УДК 343.243:004.056
DOI https://doi.org/10.24144/2788-6018.2026.01.1.14

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ

Селіхов Д.А.,
доктор юридичних наук, професор,
професор кафедри теорії держави та права
Навчально-наукового інституту права та інноваційної освіти
Дніпровського державного університету внутрішніх справ
ORCID: 0000-0002-2109-9172

Селіхов Д.А. Кібербезпека як складова інформаційної безпеки: теоретичні та прикладні аспекти.

У статті розкрито теоретичні та практичні правові аспекти забезпечення кібербезпеки як складової інформаційної безпеки в Україні.

Зазначено, що інформаційна безпека є багатовимірною концепцією, що охоплює практично всі сфери суспільного життя унаслідок стрімкого та повсюдного поширення інформаційних технологій. В умовах воєнного стану, кібербезпека є одним із найбільш проблемних питань сучасності, оскільки кіберзагрози також постійно примножуються і ускладнюються. Кібербезпеку визначено як складову інформаційної безпеки, що реалізується в умовах використання комп'ютерних систем і телекомунікаційних мереж та спрямована на захист даних, інформаційних ресурсів і критично важливих інтересів особи, суспільства та держави від кіберзагроз і кібератак.

У правовому вимірі кібербезпека постає як цілісна система нормативно врегульованих інструментів і заходів, що реалізуються у кіберпросторі з метою гарантування національної безпеки. Нормативно-правова база у сфері кібербезпеки значною мірою не встигає за стрімким розвитком інформаційних технологій і трансформацією форм та методів кібератак, що зумовлює наявність прогалин у правовому регулюванні та ускладнює практичну реалізацію відповідних норм.

Доведено, що сучасний стан правового регулювання кібербезпеки в Україні виявляє низку системних проблем, зокрема фрагментарність законодавства, відсутність цілісної концепції державної політики, дублювання повноважень суб'єктів забезпечення кібербезпеки та недостатню координацію між ними. За умов постійного зростання кількості та складності кібератак, спрямованих, у тому числі, на критичну інфраструктуру та державні інформаційні ресурси, така ситуація істотно знижує ефективність протидії кіберзагрозам.

Зроблено висновок, що зв'язку з цим особливої актуальності набуває вдосконалення нормативно-правового забезпечення кібербезпеки шляхом його гармонізації з європейськими та міжнародними стандартами, а також запровадження дієвих механізмів міжвідомчої координації та публічно-приватного партнерства. Врахування досвіду Європейського Союзу та активна участь України у міжнародному співробітництві у сфері кіберзахисту можуть стати важливими чинниками підвищення стійкості національної системи кібербезпеки та ефективної відповіді на сучасні й майбутні кіберзагрози.

Ключові слова: інформаційна безпека, національна безпека, кібербезпека, кіберпростір, воєнний стан, європейська інтеграція, європейські стандарти.

Selikhov D.A. Cybersecurity as a component of information security: theoretical and applied aspects.

The article reveals the theoretical and practical legal aspects of ensuring cybersecurity as a component of information security in Ukraine.

It is noted that information security is a multidimensional concept that covers almost all spheres of public life due to the rapid and widespread spread of information technologies. In conditions of martial law, cybersecurity is one of the most problematic issues of our time, since cyber threats are also constantly multiplying and becoming more complex. Cybersecurity is defined as a component of information security that is implemented in the use of computer systems and telecommunication networks and is aimed at protecting data, information resources and critical interests of the individual, society and the state from cyber threats and cyber attacks.

In the legal dimension, cybersecurity appears as a holistic system of normatively regulated instruments and measures implemented in cyberspace in order to guarantee national security. The regulatory and legal framework in the field of cybersecurity largely lags behind the rapid development

of information technologies and the transformation of forms and methods of cyberattacks, which causes gaps in legal regulation and complicates the practical implementation of relevant norms.

It has been proven that the current state of legal regulation of cybersecurity in Ukraine reveals a number of systemic problems, in particular, fragmentation of legislation, the absence of a holistic concept of state policy, duplication of powers of cybersecurity entities and insufficient coordination between them. Given the constant increase in the number and complexity of cyberattacks, including those aimed at critical infrastructure and state information resources, this situation significantly reduces the effectiveness of countering cyber threats.

It is concluded that in this regard, the improvement of the regulatory and legal support for cybersecurity through its harmonization with European and international standards, as well as the introduction of effective mechanisms for interagency coordination and public-private partnership, is of particular relevance. Taking into account the experience of the European Union and the active participation of Ukraine in international cooperation in the field of cyber defense can become important factors in increasing the stability of the national cybersecurity system and an effective response to current and future cyber threats.

Key words: information security, national security, cybersecurity, cyberspace, martial law, European integration, European standards.

Постановка проблеми. Актуальність дослідження кібербезпеки як складової інформаційної безпеки зумовлена не тільки стрімкою цифровізацією суспільних відносин і активним впровадженням інформаційних технологій у всі сфери життєдіяльності суспільства, а, перш за все, низкою загроз для кіберсфери України в умовах воєнного стану. В умовах війни кіберпростір є середовищем підвищених ризиків для національної безпеки.

Особливої уваги потребують саме правові аспекти забезпечення кібербезпеки України. Кіберзагрози безпосередньо впливають на реалізацію конституційних прав і свобод людини і громадянина, стабільність функціонування органів публічної влади та національну безпеку загалом, що актуалізує потребу в ефективному правовому механізмі протидії їм. Водночас сучасний стан правового регулювання кібербезпеки в Україні характеризується фрагментарністю, що знижує ефективність державної політики у сфері інформаційної безпеки.

З огляду на зазначене, наукове осмислення кібербезпеки як складової інформаційної безпеки в теоретичному та прикладному правовому вимірах є своєчасним і необхідним.

Метою статті є розкрити теоретичні та практичні правові аспекти забезпечення кібербезпеки як складової інформаційної безпеки в Україні в умовах воєнного стану.

Стан опрацювання проблематики. Різні аспекти правового забезпечення кібербезпеки як складової інформаційної безпеки України досліджували такі вітчизняні вчені, як: О. Баранов, П. Берназ, В. Бурячок, С. Гнатюк, Г. Гончаренко, О. Горбенко, Є. Живило, М. Кондратюк, В.Куцаєв, В. Ліпкан, А. Марущак, Д. Мінін, О. Манжай, О. Остапенко, С. Петров, А. Пролорензо, Е.Рижков, І. Сопілко, В.Фурашев та ін. Однак, не втрачають актуальності питання удосконалення вітчизняного законодавства у сфері забезпечення кіберзахисту та реагування на новітні кіберзагрози, особливо в умовах воєнного стану. Залишаються невирішеними низка практичних питань, що мають юридичну природу.

Виклад основного матеріалу. Безпека – це якість або стан, що характеризується свободою від небезпеки, стан захищеності від супротивників – від тих, хто може завдати шкоди навмисно чи навмисно. Інформаційна безпека є багаторівневою системою, яка передбачає стан захищеності інформаційного суверенітету держави, її інформаційного простору та ресурсів, а також інформаційних прав та інтересів суспільства.

О. Горбенко під поняттям «інформаційна безпека» пропонує розуміти стан інформаційного середовища, за якого забезпечується стійкість до зовнішніх та внутрішніх загроз, гарантовано права та свободи громадян в інформаційній сфері, а також захищені національні інтереси держави, а під поняттям «кібербезпека» – здатність систем та мереж протидіяти кіберзагрозам, забезпечуючи безперебійну роботу інформаційно-комунікаційних технологій та захист даних від несанкціонованого доступу і модифікації [1, с. 77]. Інформаційна безпека є багатовимірною концепцією, що охоплює практично всі сфери суспільного життя унаслідок стрімкого та повсюдного поширення інформаційних технологій. В умовах сучасної цифрової епохи вона набуває особливої значущості, адже відомості про велику кількість фізичних осіб і організацій зберігаються та обробляються у різноманітних комп'ютерних системах, нерідко перебуваючи поза безпосереднім контролем їх власників.

Інформаційна безпека не є абсолютною. Навіть досконале планування, правове та технологічне забезпечення та впровадження не може гарантувати стабільної і постійної інформаційної безпеки. Інформаційна безпека – це процес постійного досягання єдиної мети.

Важливою складовою інформаційної безпеки держави є кібербезпека.

На сьогодні, в умовах воєнного стану, кібербезпека є одним із найбільш проблемних питань сучасності, оскільки кіберзагрози також постійно примножуються і ускладнюються.

Кібербезпека – це використання сучасних технологій, процесів і засобів контролю з метою захистити комп'ютерні системи та мережі, програми, пристрої і дані від кібернетичних атак, а також з метою зниження ризику здійснення кібератаки [2]. О. Баранов зауважує, що кібербезпека – це інформаційна безпека в умовах використання комп'ютерних систем та/або телекомунікаційних мереж. Кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [3, с. 57]. М. Кондратюк визначає систему кібербезпеки держави як комплекс спеціальних врегульованих нормативно суб'єктів забезпечення кібербезпеки, а також відповідних методів, засобів, прийомів та заходів, які використовуються та здійснюються з даною метою у кіберпросторі [4, с. 46]. Отож, кібербезпеку можна визначити як складову інформаційної безпеки, що реалізується в умовах використання комп'ютерних систем і телекомунікаційних мереж та спрямована на захист даних, інформаційних ресурсів і критично важливих інтересів особи, суспільства та держави від кіберзагроз і кібератак.

Хоча кібербезпеку розглядають як підмножину інформаційної безпеки, обидва цих типи безпеки своєю основною метою мають захист даних. Інформаційна безпека орієнтована на захист від будь-яких загроз важливих даних, як у цифровій, так і в аналоговій формі. А кібербезпека, зосереджена на цифровій інформації, також нерозривно пов'язана із такими категоріями як кіберзлочини, кібератаки тощо [5, с. 113]. Зміст понять «інформаційна безпека» та «кібербезпека» вказує на їхню взаємопов'язаність, проте кожне з них має свої специфічні акценти. Інформаційна безпека охоплює всі аспекти захисту інформації, незалежно від її форми, тоді як кібербезпека спеціалізується на захисті цифрових систем і ресурсів у кіберпросторі [6, с. 469]. Інформаційна безпека і кібербезпека є тісно взаємопов'язаними, проте не тотожними категоріями. Обидва види безпеки мають спільну мету – захист даних, однак відрізняються за обсягом і спрямованістю.

В контексті нормативно-правового розуміння національної та інформаційної безпеки, кібербезпека може визначатися як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем [7, с. 45]. Кібербезпека в юридичному контексті спрямована на захист комп'ютерних систем і мереж від кіберзагроз, таких як атаки хакерів, віруси та інше шкідливе програмне забезпечення. Юридичні норми, що регулюють кібербезпеку, зосереджені на забезпеченні безпеки цифрових інфраструктур і протидії кіберзлочинності [6, с. 469]. У правовому вимірі кібербезпека постає як цілісна система нормативно врегульованих інструментів і заходів, що реалізуються у кіберпросторі з метою гарантування національної безпеки.

Однак кіберпростір характеризується підвищеною складністю з точки зору правового регулювання, що зумовлено його транскордонним характером, динамічним розвитком технологій та багатосуб'єктністю правовідносин.

Нині кіберпростір розглядається як важливий безпековий імператив, оскільки від його реалізації залежать економічна, військова, соціальна та інші сфери діяльності держави [8, с. 120]. Під кіберпростором розуміється кіберінформаційне середовище, що відображає семантику (сутність) об'єктів кіберінформаційної інфраструктури та системи відношень і зв'язків між цими об'єктами. До об'єктів кіберінформаційної інфраструктури відносять апаратно-технічні складові (сучасні гаджети, персональні комп'ютери тощо), програмно-технологічні складові (комп'ютерні мережі, ПЗ), інформаційні складові (інформаційні бази, веб-контенти, Інтернет-відомості тощо) [9, с. 78]. Кіберпростір – це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами» [10, с. 145]. Кіберпростір можна визначити як складне середовище, що включає взаємодію між людьми (суб'єктами правовідносин) та програмним забезпеченням (об'єктом правовідносин). Він підтримується завдяки всесвітньому поширенню інформаційно-комунікаційних технологій, отож і його правове забезпечення не може мати суто локальний, національний характер.

Він є спільним простором для великою кількістю суб'єктів, що спільно користуються важливою інформаційною інфраструктурою.

Переміщення конфліктів із традиційного фізичного простору в кіберпростір, яке спостерігається вже тривалий час, породжує нові загрози та виклики в аспекті забезпечення кібербезпеки нашої

держави, особливо в умовах протидії агресору – російській федерації. Технології інформаційної війни приваблюють саме через відносну дешевизну, доступність та ефективність, а отже, інтенсивність їх використання тільки наростатиме [11, с. 34]. Кіберпростір знаходиться у перманентному стані еволюції та модернізації, тому очікувано, що він стане ще складнішим у найближчі роки. Отож, і значно складнішим об'єктом правового регулювання та контролю.

Останнім часом суспільство дедалі частіше стикається з різноманітними видами кібератак: збої при наданні електронних послуг, блокування роботи державних органів, фішингові атаки електронною поштою, кіберзлочини, порушення цілісності та конфіденційності даних, інформаційно-психологічний тиск на населення, кібертероризм, кібершпигунство, інформаційна експансія у національний інформаційний простір країни, блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення й об'єктів підвищеної небезпеки [12, с. 644; 17]. Російська агресія супроводжується масштабними кібератаками на критичну інфраструктуру, державні інформаційні системи та приватні підприємства [13, с. 80]. За таких умов щонайменше рівень і якість нормативно-правового забезпечення кібербезпеки та протидії кіберзагрозам повинні бути належними й адекватними сучасним викликам.

Сучасний стан правового регулювання кібербезпеки в Україні характеризується значними системними вадами, які суттєво обмежують ефективність протидії кіберзагрозам та не відповідають масштабам викликів цифрової доби. Чинне законодавство демонструє фрагментарність та відсутність цілісної концепції правового забезпечення кібербезпеки, що проявляється у дублюванні функцій різних державних органів, недостатній координації їхньої діяльності та відсутності чітких механізмів розмежування компетенції [14, с. 167]. Крім того, нормативно-правова база у сфері кібербезпеки значною мірою не встигає за стрімким розвитком інформаційних технологій і трансформацією форм та методів кібератак, що зумовлює наявність прогалин у правовому регулюванні та ускладнює практичну реалізацію відповідних норм. Відсутність уніфікованого понятійно-термінологічного апарату, а також недостатня узгодженість національного законодавства з міжнародними та європейськими стандартами знижують рівень правової визначеності та ефективність міжвідомчої і міжнародної співпраці у сфері протидії кіберзагрозам. У сукупності це актуалізує необхідність комплексного перегляду та систематизації законодавства про кібербезпеку, формування цілісної державної політики у цій сфері та запровадження дієвих механізмів координації, відповідальності й контролю.

З метою удосконалення правового, інституційного, фінансового, технологічного забезпечення кібербезпеки Україні слід враховувати напрацьовані дієві підходи, що використовуються, перш за все в Європі.

Спільні зусилля світової спільноти щодо обміну досвідом, технологіями, здобутками фахівців у сфері кіберзахисту, взаємна фінансова підтримка, скоординована спільна системна відповідь країн на кіберзлочини, запровадження нових світових стандартів з кібербезпеки та інформаційної безпеки, оновлення національних та міжнародних стратегій, законодавства, які б відповідали новим кібервикликам, є запорукою подолання спільними зусиллями нових сучасних викликів [15, с. 495]. Європейський Союз активно модернізує власні сектори безпеки у кіберпросторі у відповідності до викликів сучасності. Цей процес відбувається шляхом: впорядкуванням нормативної бази, що має забезпечити цілісність державної політики в даній сфері; вироблення європейських керівних принципів щодо забезпечення стійкості і стабільності мережі Інтернет та їхнє просування на міжнародній арені; збільшенням чисельності підрозділів, зайнятих у системі кіберзахисту; посилення контролю за національним інформаційним простором; зміцнення захисних механізмів для критичної інформаційної інфраструктури ЄС; проведення загальноєвропейських навчань та досліджень з проблем безпекових інцидентів в мережі Інтернет; посилення співпраці між державним і приватним секторами; створення європейського форуму для обміну інформацією між країнами-членами; створення європейської системи раннього сповіщення про кіберзагрози та ін. [16, с. 31]. У цьому контексті досвід Європейського Союзу є показовим для України, оскільки демонструє ефективність комплексного, скоординованого та проактивного підходу до формування системи кібербезпеки.

Адаптація європейських стандартів і практик, зокрема у частині гармонізації законодавства, розвитку інституційної спроможності суб'єктів кіберзахисту [18, с. 31; 19, с. 747; 20, с. 62], запровадження механізмів публічно-приватного партнерства та систем раннього реагування на кіберінциденти, здатна суттєво посилити національну систему кібербезпеки. Водночас активна участь у міжнародному співробітництві, обмін інформацією про кіберзагрози та спільні навчання сприятимуть підвищенню стійкості держави до кібератак, що є особливо актуальним в умовах збройної агресії та гібридних загроз.

Висновки. Кібербезпека є невід'ємною складовою інформаційної та національної безпеки в цілому, яка в умовах цифровізації суспільства та збройної агресії проти України набуває особливого

значення. Сучасний кіберпростір характеризується високим рівнем динамічності, транскордонності та складності, що значно ускладнює правове врегулювання та потребує системного й адаптивного підходу.

Сучасний стан правового регулювання кібербезпеки в Україні виявляє низку системних проблем, зокрема фрагментарність законодавства, відсутність цілісної концепції державної політики, дублювання повноважень суб'єктів забезпечення кібербезпеки та недостатню координацію між ними. За умов постійного зростання кількості та складності кібератак, спрямованих, у тому числі, на критичну інфраструктуру та державні інформаційні ресурси, така ситуація істотно знижує ефективність протидії кіберзагрозам.

У зв'язку з цим, особливої актуальності набуває вдосконалення нормативно-правового забезпечення кібербезпеки шляхом його гармонізації з європейськими та міжнародними стандартами, а також запровадження дієвих механізмів міжвідомчої координації та публічно-приватного партнерства. Врахування досвіду Європейського Союзу та активна участь України у міжнародному співробітництві у сфері кіберзахисту можуть стати важливими чинниками підвищення стійкості національної системи кібербезпеки та ефективної відповіді на сучасні й майбутні кіберзагрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Горбенко О.І. Інформаційна та кібербезпека: концептуальні засади та практичні аспекти. Харків: «Фоліо». 2017. 320 с.
2. What is Cyber Security? Definition and Best Practices. IT Governance. 2020. URL: https://www.itgovernance.co.uk/what-iscybersecurity.
3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2 (42). С. 54–62. URL: https://ippi.org.ua/sites/default/files/14boavpk.pdf.
4. Кондратюк М. В. Кібербезпека України в системі національної безпеки. *Право і суспільство.* 2019. № 6. Ч. 2. С. 42–48. DOI https://doi.org/10.32842/2078-3736-2019-6-2-7.
5. Сопілко І. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Наукові праці Київського авіаційного інституту. Серія: Юридичний вісник «Повітряне і космічне право».* 2021. № 2 (59). С. 110–115. DOI: https://doi.org/10.18372/2307-9061.59.15603.
6. Гончаренко Г.А. До проблеми визначення та розмежування дефініцій «інформаційна безпека» і «кібербезпека». *Аналітично-порівняльне правознавство.* 2024. № 5. С. 466–471. DOI: https://doi.org/10.24144/2788-6018.2024.05.73.
7. Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. *Актуальні проблеми управління інформаційною безпекою держави*: зб. матер. наук.-практ. конф. (Київ, 22 березня 2011 р.). Київ: Вид-во НА СБ України, 2011. Ч. 2. С. 43–48.
8. Валюшко І. О. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник НТУУ «КПІ»*. 2016. № 3/4 (31-32). С. 117–124. URL: https://visnyk-psp.kpi.ua/article/view/140496/137578.
9. Такаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері.* 2018. № (1). С. 75–86. DOI: https://doi.org/10.31866/2617-796x.1.2018.147257.
10. Манжай О.В. Використання кіберпростору в оперативно розшуковій діяльності. *Право і безпека. Науковий журнал*. 2009. № 4. С. 142–149. URL: https://files01.core.ac.uk/download/333962960.pdf.
11. Пролорензо А. Кібербезпека в українських літературних джерелах: політичний огляд. *Вісник Прикарпатського університету. Серія: Політологія.* 2025. № 20. С. 31-35. DOI: https://doi.org/10.32782/2312-1815/2025-20-4.
12. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Том 21. № 3. С. 150–157. DOI: 10.18372/2410-7840.21.13951.
13. Остапенко О.В., Берназ П.С. Кіберзлочинність як загроза національній безпеці України. *Науковий вісник Національної академії внутрішніх справ.* 2024. № 1(130). С. 78–86. DOI:10.35774/app2025.02.164.
14. Мазепа С. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. *Актуальні проблеми правознавства*. 2025. № 2 (42). С. 164–171. URL: https://appj.wunu.edu.ua/index.php/appj/article/view/2142/2163.
15. Ємельянов В.М., Бондар Г.Л. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. *Публічне управління та регіональний розвиток.* 2019. № 5. С. 493–523. URL: http://nbuv.gov.ua/UJRN/purr_2019_5_4.

16. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права.* 2018. № 53. С. 26–37. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/a2dd0ed8-c884-4205-8d60-df50918d943e/content.
17. Трофименко О. Моніторинг стану кібербезпеки в Україні. *Правове життя сучасної України:* матер. міжнар. наук.-практ. конф. (17 травня 2019 р.). 2019, Одеса: Видавничий дім «Гельветика». С. 642–646.
18. Наливайко Л.Р., Вітвіцький С.С. Право на доступ до публічної інформації в контексті контролю громадян за діяльністю держави. *Право і суспільство.* 2014. № 5(2). С. 28–33. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID= &I21DBN=UJRN&P21DBN.
19. Ряполов А.П. Захист інформаційного простору України в умовах гібридної війни: межі між свободою слова та інформаційною безпекою. *Національні інтереси України.* 2025. № 5 (10). С. 746–758. DOI: https://doi.org/10.52058/3041-1793-2025-5(10)-746-757.
20. Наливайко Л.Р. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект. *Вісник Запорізького державного університету.* 2003. № 1. С. 60–65. URL: https://scholar.google.com/citations?view_op=view_citation&hl=uk&user=U6ecyI4AAAAJ&citation_for_view=U6ecyI4AAAAJ:tuHXwOkdijsC.

Дата першого надходження рукопису до видання: 11.01.2026
Дата прийняття до друку рукопису після рецензування: 26.01.2026
Дата публікації: 2.02.2026