощо. Попри тривалість наукових роз-

відок у сфері інформаційної безпеки, слід визнати, що науковці фрагментарно досліджували питання визначення правового статусу кібератак та кібервійськових операцій, що обумовило актуальність обраної проблематики.

Виклад основного змісту. Основи нормативного регулювання протидії кіберзагрозам містяться у рішенні Ради національної безпеки та оборони України від 29 грудня 2016 року [1], Законі України «Про основні засади забезпечення кібербезпеки України» [2], що стали у 2017 році підґрунтям для сприйняття кібернетичної площини, як повноцінної сфери, яка потребує захисту. Окрім цього, даним законодавчо було надано нормативне визначення поняттям «кіберзлочину», «кібератаки», «критичної інформаційної інфраструктури» та ін. Тобто, визначено, на нормативному рівні, конкретні форми впливу небезпеки в кібернетичній площині.

Ціннісними формами побудови кіберсистеми є уповноваження державних інституцій, які будуть регулятивною та безпековою основою розвитку цифровізованого суспільства. У сфері системи виконавчої влади такою конструктивною основою є Міністерство інформаційної політики України, Міністерство культури України, Міністерство закордонних справ України, Національна рада України з питань телебачення і радіомовлення, Державне агентство України з питань кіно, Державний комітет телебачення і радіомовлення, які створюють умови для реалізації політичних цілей та завдань політичної сили в країні [3]. Окрім того, координацію діяльності органів виконавчої влади з метою реалізації Доктрини та гарантування національної безпеки в інформаційній сфері здійснює Рада національної безпеки та оборони.

Державною службою спеціального зв'язку та захисту інформації України оприлюднено статистику кібератак на українську критичну інформаційну інфраструктуру. Відповідно до якої протягом Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA зафіксувала 60 кібератак. З них: уряд та місцеві органи влади – 11, фінансовий сектор – 6, телеком та програмне забезпечення – 4, сектор безпеки та оборони – 8, комерційний сектор – 6, енергетика – 2, інше – 22 [4].

Основними характерними ознаками кіберконфліктів, які відмежовують їх від інших загроз є: просторові межі, можливість глобального розвитку в найкоротші терміни, відсутність суб'єктної прив'язки до конкретних дій в кіберпросторі (як правило кібератаками займаються компетентні особи з відповідного розпорядження суб'єктів протиборства).

Сучасна політика держави зосереджена на спрощенні бюрократичної системи, економії часу для будь-яких реєстраційних процесів, ефективного користування соціальними гарантіями. Окрім позитивних аспектів існує ряд загроз щодо кібератак для оприлюднення персональних даних, можливості їх використання та видалення з баз даних. Саме такі загрози стоять перед сучасним сектором інформаційної політики з метою захисту та збереження персональної інформації [5]. Оприлюднення персональних даних є однієї з головних небезпек, які можуть бути відкриті у кіберпросторі, оскільки сюди можуть відноситись: данні про членів сім'ї політично-владних суб'єктів (дружина, діти, батьки); данні про наявність рухомого та нерухомого майна в активного політичного діяча та його членів сім'ї; дані про економічні транзакції, які мають сумнівно-незаконний характер та суми, які перевищують офіційні доходи особи та інші відомості, які можуть нашкодити діяльності політичного діяча. Адже, можливість створювати безлад в системі інформації, заводить суспільство в панівні настрої, а тому є тим негативним чинником, якого прагнуть сторони протидії, тобто зміна свідомості відносно сприйняття політичної сили чи політичного лідера.

Окрім того, трансформація конфліктної активності в кіберпростір провокує швидку глобалізацію конфронтації з можливістю залуження міжнародних акторів, які мають вплив на міжнародні процеси. В сучасному світі, на думку Н. Ржевської, «найефективнішим інструментарієм інформаційно-психологічного впливу на потенційні об'єкти конфлікту є засоби масової інформації. Інформаційне середовище геополітичного конфлікту формується і підтримується діяльністю засобів масової інформації. Найчастіше саме ЗМІ є головною ланкою в інформаційному полі міжнародного конфлікту. Бурхливе зростання тимчасових електронних ЗМІ та прискорений розвиток інформаційних технологій наблизили до реальності проєкти створення комплексних інформаційних систем найвищого рівня» [6].

Звичайно, роль інформаційних каналів досить актуальна, бо сучасні міжнародні конфлікти переважно реалізуються в медійному просторі, у формі боротьби за усвідомлення національних та міжнародних політичних процесів. А тому, вагому роль відіграють нормативні процеси, що є механізмом реалізації публічної риторики політичних лідерів, демонстрація їх вектору політики та рівень відповідності слів і дій. Якщо конфлікт заходить у крайню фазу свого розвитку, військове протиборство, то Н. Ржевська вдало відзначає про роль комунікаційних ресурсів поряд з військовою технікою, яка є важливою для сприйняття суспільством, тому військові дії підкріплюються інформаційними війнами.

Враховуючи особливості кіберпростору, кібератаки як форма політичного кіберконфлікту можуть призводити до міжнародних конфліктів, що охоплюють територіально визначені зони. З одного боку, прорахувати межі та наслідки таких атак в умовах глобальної взаємодії інформаційних інфраструктур окремих країн вкрай складно, а з іншого – складність ідентифікації джерела та висока ймовірність неправильної оцінки ситуації можуть призвести до непропорційних індивідуальних заходів з боку постраждалої сторони Потенціал. Це може призвести до відкритого військового конфлікту із застосуванням звичайних озброєнь [7].

Окрім того, не варто виключати психологічні технології, які вдало діють в інформаційній площині. Коли в умовах повного інформаційного хаосу відбувається процес формування керованого переговорного стану. Інформаційні та психологічні технології можуть перетворити міжнародні конфлікти на мир [6, с. 46].

Оскільки, в інформаційному суспільстві формується уявлення про кіберконфлікт, негативні наслідки його ескалації. У зв'язку з цим, можемо відзначити, що інформаційне протиборство здійснюється для впливу на масову свідомість, за допомогою спотворення реальності щодо наслідків конфронтації сторін. Результатом кіберконфлікту можуть бути політичні рішення глобального значення. Звичайно, результати кіберконфліктів мають вагомий вплив на процес прийняття найважливіших у світі політичних рішень. Політична еліта використовує результати конфронтації, як площину для легітимації персональних рішень та реалізації цілей геополітичного рівня.

Тому, трансформація у військових атак у кібервійськові є проявом осучаснення ведення військових дій та реалізації глобалізаційних змін. Тому, кібервійськові атаки стають невід'ємною формою існуваннядемократичного устрою, у зв'язку з цим, виникає потреба у формуванні системи реагування органами управління, на небезпеку, яку вони можуть нести суспільству.

Натомість функцію е-демократії можна розглядати як модель електронного уряду, що гарантує двосторонню політичну комунікацію та участь недержавних суб'єктів у процесі прийняття рішень. Дуже важливим є забезпечення правдивість інформації, в умовах відсутності дієвої міри відповідальності, яка регламентована в праві з чіткою процедурою застосування. В свою чергу, виникає необхідність у цифровій трансформації, як діяльності

направленій на пошук ефективних механізмів захисту інформаційного середовища.

Сучасний міжнародний досвід щодо реакції на кібератаки, або окремі форми прояву кіберборотьби, зводиться до практики глобальних учасників, на внутрішньому та зовнішньому рівні щодо реалізації кібервпливу на політичні процеси. Дієвими зразками впливу, які продовжують розвиватись є досвід Сполучених Штатів Америки та Китайської народної республіки. Їх діяльність трансформується в співпрацю з країнами-однодумцями та міжнародними організаціями, які переслідують принципи, щодо спільної боротьби та співпраці у галузі кібербезпеки. Ще у 2003 році була опублікована Національна стратегія безпеки кіберпростору США (National Strategy to Secure Cyberspace) [8]. Це період коли в Україні розпочинався процес використання комп'ютерів та ноутбуків в індивідуальній діяльності, а про будь-які процеси захисту чи боротьби не було актуальної потреби. Однак, у США стратегія захисту кіберпростору стала частиною загально-національної безпеки. NSSC проголошує три стратегічні цілі, а саме: 1) захист від кібератак критичних інфраструктур США; 2) мінімізація збитків та часу відновлення від кібератак; 3) зменшення вразливості від кібератак в загальнонаціональному масштабі [9]. У квітні 2015 року був підписаний указ «Про арешт власності осіб, причетних до серйозних протиправних дій у кіберпросторі», суть його в побудові системи відповідальності за протиправні дії в кіберпросторі. Сполучені Штати розробили правові умови для застосування санкцій до компаній та осіб, причетних до кібератак, які порушують стабільне функціонування критично важливої інфраструктури США та ключових комп'ютерних мереж і систем. Відповідні санкції також мають бути накладені на осіб і компанії, які привласнюють кошти або інші активи, такі як комерційна таємниця, персональні дані або фінансова інформація американських компаній і організацій через кібератаки, або свідомо використовують такі активи, викрадені третіми особами в ході кібератак. Окрім цього, процес розвитку потенційного захисту від будь-яких провокативних атак в США, чи публічних висловлювань в інформаційному просторі досить уважно прослідковується та викорінюється.

Ще однією інформаційно прогресивною країною на глобальному рівні є Китай. В сучасному глобальному інформаційному просторі існує достатня свобода щодо світосприйняття та висловлювань в напрямку політичних процесів. В кіберпросторі Китайська народна республіка, за останнє десятиріччя, також формує власну систему дій щодо укріплення національного інформаційного суверенітету, що створює двозначну форму сприйняття у світі: з одного боку, це трактується як спроба руйнації цілісності мережі Інтернет, а з іншого, як захист державницьких інтересів з жорсткою системою реагування та санкціонування. Ще однією важливою складовою є кількість користувачів мережі Інтернет, яка в Китаї досить велика. Так до прикладу у 2013 році показники користувачів Інтернет у КНР та користувачів Інтернет в усьому ЄС перевищувались у рази [10]. Звичайно, одним із пріоритетів, є чисельність населення та прогресивний розвиток Китаю, який відбувається досить швидко. В свою чергу у Європі спостерігається старіння населення та значне зменшення чисельності молодих людей, які є рушієм прогресу та сприйняття новітніх розробок. На думку Дубова Д. В. у Китаї умовно можливо виокремити два основні напрями контролю. Перший напрям так званого «низького рівня», а другий «високого рівня». Перший рівень контролює не технологічні, а регуляційні та організаційні методики котрі стосуються цензури, тобто допустимості окремого контенту, його непорушності національних інтересів. Другий «Високий рівень» здійснення контролю, передбачає обмеження поширення так званої небажаної інформації, яка пов'язана з інформаційно-кібернетичними технологіями, з метою контролю над внутрішнім станом суспільства, впливом на його свідомість. Сучасники називають це новим виміром для прояву домінування в просторі країни [11].

Україна в сучасних умовах війни з 2014 року досить часто відчувала вплив на систему захисту об'єктів критичної інфраструктури, що сформувало необхідність нормативного регулювання, розвитку кіберзахисту, формування відповідних інститутів державного регулювання питань безпеки в інформаційній сфері.

В умовах консолідації прогресивних, мирних країн світу формуються умови для спільної міждержавної боротьби з кібератаками. У серпні 2022 р. між Україною та Польщею підписано меморандум про співпрацю у сфері кіберзахисту [12]. Також на Мадридському саміті НАТО оголосило про нову програму швидкого реагування на кібератаки. Альянс також пообіцяв посилити кіберзахист України перед обличчям постійних російських атак. Адже, Росія систематично здійснює кібератаки на енергетику, банківську систему та інші критичні для економіки України об'єкти. Важливу роль відіграють нормативні акти НАТО, спрямовані на вирішення поточних питань у кіберпросторі і які відображають сучасні виклики інформаційних загроз, наприклад, Комплексна політика НАТО з кіберзахисту, спрямована на забезпечення мирного і безпечного кіберпростору [13]. Альянсом проголошено, що кіберпростір належить до сфери відповідальності та діяльності НАТО, а кібероборона є основною в сучасному інформаційному світі [14].

Щодо співпраці України з НАТО у сфері запобігання та врегулювання конфліктів у кіберпросторі, зазначимо, що у 2018 році Україна розпочала розбудову системи захисту кіберпростору за натовським зразком. Така трансформація є проявом необхідності в нинішньому становищі України. Однак у практичній реалізації поставлених завдань українські фахівці продемонстрували високу та розвинену спроможність реагувати на нові виклики [15]. Так, нова редакція Стратегії кібербезпеки України, регламентує вагомим елементом інтеграцію з системою кіберзахисту НАТО, бо боротьба України з кіберзагрозами стала досить актуальною в сучасному інформаційно-політичному просторі. Адже, ефективна політична система тоді, коли ефективні органи управління. Основними викликами у сфері кібербезпеки України є активне використання кіберінструментів у міжнародній конкуренції та вираження індивідуального впливу на глобальному рівні, а також конкурентний характер розвитку засобів кібербезпеки в умовах швидких змін в інформаційно-комунікаційних технологіях, зокрема хмарних та квантових обчислень, мереж 5G, великих даних, інтернету речей та штучного інтелекту [16].

Актуальною загрозою, яку виділено в стратегії, і яка фактично реалізована країною агресором на території України – «мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі» [16]. Сучасна російсько-українська війна демонструє використання спецслужбами інформації, яку громадяни публікують публічно в соціальних мережах [17]. Окрім того, для політичних лідерів соціальні мережі стали майданчиком публічного спілкування з населенням в умовах війни та формою звіту про виконану та плановану роботу. А відеоролики, які з'являються в соціальних мережах розцінюють, як прямі публічні звернення уповноважених осіб до суспільства. Тому, агресор використовує будь-яку інформацію, яка може допомогти.

Держава-агресор активно використовує кіберпростір. Основною формою цього є створення арсеналу наступальної кіберзброї, застосування якої є незворотнім і може мати незворотні деструктивні наслідки. Водночас інформа-

ційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури зазнають впливу, спрямованого на виведення їх з ладу (кібердиверсії), отримання негласного доступу та управління, ведення розвідувально-підривної діяльності.

Висновки. Підсумовуючи зазначимо, що об'єднання України у боротьбі з кіберзагрозами з окремими країнами чи міжнародними безпековими організаціями є шляхом обміну досвідом та практичними заняттями по боротьбі з агресорами. Кібератаки є інструментом впливу, який також активно виступає елементом спеціальних розвідувальних операцій для маніпулювання населенням та дискредитації України як держави. Також, вони використовувались під час виборчих компаній в країні та могли бути неправильно трактовані, як «чорний піар» та виборчі технології. Разом з тим, негативну складову кіберборотьби не варто виключати, бо шкода її для суспільства та держави є суттєвою та потребує значного часу для відновлення. А тому, робота по вдосконаленню системи органів швидкого реагування потребує вдосконалення, а відповідно нормативна система повинна відповідати викликам часу, що демонструє потребу у фахівцях інформаційного спрямування.

ЛІТЕРАТУРА

1. Доктрина інформаційної безпеки : Указ Президента України від 25.02.2017 № 47/2017. Офіційний веб-портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 08.02.2024).
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Офіційний веб-портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 08.02.2024).
3. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експерті. Центр досліджень соціальних комунікацій НБУВ. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2759:doktrina-informatsijnoji-bezpeki-yak-zasib-protidiji-informatsijnim-zagrozam&catid=8& Itemid=350 (дата звернення: 08.02.2024).
4. Статистика кібератак на українську критичну інформаційну інфраструктуру: 15–22 березня. Офіційний веб-портал Державної служби спеціального зв'язку та захисту інформації України. 2022. URL: https://www.cip.gov.ua/ua/news/statistika-kiberatak-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya (дата звернення: 08.02.2024).
5. Завгородня Ю.В. Кіберконфлікти як сучасна загроза цифровізації суспільства: політичний аспект. *Актуальні проблеми філософії та соціології.* 2022. № 35. С. 90.
6. Ржевська Н.Ф. Геоінформаційний чинник, як механізм трансформації міжнародних конфліктів. *Вісник Донецького національного університету. Політичні науки*. 2016. С. 45–46.
7. Ожеван М. Фронти й тили великих інформаційних війн: загальні інформаційні потреби та інтереси. *Підприємництво в Україні*. 2001. № 4(5). С. 20.
8. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навч. посіб. / за заг. ред. В.О. Жадька ; ред.-упор. О.І. Харитоненко, Ю.С. Полтавець. Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.
9. The National Strategy to Secure Cyberspace. U.S. government via Department of Homeland Security (February 2003). URL: https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf (дата звернення: 08.02.2024).
10. Zavhorodnia Yu. Features of protection of China's national interests within cybernetic space. *European Political and Law Discourse.* 2021. Volume 8. Issue 6. P. 38.
11. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 190 с.
12. Костюкова Ю. Польща та Україна підписали меморандум про співпрацю у сфері кіберзахисту. Вебсайт mind.ua. 22.08.2022. URL: https://mind.ua/news/20245980-polshcha-ta-ukrayina-pidpisali-memorandum-pro-spivpracyu-u-sferi-kiberzahistu (дата звернення: 08.02.2024).
13. Лідери країн НАТО схвалили комплексну політику кіберзахисту альянсу. Вебсайт Інтерфакс-Україна. 14.06.2021. URL: https://ua.interfax.com.ua/news/general/750063.html (дата звернення: 08.02.2024).
14. Гвоздь В. Кіберконфлікт і геополітика – новий фронт «холодної війни». *Європа загальних цінностей або Європа спільних інтересів?* : матеріали 28-ого економічного форуму, м. Криниця-Здруй, Польща, 4-6 вересня 2018 р. Криниця-Здруй, Польща, 2018. URL: https://bintel.org.ua/nash_archiv/arxiv-voyenni-pitannya/arxiv-gibridnia-vijna/09_05_krynica/ (дата звернення: 08.02.2024).
15. Завгородня Ю.В. Роль НАТО у боротьбі з кіберконфліктами. *Регіональні студії*. 2022. № 30. С. 67.
16. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України №447/2021. Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 08.02.2024).
17. Zavhorodnia Yu.V. Political conflicts as a prerequisite for the Russian-Ukrainian war: manipulative features. The Russian-Ukrainian war (2014–2022): historical, political, cultural-educational, religious, economic, and legal aspects : Scientific monograph. Riga, Latvia : «Baltija Publishing», 2022. С. 911. 1436 p).