УДК 341.1/.8:355.01
DOI 10.33244/2617-4154.2(23).2026.414-423

К. С. Лісова,
кандидат історичних наук, доцент,
доцент кафедри міжнародного права та права Європейського Союзу,
Державний податковий університет
K. S. Lisova,
Candidate of History, Associate Professor, Associate Professor of the Department of International Law and Law of the European Union,
State Tax University
email: Lisova.k@ukr.net
ORCID 0000-0002-2664-7721;
В. Ю. Іскович,
здобувач вищої освіти Навчально-наукового інституту права,
Державний податковий університет
V. Yu. Iskovich,
student of higher education at the Educational and Scientific Institute of Law,
State Tax University
email: pozityv228@gmail.com
ORCID 0009-0008-0820-6720

ГІБРИДНІ ЗАГРОЗИ ТА ЇХ ВПЛИВ НА ТРАНСФОРМАЦІЮ МІЖНАРОДНО-ПРАВОВИХ НОРМ

HYBRID THREATS AND THEIR IMPACT ON THE TRANSFORMATION OF INTERNATIONAL LEGAL NORMS

У статті досліджено сутності гібридних загроз як сучасного феномена міжнародних відносин, а також визначено їхній вплив на трансформацію міжнародно-правових норм і механізмів забезпечення безпеки. Особлива увага приділяється ролі українського досвіду у формуванні нових підходів до правового регулювання гібридної агресії.

У дослідженні використано загальнонаукові та спеціально-юридичні методи, зокрема системний аналіз, порівняльно-правовий метод, формально-юридичний підхід, а також метод узагальнення наукових джерел. Застосовано міждисциплінарний підхід до вивчення гібридних загроз як багатовимірного явища, що охоплює військову, інформаційну,

економічну та кібернетичну сфери. Додатково використано аналітичні дані щодо ефективності інструментів протидії гібридним загрозам.

Встановлено, що гібридні загрози спричиняють суттєві зміни в міжнародному праві, зокрема розширення поняття агресії за рахунок внесення кібероперацій та інформаційних впливів. Виявлено трансформацію підходів до відповідальності держав, що зумовлює потребу в удосконаленні механізмів атрибуції дій у складних багаторівневих конфліктах. Доведено зростання ролі міжнародних організацій у формуванні колективних механізмів безпеки та адаптації стратегій до нових викликів. Обґрунтовано активізацію розвитку міжнародного гуманітарного права в умовах нетрадиційних форм конфліктів. Визначено, що український досвід протидії гібридній агресії став важливим чинником переосмислення міжнародно-правових категорій і сприяв формуванню нових підходів до кваліфікації агресії та відповідальності. Проаналізовано ефективність основних інструментів протидії, серед яких найбільш дієвими є військове стримування та економічні санкції, тоді як міжнародно-правові механізми потребують подальшого вдосконалення.

Зроблено висновок, що гібридні загрози є системним викликом для сучасного міжнародного права, який зумовлює його еволюцію та адаптацію до нових реалій. Трансформація правових норм проявляється в розширенні змісту ключових категорій, розвитку інструментів відповідальності та посиленні ролі інституційних механізмів. Обґрунтовано потребу в подальшій розробці універсальних міжнародно-правових підходів до регулювання гібридних конфліктів, що враховуватимуть їхній комплексний та динамічний характер.

Ключові слова: *гібридні загрози, міжнародне право, агресія, кібербезпека, інформаційна війна, санкції, міжнародна безпека, Україна.*

The aim of this study is to conduct a comprehensive analysis of the nature of hybrid threats as a contemporary phenomenon in international relations, as well as to determine their impact on the transformation of international legal norms and security mechanisms. Particular attention is paid to the role of Ukraine's experience in shaping new approaches to the legal regulation of hybrid aggression.

The study employs general scientific and specialized legal methods, including systemic analysis, the comparative legal method, the formal-legal approach, and the method of synthesizing scientific sources. An interdisciplinary approach is applied to the study of hybrid threats as a multidimensional phenomenon encompassing the military, informational, economic, and cyber spheres. Additionally, analytical data on the effectiveness of tools for countering hybrid threats are utilized.

It has been established that hybrid threats cause significant changes in international law, in particular the expansion of the concept of aggression through the inclusion of cyber operations and information influence. A transformation in approaches to state responsibility has been identified, necessitating the improvement of mechanisms for attributing actions in complex, multi-level conflicts. The growing role of international organizations in shaping collective security mechanisms and adapting strategies to new challenges has been demonstrated. The need to intensify the development of international humanitarian law in the context of non-traditional forms of conflict has been substantiated.

It has been determined that Ukraine's experience in countering hybrid aggression has become an important factor in rethinking categories of international law and has contributed to the development of new approaches to the classification of aggression and liability. The effectiveness of the main countermeasures has been analyzed; among them, military deterrence and economic sanctions are the most effective, while international legal mechanisms require further improvement.

It is concluded that hybrid threats pose a systemic challenge to modern international law, driving its evolution and adaptation to new realities. The transformation of legal norms manifests itself in the expansion of the content of key categories, the development of accountability instruments, and the strengthening of the role of institutional mechanisms. The necessity of further developing universal international legal approaches to regulating hybrid conflicts, which will take into account their complex and dynamic nature, is substantiated.

Keywords: *hybrid threats, international law, aggression, cybersecurity, information warfare, sanctions, international security, Ukraine.*

Постановка проблеми. Поняття гібридних загроз є порівняно новим для міжнародного права й не має єдиного універсального визначення, що зумовлює наукові дискусії щодо його змісту та правової природи. У сучасній науковій літературі гібридні загрози розглядаються як комплексне явище, що поєднує різноманітні інструменти впливу (військові, політичні, економічні, інформаційні та кібернетичні), які застосовуються державами.

Особливістю гібридних загроз є їх багатовимірність, прихований характер і складність ідентифікації джерела агресії, що підриває традиційні механізми забезпечення міжнародної безпеки. Вони часто реалізуються через поєднання відкритих і латентних форм впливу, охоплюючи інформаційні кампанії, кібератаки, економічний тиск, використання проксі-суб'єктів, що унеможливлює чітке розмежування між станом війни та миру. У зв'язку з цим класичні підходи міжнародного права, які ґрунтуються на чітких категоріях збройного конфлікту та агресії, виявляються недостатніми для адекватного реагування на новітні виклики.

Актуальність дослідження посилюється трансформацією глобального безпекового середовища, в якому гібридні загрози стають домінантною формою протистояння між державами. Особливої гостроти ця проблема набула в контексті агресії проти України, що продемонструвала практичне застосування широкого спектра гібридних інструментів та виявила обмеженість наявних міжнародно-правових механізмів реагування. За таких умов виникає об'єктивна потреба в переосмисленні традиційних правових підходів, удосконаленні категоріального апарату міжнародного права та розробці ефективних механізмів протидії гібридним загрозам.

Аналіз останніх досліджень і публікацій. У сучасній науковій літературі проблематика гібридних загроз та їхнього впливу на міжнародне право активно досліджується як українськими, так і зарубіжними науковцями. Значний внесок у розробку цієї тематики зробили такі українські дослідники, як А. В. Тарасюк, В. П. Кононенко, М. С. Тєтєвін,

Р. В. Черниш, О. С. Вареник, О. М. Поляков, а також інші автори, які аналізують трансформаційні процеси у сфері міжнародної безпеки в умовах новітніх викликів.

Зокрема, у працях А. В. Тарасюк обґрунтовується потреба в перегляді класичних підходів до визначення агресії з урахуванням цифрових та інформаційних форм впливу, які мають деструктивні наслідки й можуть прирівнюватися до традиційних військових засобів [5]. В. П. Кононенко досліджує інформаційну безпеку як ключовий елемент сучасного безпекового середовища, акцентуючи увагу на трансформації безпекових відносин під впливом цифровізації та зростанні ролі інформаційних операцій як інструменту стратегічного впливу [3].

Вагомим є внесок О. С. Вареник, яка аналізує тенденції міжнародного співробітництва у сфері кібербезпеки, підкреслюючи потребу в посиленні координації між державами та міжнародними інституціями в протидії кіберзагрозам [2]. О. М. Поляков у своїх дослідженнях розглядає способи активізації міжнародної співпраці у сфері кібербезпеки та наголошує на потребі у вдосконаленні правових механізмів взаємодії держав у сучасних умовах [4].

М. С. Тєтєвін приділяє увагу досвіду України у сфері міжнародного співробітництва з питань кібербезпеки, акцентуючи на важливості інтеграції національних механізмів у глобальні безпекові системи. Р. В. Черниш досліджує міжнародний організаційний досвід забезпечення кібербезпеки та підкреслює роль міжнародних інституцій у формуванні ефективних механізмів реагування на новітні загрози [6].

Окрему увагу заслуговують праці, присвячені безпосередньо феномену гібридної війни. Зокрема, В. П. Горбулін ще на початкових етапах формування цього поняття наголошував на комплексному характері гібридних конфліктів та їх здатності поєднувати військові й невійськові інструменти впливу, що значною мірою передбачило подальший розвиток наукових підходів до цієї проблематики [8].

Серед зарубіжних досліджень варто зазначити роботи, присвячені аналізу кібербезпеки, інформаційних операцій, санкційної політики та ролі міжнародних організацій у протидії гібридним загрозам. У цих публікаціях (зокрема, за останні п’ять років) розглядаються питання кваліфікації кібератак як акту агресії, удосконалення механізмів міжнародної відповідальності держав, а також розвитку колективних інструментів безпеки.

Аналіз наукових джерел свідчить про наявність різних підходів до розуміння сутності гібридних загроз. Частина дослідників розглядає їх переважно як військово-політичне явище, інші – як комплексний міждисциплінарний феномен, що охоплює економічну, інформаційну та кібернетичну складові. Водночас спостерігаються певні розбіжності в підходах до визначення меж гібридної агресії та критеріїв її кваліфікації, що свідчить про відсутність усталеного наукового консенсусу.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значну кількість досліджень, низка важливих аспектів залишається недостатньо розкритою. Зокрема, потребують подальшого наукового опрацювання питання комплексної адаптації міжнародно-правових норм до гібридних форм конфліктів, удосконалення механізмів атрибуції дій держав у кіберпросторі, а також визначення ролі санкцій як повноцінного інструменту міжнародно-правового регулювання. Крім того, недостатньо

дослідженим залишається питання інтеграції національного досвіду (зокрема, України) у формування універсальних міжнародно-правових підходів до протидії гібридним загрозам.

Причинами цього є швидкий розвиток технологій, динамічність глобального безпекового середовища та випереджальний характер гібридних загроз порівняно з нормативно-правовим регулюванням. У зв'язку з цим виникає об'єктивна потреба в подальших дослідженнях, спрямованих на формування цілісної концепції правового реагування на гібридні виклики, що й обумовлює актуальність цієї статті.

З урахуванням викладеного, доцільно виокремити низку невирішених наукових питань, що потребують подальшого дослідження. Зокрема, дискусійними залишаються питання визначення правової природи гібридних загроз у системі міжнародного права, встановлення чітких критеріїв кваліфікації кібероперацій та інформаційних впливів як акту агресії, а також удосконалення механізмів міжнародно-правової відповідальності держав в умовах використання непрямих форм впливу. Окремої уваги потребує проблема інтеграції національного досвіду, зокрема України, у формування універсальних міжнародно-правових підходів до протидії гібридним загрозам.

Вирішення зазначених питань має важливе значення для забезпечення ефективності міжнародно-правового регулювання сучасних конфліктів, оскільки відсутність чітких правових механізмів ускладнює реагування міжнародної спільноти на новітні виклики безпеки.

Отже, аналіз сучасних наукових підходів свідчить про наявність низки невирішених теоретичних і практичних проблем у сфері правового регулювання гібридних загроз. Зокрема, відсутність єдиного підходу до визначення їхньої правової природи, нечіткість критеріїв кваліфікації новітніх форм агресії, а також недостатня ефективність механізмів міжнародно-правової відповідальності зумовлюють потребу в подальшому комплексному дослідженні. Вирішення цих питань є важливим для формування ефективної системи міжнародної безпеки та вдосконалення правових механізмів реагування на сучасні виклики.

Метою статті є комплексний аналіз впливу гібридних загроз на трансформацію міжнародного права, зокрема в частині розширення поняття агресії, удосконалення механізмів відповідальності держав та розвитку інституційних і правових інструментів протидії. Для досягнення поставленої мети передбачено вирішення таких завдань: проаналізувати наявні наукові підходи до визначення гібридних загроз; визначити основні напрями трансформації міжнародно-правових норм; дослідити проблеми атрибуції дій держав у кіберпросторі; обґрунтувати роль українського досвіду у формуванні нових підходів до міжнародно-правового регулювання.

Виклад основного матеріалу. Аналіз впливу гібридних загроз на міжнародне право дає змогу виокремити кілька ключових напрямів його трансформації.

По-перше, відбувається розширення поняття агресії. Традиційне визначення агресії, закріплене в резолюціях ООН, не охоплює багатьох сучасних форм впливу, зокрема кібератак та інформаційних операцій. У зв'язку з цим поступово формується підхід, відповідно до якого новітні форми ворожих дій можуть розглядатися як складові

агресії. Особливого значення набуває питання кваліфікації масштабних кібератак як акту агресії, оскільки їхні наслідки можуть бути зіставними з традиційними військовими діями. Отже, сучасні безпекові виклики зумовлюють потребу в перегляді класичних міжнародно-правових підходів і розширенні змісту відповідних категорій за рахунок внесення цифрових та інформаційних форм впливу.

По-друге, спостерігається зміна підходів до відповідальності держав. У разі гібридної агресії доведення прямої причетності держави до конкретних дій значно ускладнюється, оскільки часто використовуються посередники, приватні військові структури або анонімні кіберсуб'єкти. Це зумовлює потребу в удосконаленні механізмів встановлення відповідальності, зокрема через розширення критеріїв атрибуції дій державі та вдосконалення процедур доказування. У сучасних умовах традиційні підходи до відповідальності виявляються недостатньо ефективними, що потребує їхньої адаптації до нових форм загроз.

По-третє, посилюється роль міжнародних організацій у забезпеченні безпеки. Такі організації, як ООН, НАТО та ЄС, поступово адаптують свої стратегії до нових умов, розробляючи комплексні механізми протидії гібридним загрозам. Це охоплює створення спеціалізованих структур, розвиток стратегій кібербезпеки, а також впровадження інструментів інформаційної протидії. Важливим чинником стає здатність інституцій швидко реагувати на динамічні виклики, що передбачає інтеграцію інноваційних підходів, автоматизацію процесів та використання цифрових технологій.

По-четверте, активізується розвиток міжнародного гуманітарного права в контексті нових форм конфліктів. Гібридні війни супроводжуються порушенням прав людини, використанням цивільної інфраструктури у військових цілях і маніпуляціями інформаційним простором. Це зумовлює потребу в адаптації наявних норм до нових реалій, а також перегляду підходів до забезпечення гуманітарних принципів у сучасних конфліктах. Особливої актуальності набуває питання дотримання етичних стандартів навіть в умовах складних і нестандартних форм протистояння.

Окремої уваги заслуговує український досвід, який відіграє системоутворювальну роль у трансформації сучасного міжнародного права. Саме на прикладі протидії гібридній агресії проти України міжнародна спільнота отримала практичний матеріал для переосмислення наявних правових підходів. Події, що розпочалися 2014 року та набули особливої інтенсивності після повномасштабного вторгнення 2022 року, продемонстрували обмеженість традиційних категорій міжнародного права, зокрема понять «збройна агресія», «війна» та «окупація». Це зумовило потребу в їхньому уточненні та розширенні з урахуванням комплексного характеру сучасних загроз, які поєднують військові, інформаційні, економічні, кібернетичні та політичні інструменти впливу. У цьому контексті Україна фактично є як практична платформа для формування нових міжнародно-правових механізмів реагування на гібридні виклики [3].

Важливо підкреслити, що гібридна агресія проти України охоплює широкий спектр дій: від прямого військового вторгнення та окупації територій до масштабних інформаційних кампаній, кібератак на критичну інфраструктуру, економічного тиску, енергетичного шантажу та використання міжнародних інституцій у власних інтересах. У зв'язку з цим

міжнародне право поступово відходить від вузького трактування агресії як виключно військового вторгнення й починає розглядати її як багатовимірне явище, що потребує комплексного правового регулювання [8].

У цьому контексті Україна є ініціатором нових підходів до визначення агресії та відповідальності за неї. Зокрема, на міжнародному рівні активно обговорюється потреба в розширенні юрисдикції міжнародних судових інституцій для розгляду справ, пов'язаних із гібридними загрозами, охоплюючи кіберзлочини, інформаційні атаки та економічні маніпуляції. Україна також наполягає на створенні спеціального міжнародного трибуналу стосовно злочину агресії, що є важливим кроком у напрямі зміцнення механізмів притягнення до відповідальності держави-агресора [2].

Окремої уваги заслуговує розвиток санкційного механізму як одного із ключових інструментів протидії гібридним загрозам. У сучасних умовах санкції перестають бути лише допоміжним засобом і набувають статусу повноцінного елементу міжнародно-правового реагування. Економічні обмеження, замороження активів, відключення від міжнародних фінансових систем, обмеження експорту технологій та енергоресурсів – усе це формує нову модель впливу на агресора, яка дає змогу досягати стратегічних результатів без прямого військового втручання. Важливо, що санкційна політика щодо Російської Федерації стала безпрецедентною за масштабами: за різним оцінюванням, запроваджено тисячі індивідуальних та секторальних санкцій, які суттєво вплинули на економічний потенціал держави-агресора.

Крім того, санкції дедалі більше інтегруються в правову систему міжнародних відносин як інструмент превенції. Вони використовуються не лише як реакція на вже вчинену агресію, але й як засіб стримування потенційних загроз. Це свідчить про поступове формування нової парадигми міжнародного права, в якій економічні та фінансові інструменти відіграють не меншу роль, ніж традиційні військові механізми [6].

Ще одним важливим напрямом трансформації є інтеграція національних правових систем у глобальний процес протидії гібридним загрозам. Україна, реагуючи на виклики, активно реформує власне законодавство, зокрема у сфері національної безпеки, кіберзахисту, інформаційної політики та протидії дезінформації. Водночас ці зміни відбуваються в тісній координації з міжнародними партнерами, що сприяє уніфікації підходів та створенню спільного правового простору для протидії гібридним викликам.

У цьому аспекті варто звернути увагу на те, що держави світу дедалі частіше вносять елементи боротьби з гібридними загрозами до своїх національних стратегій безпеки. Це передбачає розробку комплексних механізмів реагування, які охоплюють як військову сферу, так і інформаційний, економічний та кіберпростір. Такий підхід свідчить про усвідомлення багатовимірності сучасних загроз і потребу в міждисциплінарному правовому регулюванні [11].

З метою більш наочного відображення ефективності різних інструментів протидії гібридним загрозам доцільно проаналізувати їхній вплив у відсотковому співвідношенні, що наведено в таблиці 1.

Таблиця 1 – Оцінювання ефективності інструментів протидії гібридним загрозам (за міжнародним аналітичним оцінюванням)

Інструмент протидії	Рівень ефективності	Частка застосування
Економічні санкції	75 %	90 %
Кіберзахист та кібероперації	68 %	80 %
Інформаційна протидія (контрпропаганда)	60 %	85 %
Дипломатичний тиск	55 %	70 %
Військове стримування	82 %	65 %
Міжнародно-правові механізми	50 %	60 %

Джерело: розроблено авторами.

Як видно з наведених даних таблиці 1, найбільш ефективним інструментом залишається військове стримування, однак його застосування є обмеженим через високі ризики ескалації. Водночас економічні санкції демонструють високий рівень ефективності та найбільшу частку застосування, що підтверджує їх ключову роль у сучасній системі міжнародної безпеки. Кіберзахист і інформаційна протидія також займають важливе місце, що свідчить про зростання значення нематеріальних чинників у міжнародних конфліктах [10]. Водночас порівняно нижча ефективність міжнародно-правових механізмів вказує на потребу в їхньому подальшому вдосконаленні та адаптації до нових реалій.

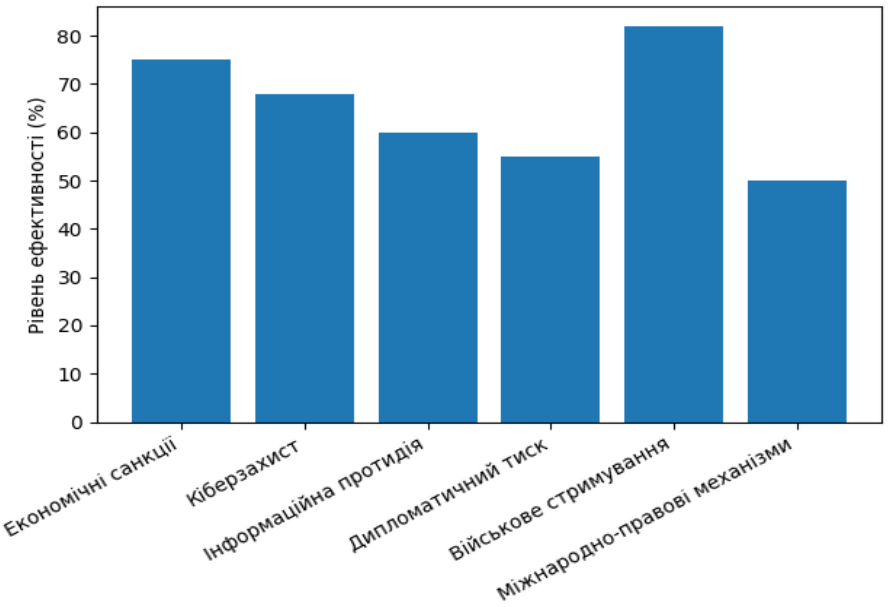

Рисунок 1 – Оцінювання ефективності інструментів протидії гібридним загрозам (за міжнародним аналітичним оцінюванням)

Висновки. Отже, гібридні загрози є одним із ключових викликів сучасності, що суттєво впливають на розвиток міжнародного права. Їх багатовимірний характер і складність ідентифікації зумовлюють потребу в переосмисленні традиційних правових підходів до забезпечення міжнародної безпеки. Повномасштабне вторгнення Російської Федерації в Україну стало каталізатором цих процесів, продемонструвавши обмеженість наявних механізмів і потребу в їхній модернізації.

Трансформація міжнародно-правових норм проявляється в розширенні поняття агресії, удосконаленні механізмів відповідальності держав, посиленні ролі міжнародних організацій і розвитку нових інструментів протидії, як-от санкції та кібербезпека. Водночас цей процес потребує подальшого розвитку, зокрема в напрямі створення універсальних правових норм, які б ефективно регулювали новітні форми конфліктів [9].

Перспективи подальших досліджень пов'язані з розробкою комплексних міжнародно-правових механізмів протидії гібридним загрозам, що враховуватимуть їх динамічний характер і технологічний розвиток. В умовах зростаючої нестабільності міжнародного середовища такі дослідження набувають особливого значення для забезпечення глобальної безпеки та стабільності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Богів Я., Шардакова А. Майбутнє міжнародного права: інтеграція сучасних технологій, гібридних підходів та створення нових нормативних рамок для глобального співтовариства. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки».* 2023. Т. 10, № 3 (39). С. 243–249.

2. Вареник О. С. Тенденції міжнародного співробітництва у сфері кібербезпеки. *Юридичний науковий електронний журнал.* 2024. № 11. С. 591–593. URL : https://doi.org/10.32782/2524-0374/2024-11/139

3. Кононенко В. П. Інформаційна безпека як стан. *Науковий вісник Ужгородського університету.* 2023. Т. 2, вип. 76. С. 244–250. URL : https://doi.org/10.24144/2307-3322.2022.76.2.39

4. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право.* 2021. № 2 (37). С. 129–138. URL : https://doi.org/10.37750/2616-6798.2021.2(37).238348

5. Тарасюк А. В. Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі. *Прикарпатський юридичний вісник.* 2020. Вип. 1. С. 133–136. URL : https://doi.org/10.32837/pyuv.v0i1(30).532

6. Тєтєвін М. С. Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки. *Науковий вісник Ужгородського національного університету.* 2024. Вип. 82, ч. 3. С. 263–266. URL : https://doi.org/10.24144/2307-3322.2024.82.3.41

7. Черниш Р.В. Міжнародний організаційний досвід у сфері забезпечення кібербезпеки. *Вісник кримінального правосуддя.* 2023. № 3–4. С. 112–121. URL : https://doi.org/10.17721/2413-5372.2021.3-4/112-121

8. Горбулін В.П. Гібридна війна: все тільки починається… *Дзеркало тижня.* 2016. № 11. С. 5–9.

9. Магда Є. В. Гібридна війна: вижити і перемогти. Київ : Віват, 2015. 304 с.

10. Почепцов Г. Г. Смисли і війни: Україна і Росія в інформаційній і смисловій війні. Київ : Києво-Могилянська академія, 2016. 316 с.

11. Резніков О. О. Національна стійкість в умовах гібридних загроз: український досвід. Київ : НІСД, 2022. 112 с.

Дата надходження 03.04.2026
Дата прийняття 23.04.2026
Дата рекомендації 28.05.2026
Дата публікації 30.06.2026