УДК 327:004.738.5
DOI https://doi.org/10.32782/cuj-2026-1-3

Верховцева Ірина Геннадіївна
доктор історичних наук, професор,
професор кафедри національної безпеки та підприємництва
Державного університету «Київський авіаційний інститут»
Scopus-Author ID: 57483471400
Researcher ID: LRS-2726-2024
ORCID: 0000-0002-5682-993X

Малахова Тетяна В'ячеславівна
доктор наук з державного управління, професор,
професор кафедри публічного управління, адміністрування та соціальної роботи
Національного університету охорони здоров'я України імені П. Л. Шупика
Scopus-Author ID: 58950305900
ORCID: 0009-0001-1113-5723

Нестеренко Галина Петрівна
кандидат наук з державного управління, доцент,
доцент кафедри національної безпеки та підприємництва
Державного університету «Київський авіаційний інститут»
ORCID: 0000-0002-1106-3790

Ситюк Антоніна Анатоліївна
кандидат наук з державного управління,
радник з питань освіти та ринку праці
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
ORCID: 0000-0002-0698-2530

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ КІБЕРСУСПІЛЬСТВА: КОГНІТИВНИЙ ВИМІР, УКРАЇНСЬКИЙ КОНТЕКСТ

Метою статті визначено охарактеризувати принципові засади управління інформаційною безпекою України за умов кіберсуспільства з фокусом на когнітивних аспектах проблеми в рамках опору деструктивній масово-інформаційній діяльності антиукраїнського характеру. Акцентовано на викликах цифрової епохи та якісних змінах у соціальних взаємодіях і когнітивних практиках, зумовлених застосуванням новітніх технологій (штучного інтелекту, нейронних мереж тощо) в рамках смислових аспектів мережевих

взаємодій. На основі аналізу провідних світових моделей управління інформаційним простором окреслено завдання забезпечення інформаційної безпеки України в частині формування інформаційних кордонів з огляду на когнітивну безпеку вітчизняного соціуму. Наголошено на потребах принципового оновлення державної інформаційної політики, гармонізації національного законодавства в інформаційній сфері з відповідними європейськими стандартами та доповнення системи інформаційних фільтрів елементами, пов'язаними з когнітивною безпекою українського суспільства й регулюванням транскордонних потоків даних. У рамках системного й багаторівневого підходу до управління інформаційною безпекою шляхами зміцнення інформаційного суверенітету України визначено інтенсифікацію міждержавного співробітництва у формуванні міжнародно-правового режиму інформаційної безпеки й регламентації поведінки держав в інформаційному просторі, сприяння ефективній взаємодії у сфері кіберзахисту, подолання концептуальної і термінологічної неузгодженості в даній сфері, пошук балансу між відкритістю і безпекою. Резюмовано, що управління інформаційною безпекою України в частині когнітивної безпеки є процесом, який потребує постійної уваги, творчих підходів, гнучких і швидких реагувань із боку держави, усього українського соціуму.

Ключові слова: *кіберпростір, кіберсуспільство, інформаційний простір, інформаційні кордони, інформаційна безпека, когнітивна безпека, управління інформаційною безпекою.*

Verkhovtseva I. H., Malakhova T. V., Nesterenko H. P., Sytiuk A. A. Information security management in the context of cyber society: cognitive dimension, Ukrainian context

The purpose of the article is to characterize the fundamental principles of information security management in Ukraine in the context of a cyber society, with a focus on the cognitive aspects of the problem in the context of resistance to destructive anti-Ukrainian mass media activities. Emphasis is placed on the challenges of the digital age and qualitative changes in social interactions and cognitive practices caused by the use of new technologies (artificial intelligence, neural networks, etc.) within the framework of the semantic aspects of network interactions. Based on an analysis of leading global models of information space management, the tasks of ensuring Ukraine's information security in terms of forming information borders with regard to the cognitive security of the domestic society are outlined. The need for a fundamental update of state information policy, harmonisation of national legislation in the information sphere with relevant European standards, and supplementation of the information filter system with elements related to the cognitive security of Ukrainian society and the regulation of cross-border data flows is emphasised. As part of a systematic and multi-level approach to information security management aimed at strengthening Ukraine's information sovereignty, the following measures have been identified: intensification of intergovernmental cooperation in the formation of an international legal regime for information security and regulation of states' behaviour in the information space; promotion of effective cooperation in the field of cyber defence; overcoming conceptual and terminological inconsistencies in this area, and finding a balance between openness and security. In summary, managing Ukraine's information security in terms of cognitive security is a process that requires constant attention, creative approaches, and flexible and rapid responses from the state and Ukrainian society as a whole.

Key words: *cyberspace, cyber society, information space, information borders, information security, cognitive security, information security management.*

Вступ. Новітні цифрові технології здатні миттєво, у великих обсягах переміщувати інформацію трансграничним і транскордонним за своїм характером кіберпростором та «створювати» віртуальну, по суті, «паралельну», реальність (зокрема, завдяки штучному інтелекту (ШІ), нейронним мережам тощо). Це зумовлює якісні зміни соціальних взаємин та когнітивної сфери й сприяє формуванню нового суспільного типу – кіберсуспільства («кібер» буквально з грецької – «над»). Під впливом мережевої цифрової взаємодії у ньому формуються нові ідентичності та організаційні форми, що мають переважно віртуальні виміри, але цілком фізичні наслідки у форматах геополітичних протистоянь, міжнародних альянсів, державних суверенітетів, економічних політик, освітніх і культурних практик тощо. Надзвичайно загрозливим у цьому ключі, як доводить інформаційне протиборство 2014–2026 рр. між Україною і росією, є застосування агресором, що прагне вплинути на спосіб мислення соціуму опонента та зарубіжної громадськості загалом, цифрових технологій для поширення фейкової інформації ворожого, зокрема антиукраїнського, характеру [1, с. 288; 2, с. 215–228]. Це впливає на імідж нашої держави, її влади, політиків, публічних діячів, соціокультурні процеси загалом, а також, відповідно, на прийняття публічно-управлінських рішень щодо протидії російській інвазії й підтримки виживання

українців під пресингом російських геноцидних практик. З огляду на це, надважливим є осмислення питань управління інформаційною безпекою за умов кіберсуспільства, зокрема в когнітивному вимірі, з урахуванням усіх викликів і загроз сучасності.

Дана проблематика, будучи міждисциплінарною за характером студіювання, у тих чи інших аспектах інтенсивно вивчається зарубіжними науковцями (Л. Флоріді, М. Кастельс, Б. Латур, А. Шокер, Л. Чуліаракі, М. Георгіу, Дж. Голдсміт, Т. Вью, Е. Снайдер, Дж. Ночетті та ін.). Окрім впливу цифрових технологій на інформаційно-комунікаційні процеси у соціальному сегменті кіберпростору в контексті міжнародних комунікацій, інформаційних і когнітивних протистоянь у фокус уваги потрапили питання інформаційних кордонів, управління інформаційним простором країни тощо. Зокрема, Л. Флоріді, Б. Латур і М. Кастельс, указуючи на інфосферу як нову реальність, у якій живе і діє сучасна людина, наголошують на тому, що інформаційні системи невіддільні від людських практик і створюють нові форми суспільної взаємодії [3–5]. А. Шокер [5], Л. Чуліаракі й М. Георгіу [6] сфокусувалися на цифровому суверенітеті (Digital Sovereignty). Дж. Голдсміт і Т. Вью [7] розмірковують над впливом Інтернет-комунікацій на глобальний кіберпростір та вказують на пов'язані із цим проблеми інформаційного суверенітету країн. Л. Еверус осмислює проблему інформаційних фільтрів і кордонів [8].

Українські дослідники (Г. Почепцов, Д. Дубов, О. Резнікова, Г. Радзівілов, В. Кротюк, О. Панфілов, І. Верховцева, А. Миколюк та ін.) також інтенсивно вивчають питання інформаційної безпеки за умов цифровізації, надаючи перевагу практичним аспектам захисту національного інфопростору в умовах російсько-української війни. Зокрема, акцентується на тому, що нині авторитет держави значною мірою залежить від її можливості впливати на світові та регіональні події не так конвенційно, як інформаційно [9; 10]. Вивчаються аспекти протидії інформаційному насиллю у кіберпросторі [2] та інформаційна стійкість за умов цифровізації [11–14]. Активовано осмислення проблем управління інформаційною безпекою [15; 16] й застосування новітніх цифрових технологій у рамках інноваційного оновлення публічного управління загалом [17]. Варто відзначити доробок, що актуалізує проблему когнітивної безпеки [18; 19].

Однак загалом, попри те, дискусія щодо базових засад управління інформаційною безпекою за умов кіберсуспільства далека від логічного завершення, адже новітні цифрові технології, якісно змінюючи когнітивну сферу і соціальний ландшафт, провокують тектонічні зміни управлінського простору країн і регіонів, світоустрою загалом. Відповідно, указані питання потребують масштабного й глибокого студіювання на різних рівнях та в різних форматах: філософському, теоретико-методологічному, термінознавчому, нормативно-правовому, публічно-управлінському, кібердипломатичному тощо.

Не претендуючи на всебічне висвітлення даної проблеми, **метою** статті визначаємо охарактеризувати принципові засади управління інформаційною безпекою в Україні за умов кіберсуспільства з фокусом на когнітивних аспектах проблеми в рамках опору деструктивній масовоінформаційній діяльності антиукраїнського характеру. Конкретизується це в таких дослідницьких завданнях: з'ясувати основні виклики масово-комунікаційного сегменту кіберсуспільства у когнітивному вимірі; на основі аналізу провідних світових моделей управління інформаційним простором визначити завдання інформаційної безпеки в частині формування інформаційних кордонів з огляду на когнітивну безпеку українського соціуму; окреслити базові засади управління інформаційною безпекою в системі координат публічного управління України за умов протидії російській інформаційній агресії з акцентом на завданнях когнітивної безпеки.

Матеріали та методи. Нормативною основою дослідження є Конституція України, чинні законодавчі та підзаконні нормативно-правові акти, що визначають засади публічного управління інформаційною безпекою в Україні. Під час студіювання проблеми, окрім методів загальнонаукових (логіки, аналізу, синтезу, індукції, дедукції тощо), застосовувалися, відповідно, спеціально-наукові: історичний (сприяв

розкриттю історичних аспектів розроблення політики інформаційної безпеки України), логіко-семантичний (дав змогу розкрити поняття когнітивної безпеки як об'єкт публічно-управлінської діяльності у сфері інформаційної безпеки), структурно-функціонального аналізу (дав змогу з'ясувати рівні та способи взаємодії органів публічного управління України з іншими суб'єктами забезпечення інформаційної безпеки в аспекті когнітивної безпеки).

Результати. «Кіберреволюція» останніх десятиліть з її технологічними інноваціями, змінюючи характер комунікацій, зумовлює низку викликів соціального та когнітивного характеру. Мережева взаємодія завдяки інформаційній відкритості суспільства зсуває кордони між приватним і публічним у бік останнього. Зростає роль мережевих спільнот, які здатні будь-яку інформацію надшвидко зробити масовою, перетворивши її на складник публічних комунікацій [20, с. 204–205]. Соціальні мережі, цифрові медіа, комунікативні платформи є соціотехнічними конструктами, у яких алгоритми і технології переплітаються з комунікативними стратегіями, політичними впливами й культурними сенсами [3, с. 39; 4, с. 5–75; 5, с. 6–7, 32]. Мережевізація, датифікація, платформізація впливають на соціальні й політичні відносини – від соціалізації індивідів до інституційного дизайну. У науковій літературі такі якісні зміни пов'язуються з формуванням нового суспільного типу – кіберсуспільства (інші назви – нова цифрова цивілізація, цифрове суспільство, суперінтелектуальне суспільство, Суспільство 5.0) [1, с. 288–293]. Під питанням у ньому опиняються базові безпекові аспекти, якими, власне, має забезпечуватися національна безпека. Надзвичайно злободенним, зокрема, це є з огляду на поступове злиття людини і техніки, для чого використовують поняття «транслюдина» і «постлюдина». Імплантування у тіло кібернетичного третього «ока» (eyeborg) чи інших пристроїв («біохакінг») стало новим трендом, який не лише змінює людину фізично, а й впливає на її самоідентифікацію, відкриває можливості для нових способів мислення [21, с. 186–191]. При цьому слід ураховувати, що інтенсивність соціальної взаємодії у кіберпросторі суттєво зростає порівняно з традиційною взаємодією у просторі фізичному, скорочується час, потрібний людині для осмислення інформації, міркувань, формування власної думки тощо.

Завдяки соціальним мережам і цифровим гаджетам практично межі «адської досконалості» досягли технології масово-комунікаційного впливу, ідеї застосування яких сягають минулих тисячоліть, а новітній етап було розпочато у першій половині XX ст. В. Ліпманом, Е. Бернейсом, Г. Ласвелом та іншими політологами в рамках осмислення інструментів керування суспільною свідомістю епохи масовізації. Неабиякі можливості нині отримали генератори контенту для перенаправлення уваги користувачів, формування чи зміни їхніх оцінок у потрібному напрямі в аспектах диференціювання цільових аудиторій (наприклад, засобом технологій таргетингу) чи маніпулювання масовою думкою застосуванням різноманітних медіакомунікаційних технологій: фреймування, візуального сторітелінгу тощо. Дезінформація вийшла на новий рівень і стала одним із головних викликів кіберепохи. Засоби когнітивного впливу: «керований коментар», «відволікання уваги», «хибна аналогія», «принцип контрасту», «принцип психологічного шоку» та інші [22, с. 53–63] завдяки технічним пристроям індивідуального формату дають змогу комунікувати водночас з окремою особою та з масами загалом, провокуючи потрібні генераторові контенту думки, уявлення, акцентуючи на емоційних аспектах взаємодії та ставлячи під удар раціональну й усю когнітивну сферу адресатів. Значно звужено простір осмислень людиною своїх дій у рамках вирішення побутових й кожноденних завдань – годі вести мову про якісну рефлексію суспільно значущих явищ. Отже, цифрова епоха змушує людину опановувати нові алгоритми суспільної взаємодії – як у розрізі малих чи великих груп, так і в розрізі масово-комунікаційному, зокрема публічно-комунікаційному, який охоплює сферу внутрішньо- та міждержавних взаємин.

Доволі загрозливою для долі держави та національного соціуму може бути запізніла реакція їхніх еліт на такі явища, оскільки новітні цифрові технології разом із медіатехнологіями здатні впливати на «святая святих»

національних соціумів – процеси національної ідентифікації. Відтепер їх можна корелювати у векторі, що здатен звести нанівець результати кількасотлітньої боротьби попередніх поколінь співвітчизників за національне самовизначення, знецінивши ці здобутки. З огляду на це, слід констатувати, що зміни когнітивної сфери за умов кіберсуспільства спричинюють значні ризики для соціальної сталості й стійкості.

Але особливу загрозу когнітивній сфері становить новий вид протистоянь між державами – смислові (семантичні), або когнітивні, війни, сприятливі технічні умови для ведення яких створено всеосяжною цифровізацією. Цей новий вид протистоянь впливає на пізнавальну діяльність людини й здійснюється у віртуальному середовищі. В. Кротюк та О. Панфілов акцентують: ворог спочатку «перемагає» розум і лише потім території. Фахівці вважають, що саме російсько-українська війна, розпочата в 2014 р., довела: ключовим об'єктом сучасної війни є не кіберпростір, а когнітивна та емоційна сфери людини. Із 2017 р. її свідомість стали називати «шостим полем бою» (згідно з Військовою доктриною Пентагону, п'ять інших – земля, вода, повітря, космос, віртуальне середовище). Смислова / когнітивна війна є складником сучасної гібридної війни. Ключова відмінність когнітивної війни від інформаційної полягає у меті: смислові операції спрямовані на ураження системи знань і суджень об'єкта агресії, усієї його системи цінностей, картини світу. Тактична мета смислової війни – зробити кожну людину своєрідним «цензором», який сам буде тлумачити факти в потрібному, керованому, сенсі: усе, визначене як «неправильне», відкидати, а засвоювати лише те, що «дозволено». У стратегічному вимірі метою смислової війни є самознищення об'єкта агресії (соціальної групи, нації тощо). У межах інформаційної війни ворог оперує інформаційними потоками, його «зброя» спрямована на ситуаційно актуалізовані в суспільно-політичному дискурсі події та особистості. У смисловій війні агресора цікавить не інформація, а механізми пізнання, культурологічні константи, мішенню стають факти історії, мова, об'єкти культурної спадщини, моральні пріоритети, ментальні стереотипи [14, с. 211–212]. Г. Почепцов наголошує: якщо інформаційна війна формує порядок денний, то смислова – порядок десятиріч, бо знання є більш довготривалим продуктом, аніж інформація. Факти можуть змінюватись, а правила, за якими ми їх розуміємо, залишаються тими самими [10, с. 21–27].

Осмислення нових, зокрема смислових / когнітивних, загроз цифрової епохи в науковому дискурсі відбувається загалом у контексті інформаційної безпеки. При цьому дослідники наголошують на неготовності міжнародно-правових інституцій давати організовану відсіч інформаційній агресії. Ба більше, у світовому правовому просторі не існує поняття «інформаційний суверенітет країни», а «територіальність» дії державного суверенітету не співвідноситься з екстериторіальністю інформаційних потоків, що є суттєвою проблемою в умовах інформаційно-комунікаційної глобалізації [23, с. 181, 184–187]. Натомість певний досвід управління інформаційною безпекою у кіберпросторі провідними країнами напрацьовано. Як акцентує А. Шокер, раціональною стратегією у цьому контексті є не повна ізоляція, а створення системи взаємозалежностей, де порушення суверенітету однієї сторони стає невигідним для іншої. Аналіз джерел дає змогу виділити три домінуючі парадигми / моделі керування інформаційним простором країн (табл. 1) [6; 24–27].

Середовищем, у якому здійснюються заходи з інформаційної безпеки, є інформаційний простір – система зовнішньо- та внутрішньоорганізаційних потоків інформації, які можуть мати різні характеристики з огляду на зміст, методи, засоби передачі та інтенсивність обміну інформацією. Значущість в інформаційному просторі мають ті його компоненти і процеси, вплив на які засобами та методами інформаційної політики дає змогу впливати на перспективи, на осіб, що приймають рішення, контролювати системи збору, обробки, зберігання та передачі інформації, примножувати ресурси, посилювати ключову роль держави у його формуванні, адже інформація виробляється й циркулює серед великої кількості соціальних агентів – основних суб'єктів «змістовного наповнення» кіберпростору. Держава, своєю чергою, визначає цілі, пріоритети, стратегії, запроваджує умови і правила створення

Таблиця 1

Домінуючі парадигми / моделі керування інформаційним простором країн

Критерій порівняння	**США (ринкова / лібертаріанська)**	**КНР / РФ (авторитарна / етатистська)**	**ЄС (нормативна / регуляторна)**
Ключовий драйвер	комерційні інтереси корпорацій, інновації, глобальне домінування Big Tech	політична стабільність режиму, національна безпека, соціальний контроль	захист прав людини, створення єдиного цифрового ринку, конкуренція
Підхід до даних	«Вільний потік даних з довірою» (Data Free Flow with Trust); дані як товар	жорстка локалізація даних; заборона транскордонної передачі критичної інформації	захист персональних даних (GDPR); суверенітет індивіда над своїми даними
Роль платформ	партнери держави та інструменти «м'якої сили»; саморегулювання	інструменти державного контролю та цензури (WeChat, VK)	об'єкти жорсткого регулювання (DSA/DMA); відповідальність за контент
Інформаційні кордони	прозорі для союзників, вибіркові обмеження для загроз (наприклад, TikTok, Huawei)	«Великий Китайський Фаєрвол», «Суверенний Рунет»; технічна ізоляція	«Брюссельський ефект» – експорт внутрішніх норм як глобальних

та обміну інформацією, її оптимального використання, спрямованого на розвиток усього суспільства [28, с. 21–24].

У кіберепоху актуалізовано проблему структурування інформаційного простору та його кордонів. За Л. Еверуссом, інформаційні кордони – це багатошарові структури фільтрації, що мають три рівні: *фізично-інфраструктурний* (включає фізичні канали зв'язку (оптоволокно, супутникові лінки), точки обміну трафіком (IXP) та центри обробки даних (ЦОД); контроль на цьому рівні дає змогу державі фізично відключати сегменти мережі (kill switch) або обмежувати зовнішній трафік); *нормативно-правовий* (система законів і правил, що регулюють обіг інформації; ключовим інструментом виступає локалізація даних (data localization) – вимога зберігати персональні дані громадян на серверах у межах країни); *логічно-алгоритмічний* (установлення кордонів через протоколи маршрутизації (BGP), систему доменних імен (DNS) та через алгоритми пошукових систем і соціальних мереж; дослідники називають це «символічним окордоненням» (symbolic bordering); тут держава часто втрачає монополію, поступаючись владою корпораціям (Facebook, Google чи TikTok), які формують інформаційну бульбашку для користувача, вирішуючи, який контент є видимим, а який – ні) [9].

Як бачимо, у цій системі інформаційних кордонів з їх системою фільтрів не враховуються когнітивні загрози в рамках питань інформаційної безпеки. Натомість у контексті нормативно-правового та логічно-алгоритмічного рівнів, на наше переконання, доцільним було б детальне осмислення цього моменту разом із посиленням повноважень держави у протидії інформаційним небезпекам. Оцінюючи перспективи врахування даного напрацьованого досвіду в українському контексті та з огляду на курс України на євроінтеграцію, найбільш релевантною для неї уявляється європейська модель управління інформаційним простором.

Натепер в Україні напрацьовано певну правову базу політики національної безпеки в аспекті інформаційної безпеки. Її основою є Конституція України, у ст. 17 якої йдеться про те, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави та справою всього українського народу. До вказаних правових засад також входять «Доктрина інформаційної безпеки України» (2017) та Закон «Про національну безпеку України» (2018). Відповідно, під інформаційною безпекою розуміється стан захищеності національних інтересів України в інформаційній сфері, тобто сукупність збалансованих інтересів особистості, суспільства, держави. У цьому контексті враховано і смисловий (когнітивний) вимір інформаційної безпеки, пов'язаний із протидією деструктивним інформаційним впливам на народ України та його повноцінною світоглядною мобілізацією. Вагомим кроком стало прийняття «Стратегії національної безпеки України» (2020), яка акцентує на загрозах інформаційній безпеці та важливості розвитку механізмів захисту інформаційної сфери, констатує відсутність

цілісної інформаційної політики держави та слабкість системи стратегічних комунікацій [29]. Натомість термін «когнітивна безпека» (під цим розуміються заходи і стратегії для захисту когнітивних процесів та інтелектуальної діяльності в особистому й колективному сприйнятті та обробці інформації) в українському правовому полі й законодавстві не вживається. Як наголошують дослідники, метою когнітивної безпеки є забезпечення стійкого і безпечного функціонування інтелектуальних систем, попередження зловживань, збереження довіри і прозорості в інформаційному середовищі. В умовах інтенсивного впливу цифрових технологій та онлайн-середовищ когнітивна безпека фокусується на розпізнаванні, аналізі, протидії загрозам, пов'язаним із маніпулюванням когнітивними процесами: мислення, сприйняття, увага, прийняття рішень тощо сприяє стійкості людей до шкідливих і зловмисних інформаційно-психологічних впливів, загалом здатності раціоналізувати свої відповіді на інформаційні виклики [13, с. 54–60, 67–70, 72; 18, с. 280–281; 19, с. 378].

З огляду на це, на наше переконання, суттєвого переосмислення потребує забезпечення когнітивної безпеки в рамках вітчизняного нормативно-правового поля в частині розроблення механізмів захисту когнітивної сфери за умов кіберсуспільства від інформаційних загроз якісно нового типу, спричинених вищеописаними соціокомунікаційними явищами. Нагальним є пошук нових підходів до формування політики забезпечення інформаційної стійкості українського суспільства з урахуванням принципів убезпечення когнітивної сфери. Один з імпульсів цьому надав той факт, що після лютого 2022 р. ворог значно масштабував і радикально оновив злочинну діяльність у цьому напрямі, застосовуючи інструменти ШІ, здатні генерувати в «промислових» масштабах не лише текстові фейкові наративи та розміщувати їх у світових медіа, а й фальшиві відеонаративи, створюючи тим самим «паралельну віртуальну реальність», уводячи в оману маси й впливаючи на суспільну думку в потрібному агресорові напрямі [2, с. 216–220; 12, с. 581–583; 17, с. 54–57].

Натомість, як наголошують у цьому ключі Г. Радзівілов, А. Пазюк та А. Миколюк, загалом і правове забезпечення інформаційної безпеки України не відповідає сучасному розвитку інформаційних технологій. Учені пропонують застосувати системний, багаторівневий підхід в управлінні інформаційною безпекою, що поєднує правові, організаційні, технічні, освітні, міжнародні інструменти. Така діяльність передбачає її ведення на чотирьох відповідних рівнях – від стратегічного до суб'єктів невладного характеру відповідно. На *стратегічному* рівні – це встановлення порядку застосування сил і засобів інформаційного протистояння, поведінки суб'єктів у критичних ситуаціях. На *організаційно-виконавчому* – організаційне і методичне забезпечення інформаційної безпеки у відповідних галузях та адміністративно-територіальних утвореннях, координація і контроль діяльності міжвідомчим спеціально уповноваженим органом державної влади з питань інформаційної безпеки. На рівні *критично важливої інфраструктури* – забезпечення сталого функціонування об'єктів, управління якими здійснюється з використанням електронно-комунікаційних засобів та інформаційних технологій. На рівні *суб'єктів невладного характеру* – залучення структур громадянського суспільства (громадських формувань, засобів масової інформації, блогерів тощо) до об'єктивного висвітлення подій, ужиття заходів інформаційного спротиву, громадського контролю за діяльністю органів державної влади під час виконання ними функцій у сфері інформаційної безпеки. Ключовим пріоритетом дослідникам убачається утвердження інформаційного суверенітету України та створення відповідної цілісної системи у форматі Інформаційного кодексу та спеціалізованих структур, що відповідають за безпеку в кіберпросторі. Важливим є також вироблення відповідної стратегії у міждержавному співробітництві для формування міжнародно-правового режиму інформаційної безпеки та регламентації поведінки держав в інформаційному просторі. Звертаються науковці й до завдань розвитку людського потенціалу (підвищення цифрової грамотності населення, підготовка фахівців з інформаційної безпеки,

зміцнення потенціалу інформаційної культури суспільства, підтримка наукових досліджень, інновацій та технологічних розробок у сфері захисту інформації). Окрім того, назрілим є подолання концептуальної і термінологічної неузгодженості в даній сфері, оскільки досі спостерігається застосування застарілих та неефективних норм, неадекватних сучасним загрозам понять. Варто погодитися з дослідниками й у тому, що вельми важливим є також завдання знайти баланс між відкритістю та безпекою [15, с. 738–743; 16, с. 158–159; 23, с. 196–197, 201–202].

Однак, на нашу думку, попри цей напрацьований матеріал, недооціненими вітчизняними дослідниками залишилися питання, актуалізовані їхніми західними колегами. Зокрема, варто звернути увагу на висловлене Л. Чуліаракі та М. Георгіу в контексті впливу інформаційних технологій на економіку, політику, культуру, медіа: зокрема, акцентується на поєднанні / взаємодії територіального контролю із символічними наративами, зосередившись на реалізації владного впливу через управління інформаційними потоками в умовах сучасного суспільства [7]. Потребують уваги й думки Дж. Голдсміта та Т. Вью, які вважають за необхідне поглибити розроблення питань інформаційного суверенітету країн у контексті впливу Інтернет-комунікацій на глобальний кіберпростір [8]. Доцільно, на нашу думку, урахувати й висловлене Дж. Казою, яка впевнена, що Інтернет має подолати межі територіального права. Учена акцентує на впливові нових технологій на «радикальну трансформацію» культури й функціонування нової культури віртуальної реальності та / або реальної віртуальності. Ця нова культура, на переконання дослідниці, є «прецесією симулякрів» та множенням знаків і образів, розмиванням межі між реальним, семіотичним та символічним. Науковиця закликає осягати її не лише з технологічної, а й із соціологічної, економічної, філософської (онтологічної) перспектив [30].

Висновки. За умов кіберсуспільства та впливу нових технологій якісних змін зазнає когнітивна сфера соціуму. Зокрема, загрозливим явищем, з огляду на завдання національної безпеки, є деструктивні трансформації раціонального реагування на інформаційні загрози. У цьому контексті травмуючий вплив на українське суспільство і весь вітчизняний когнітивний простір справляє російська ворожа інформаційна діяльність, що ведеться у кіберпросторі часто засобом поширення світовим інформаційним простором згенерованих за допомогою інструментів ШІ злочинного характеру наративів, націлених на руйнування суспільної єдності та волі до спротиву українського народу, на дискредитацію української влади та всього вітчизняного соціокультурного середовища. Отже, доленосним для нашої країни є питання управління інформаційною безпекою в частині когнітивної безпеки. Насамперед це передбачає принципове оновлення державної інформаційної політики. Одним із можливих напрямів є розроблення Інформаційного кодексу України разом із уведенням до правового й законодавчого вітчизняних просторів поняття когнітивної безпеки. Окрім цього, доцільною є гармонізація національного законодавства в інформаційній сфері з європейськими стандартами управління інформаційним простором країн та доповнення системи інформаційних фільтрів елементами, пов'язаними з когнітивною безпекою українського суспільства та регулюванням транскордонних потоків даних у рамках системного й багаторівневого підходу до управління інформаційною безпекою. Цей підхід поєднує правові, організаційні, технічні, освітні, міжнародні інструменти. Із метою зміцнення інформаційного суверенітету України актуалізуються завдання інтенсифікації міждержавного співробітництва для формування міжнародно-правового режиму інформаційної безпеки та регламентації поведінки держав в інформаційному просторі, сприяння ефективній взаємодії у сфері кіберзахисту, а також питання концептуальної і термінологічної неузгодженості в даній сфері. Нагальним є й пошук балансу між відкритістю і безпекою.

Разом із тим чимало проблемних питань, пов'язаних із вивченням новітніх форм взаємодії у кіберпросторі, перебувають у стадії активного розроблення науковцями і далекі від їх остаточного концептуального осмислення. Тож далекою від логічного

завершення є й наукова дискусія щодо публічно-управлінських аспектів інформаційної безпеки, адже кіберсуспільство перебуває у стадії формування, нові технологічні новації з'являються чи не щодня. Отже, варто резюмувати: управління інформаційною безпекою України в частині когнітивної безпеки є процесом, який потребує постійної уваги, творчих підходів, гнучких і швидких реагувань із боку держави та всього українського соціуму.

Перспективи подальшого студіювання даної проблеми пов'язані, зокрема, з детальним розробленням її теоретико-методологічного, філософського, термінознавчого, правового, організаційно-адміністративного, медійно-комунікаційного, кібердипломатичного аспектів.

Література

1. Ярова Л. В., Куртіков М. В. Кіберпростір та «цифрове суспільство»: технології, соціум, політика. *Актуальні проблеми філософії та соціології*. 2025. Вип. 52. С. 288–293. DOI: https://doi.org/10.32782/apfs.v052.2024.46

2. Верховцева І. Г. Глобальний кіберпростір та опір інформаційній агресії: кібердипломатія України у протидії російській інформаційній інвазії. *Міжнародне співтовариство та Україна в процесах економічного та цивілізаційного поступу: актуальні економіко-технологічні, ресурсні, інституціональні, безпекові та соціогуманітарні проблеми :* монографія. Ryga : Baltija Publishing, 2024. С. 213–243. DOI: https://doi.org/10.30525/978-9934-26-480-1-9

3. Floridi L. *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality.* Oxford: Oxford University Press, 2014. URL: https://philpapers.org/rec/FLOTFR-3 (дата звернення: 23.01.2026).

4. Latour B. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford : Oxford University Press, 2005. 311 p.

5. Castells M. *The Rise of the Network Society*. Vol. 1. Oxford: Blackwell, 1996. 625 p.

6. Shoker A. Digital Sovereignty. Strategies for Every Nation. *ACIG Journal.* 2022. Vol. 1 (1). P. 1–17. DOI: https://doi.org/10.5604/01.3001.0016.0943

7. Chouliaraki L., Georgiou M. The digital border: Mobility, technology and power. *European Journal of Communication*. 2019. Vol. 34 (6). P. 594–605. URL: https://eprints.lse.ac.uk/103224/1/EJC._Chouliaraki_and_Georgiou._FINAL_3.pdf (дата звернення: 23.01.2026).

8. Goldsmith J., Wu T. *Who Controls The Internet? Illusions Of A Borderless World*. Oxford University Press, Inc., 2006. URL: https://jost.syr.edu/wp-content/uploads/who-controls-the-internet_illusions-of-a-borderless-world.pdf (дата звернення: 23.01.2026).

9. Everuss L. Entangled Borders: How the Digital Transformation of Sovereign Borders Creates Transnational Population Filters. *Philosophy & Technology.* 2025. Vol. 38 (4). DOI: https://doi.org/10.1007/s13347-025-00960-y

10. Почепцов Г. Г. Смислові та інформаційні війни. *Інформаційне суспільство.* 2013. Вип. 18. С. 21–27.

11. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с.

12. Верховцева І. Г., Христокін Г. В., Силка О. З. Соціоінформаційна стійкість України у цифрову епоху. *Національна стійкість (резилієнтність) як ключовий елемент національної безпеки: архітектура, виклики та шляхи посилення* : матер. І Міжнар. наук.-практ. конф., м. Івано-Франківськ, 27 листопада 2025 р. Івано-Франківськ : ІФНТУНГ, 2025. С. 579–584.

13. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 532 с.

14. Кротюк В. А., Панфілов О. Ю. Смислова зброя у війнах сучасності. *Інформаційно-комунікаційна безпека: сучасні тренди* : монографія / за заг. ред. О.В. Курбан, А.Л. Лісневської. Київ : Київ. ун-т ім. Б. Грінченка, 2022. С. 210–238.

15. Радзівілов Г. Д. Механізми та методи державного управління інформаційною безпекою в умовах сучасних викликів. *Суспільство та національні інтереси.* 2025. № 9. С. 735–744. DOI: https://doi.org/10.52058/3041-1572-2025-9(17)-735-744

16. Миколюк А. В. Публічне управління інформаційною безпекою: діджиталізація та інформаційна війна. *Право та державне управління*. 2022. № 1. С. 156–161. DOI: https://doi.org/10.32840/pdu.2022.1.23

17. Нестеренко Г. П., Бойко В. В. Використання ШІ під час прийняття рішень у публічному управлінні та відповідальність за них. *Вчені записки ТНУ імені В. І. Вернадського. Серія «Публічне управління та адміністрування»*. 2024. Т. 35 (74). № 6. С. 54–59. DOI: https://doi.org/10.32782/TNU-2663-6468/2024.6/10

18. Кобець Т. Основні підходи до розуміння поняття «когнітивна безпека» в сучасній науці: політичний та інформаційний аспекти. *Вісник Львівського університету. Філософсько-політологічні студії*. 2023. Вип. 49. С. 278–285. DOI: https://doi.org/10.30970/PPS.2023.49.34

19. Тараненко Г. Г. Когнітивна безпека як вимір російсько-української війни. *Politology bulletin.* 2024. Вип. 92. С. 371–382. DOI: https://doi.org/10.17721/2415-881x.2024.92.371-382

20. Яковлєва Л. І. Легітимність публічної влади у мережевому суспільстві. *Актуальні проблеми філософії та соціології.* 2023. Вип. 40. С. 201–205. DOI: https://doi.org/10.32782/apfs.v040.2023.34

21. Сінельнікова М. Транс- і постлюдина – світле майбутнє чи кінець людства? *Вісник Львівського університету. Серія «Філософсько-політологічні студії».* 2024. Вип. 55. С. 186–192. DOI: https://doi.org/10.30970/PPS.2024.55.22

22. Гривнак Б., Лопушинський І., Сапіжак І. Дезінформація як загроза національній безпеці України в умовах неоголошеної російсько-української війни. *Науковий вісник Вінницької академії безперервної освіти*. *Серія «Екологія. Публічне управління та адміністрування».* 2024. Вип. 1. С. 53–63. DOI: https://doi.org/10.32782/2786-5681-2024-1.07

23. Пазюк А. В. Міжнародне інформаційне право: теорія і практика : монографія. Дніпро : Середняк Т. К., 2015. 447 с.

24. Snyder E. A. *Global Tensions: Splinternet*. Yale School of Management, 2025. URL: https://som.yale.edu/sites/default/files/2025-06/Brief%20on%20Global%20Tensions.pdf (дата звернення: 23.01.2026).

25. Falkner G., Heidebrecht S., Obendiek A., Seidl T. Digital sovereignty – Rhetoric and reality. *Journal of European Public Policy.* 2024. Vol. 31 (8). P. 2099–2120. DOI: https://doi.org/10.1080/13501763.2024.2358984

26. Musiani F. Reassessing «infrastructuring digital sovereignty»: digital self-determination as a set of infrastructure-embedded practices. *Frontiers in Communication*. 2025. Vol. 10. DOI: https://doi.org/10.3389/fcomm.2025.1562072

27. Nocetti J. "A Splintered Internet? Internet Fragmentation and the Strategies of China, Russia, India and the European Union". Études de l'Ifri, Ifri, 2024. URL: https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_nocetti_internet_fragmentation_february_2024.pdf (дата звернення: 17.01.2026).

28. Дубняк К. А. Інформаційний простір: структура та функціональні параметри. *Держава та регіони. Серія «Соціальні комунікації»*. 2015. № 4 (24). С. 21–25.

29. Стратегія національної безпеки України «Безпека людини – безпека країни», уведена в дію Указом Президента України № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 17.01.2026)

30. Kasza J. Simulacra and Simulation: The Impact of ICT Upon "Radical Transformation" of Culture. 2017. URL: https://www.semanticscholar.org/paper/Simulacra-and-Simulation%3A-The-Impact-of-ICT-Upon-of-Kasza/e6a97d2831fc4df5ed849dbfd492ea1a52a02b82 (дата звернення: 23.01.2026).

References

1. Iarova, L. V., Kurtikov, M. V. (2025). Kiberprostir ta tsyfrove "suspilstvo": tekhnolohii, sotsium, polityka. [Cyberspace and "digital society": technology, society, politics]. *Aktualni problemy filosofii ta sotsiolohii. – Current problems of philosophy and sociology*, 52, 288–293. https://doi.org/10.32782/apfs.v052.2024.46 [in Ukrainian].

2. Verkhovtseva, I. H., Khrystokin, H. V., & Sylka, O. Z. (2025). Sotsioinformatsiyna stiykist′ Ukrayiny u tsyfrovu epokhu. [Socio-informational stability of Ukraine in the digital age]. *Natsional'na stiykist' (rezyliyentnist') yak klyuchovyy element natsional'noyi bezpeky: arkhitektura, vyklyky ta shlyakhy posylennya – National stability (resilience) as a key element of national security: architecture, challenges and ways of strengthening:* mater. I-yi Mizhnar. nauk.-prakt. konfer. (Ivano-Frankivs′k, 27 lystopada 2025 r.). Ivano-Frankivs′k : IFNTUNH, 579–584 [in Ukrainian].

3. Floridi, L. (2014). The Fourth Revolution: How the Infosphere Is Reshaping Human Reality. Oxford : Oxford University Press. Retrieved from: https://philpapers.org/rec/FLOTFR-3 [in English].

4. Latour, B. (2005). Reassembling the Social: An Introduction to Actor-Network-Theory. Oxford : Oxford University Press, 311 p. [in English].

5. Castells, M. (1996). The Rise of the Network Society. Vol. 1. Oxford: Blackwell, 625 p. [in English].

6. Shoker, A. (2022). Digital Sovereignty. Strategies for Every Nation. *ACIG Journal*, 1 (1). https://doi.org/10.5604/01.3001.0016.0943 [in English].

7. Chouliaraki, L., & Georgiou, M. (2019). The digital border: Mobility, technology and power. *European Journal of Communication*, 34 (6), 594–605. Retrieved from: https://eprints.lse.ac.uk/103224/1/EJC._Chouliaraki_and_Georgiou._FINAL_3.pdf [in English].

8. Goldsmith, J. & Wu, T. (2006). *Who Controls The Internet? Illusions Of A Borderless World*. Oxford University Press, Inc. Retrieved from: https://jost.syr.edu/wp-content/uploads/who-controls-the-internet_illusions-of-a-borderless-world.pdf [in English].

9. Everuss, L. (2025). Entangled Borders: How the Digital Transformation of Sovereign Borders Creates Transnational Population Filters. *Philosophy & Technology*, 38 (4). https://doi.org/10.1007/s13347-025-00960-y [in English].

10. Pocheptsov, H. H. (2013). Smyslovi ta informatsiini viiny. [Semantic and information wars]. *Informatsiine suspilstvo – Information society,* 18, 21–27 [in Ukrainian].

11. Dubov, D. V. (2014). Kiberprostir yak novyi vymir heopolitychnoho supernytstva: monohrafiia. [Cyberspace as a new dimension of geopolitical rivalry: monograph.]. Kyiv : NISD, 328 p. [in Ukrainian].

12. Verkhovtseva, I. H. (2024). Hlobalnyi kiberprostir ta opir informatsiinii ahresii: kiberdyplomatiia Ukrainy u protydii rosiiskii informatsiinii invazii. [Global cyberspace and resistance to information aggression: Ukraine's cyber diplomacy in countering the Russian information invasion]. *Mizhnarodne spivtovarystvo ta Ukraina v protsesakh ekonomichnoho ta tsyvilizatsiinoho postupu: aktualni ekonomiko-tekhnolohichni, resursni, instytutsionalni, bezpekovi ta sotsiohumanitarni problem – The international community and Ukraine in the processes of economic and civilizational progress: current economic, technological, resource, institutional, security and socio-humanitarian problems:* monohrafiia. Ryga : Baltija Publishing, 213–243. https://doi.org/10.30525/978-9934-26-480-1-9 [in Ukrainian].

13. Reznikova O. O. (2022). Natsional′na stiykist′ v umovakh minlyvoho bezpekovoho seredovyshcha. [National Stability in a Changing Security Environment] : monohrafiya. Kyyiv : NISD, 532 p. [in Ukrainian].

14. Krotyuk, V. A., & Panfilov, O. Yu. (2022). Smyslova zbroya u viynakh suchasnosti. [Meaningful weapons in modern wars]. *Informatsiyno-komunikatsiyna bezpeka: suchasni trendy – Information and communication security: modern trends*: monohr.; za zah. red.: Kurban O. V., Lisnevs′ka A. L. Kyiv : Kyiv. un-t im. B. Hrinchenka, 210–238 [in Ukrainian].

15. Radzivilov, H. D. (2025). Mekhanizmy ta metody derzhavnoho upravlinnia informatsiinoiu bezpekoiu v umovakh suchasnykh vyklykiv. [Mechanisms and methods of state management of information security in the face of modern challenges]. *Suspilstvo ta natsionalni interesy – Society and national interests*, 9, 735–744 [in Ukrainian].

16. Mykolyuk, A. V. (2022). Publichne upravlinnya informatsiynoyu bezpekoyu: didzhytalizatsiya ta informatsiyna viyna. [Public management of information security: digitalization and information warfare]. *Pravo ta derzhavne upravlinnya – Law and public administration*, 1, 156–161. https://doi.org/10.32840/pdu.2022.1.23 [in Ukrainian].

17. Nesterenko, H. P., & Boyko, V. V. (2024). Vykorystannya SHI pry pryynyatti rishen′ u publichnomu upravlinni ta vidpovidal′nist′ za nykh. [The use of AI in decision-making in public administration and responsibility for them]. *Vcheni zapysky TNU imeni V. I. Vernads'koho. Seriya: Publichne upravlinnya ta administruvannya – Scientific notes of the V. I. Vernadsky TNU. Series: Public management and administration*, 35 (74), № 6, 54–59. https://doi.org/10.32782/TNU-2663-6468/2024.6/10 [in Ukrainian].

18. Kobets′, T. (2023). Osnovni pidkhody do rozuminnya "kohnityvna bezpeka" v suchasniy nautsi: politychnyy ta informatsiynyy aspekt. [Main approaches to understanding "cognitive security" in modern science: political and informational aspects]. *Visnyk L'vivs'koho universytetu. Filosofs'ko-politolohichni studiyi – Bulletin of Lviv University. Philosophical and Political Studies*, 49, 278–285. https://doi.org/10.30970/PPS.2023.49.34 [in Ukrainian].

19. Taranenko, H. H. (2024). Kohnityvna bezpeka yak vymir rosiys′ko-ukrayins′koyi viyny. [Cognitive security as a dimension of the Russian-Ukrainian war]. *Politology bulletin*, 92, 371–382. https://doi.org/10.17721/2415-881x.2024.92.371-382 [in Ukrainian].

20. Yakovlyeva, L. I. (2023). Lehitymnist′ publichnoyi vlady u merezhevomu suspil′stvi. [Legitimacy of public power in a network society]. *Aktual'ni problemy filosofiyi ta sotsiolohiyi–Current problems of philosophy and sociology,* 40, 201–205. https://doi.org/10.32782/apfs.v040.2023.34 [in Ukrainian].

21. Sinel′nikova, M. (2024). Trans- i postlyudyna – svitle maybutnye chy kinets′ lyudstva? [Trans- and posthuman – a bright future or the end of humanity?]. *Visnyk L'vivs'koho universytetu. Seriya filos.-politoloh. Studiyi – Bulletin of Lviv University. Series of Philosophical and Political Science Studies,* 55, 186–192. https://doi.org/10.30970/PPS.2024.55.22 [in Ukrainian].

22. Hryvnak, B., Lopushyns′kyy, I., & Sapizhak, I. (2024). Dezinformatsiya yak zahroza natsional′niy bezpetsi Ukrayiny v umovakh neoholoshenoyi rosiys′ko-ukrayins′koyi viyny. [Disinformation as a threat to the national security of Ukraine in the conditions of the undeclared Russian-Ukrainian war]. *Naukovyy visnyk Vinnyts'koyi akademiyi bezperervnoyi osvity. Seriya "Ekolohiya. Publichne upravlinnya ta administruvannya" – Scientific Bulletin of the Vinnytsia Academy of Continuing Education. Series "Ecology. Public Management and Administration"*, 1, 53–63. https://doi.org/10.32782/2786-5681-2024-1.07 [in Ukrainian].

23. Pazyuk, A. V. (2015). Mizhnarodne informatsiyne pravo: teoriya i praktyka [International Information Law: Theory and Practice]: monohrafiya. Dnipropetrovs′k: “Serednyak T. K.”, 447 p. [in Ukrainian].

24. Snyder, E. A. (2025). *Global Tensions: Splinternet*. Yale School of Management. Retrieved from: https://som.yale.edu/sites/default/files/2025-06/Brief%20on%20Global%20Tensions.pdf [in English].

25. Falkner, G., Heidebrecht, S., Obendiek, A.S., & Seidl, T. (2024). Digital sovereignty – Rhetoric and reality. *Journal of European Public Policy*, 31 (8), 2099–2120. https://doi.org/10.1080/13501763.2024.2358984 [in English].

26. Musiani, F. (2025). Reassessing “infrastructuring digital sovereignty”: digital self-determination as a set of infrastructure-embedded practices. *Frontiers in Communication*, 10. https://doi.org/10.3389/fcomm.2025.1562072 [in English].

27. Nocetti, J. (2024). “A Splintered Internet? Internet Fragmentation and the Strategies of China, Russia, India and the European Union”, Études de l’Ifri, Ifri. Retrieved from: https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_nocetti_internet_fragmentation_february_2024.pdf [in English].

28. Dubnyak, K. A. (2015). Informatsiynyy prostir: struktura ta funktsional′ni parametry. [Information space: structure and functional parameters]. *Derzhava ta rehiony. Seriya: Sotsial'ni komunikatsiyi – State and regions. Series: Social communications,* 4 (24), 21–25 [in Ukrainian].

29. Ukraine’s National Security Strategy ’HUMAN SECURITY – NATIONAL SECURITY’ [Enacted by Presidential Decree No. 392/2020]. Retrieved from: https://zakon.rada.gov.ua/laws/show/392/2020#Text [in Ukrainian].

30. Kasza, J. Simulacra and Simulation: The Impact of ICT Upon “Radical Transformation” of Culture. (2017). Retrieved from: https://www.semanticscholar.org/paper/Simulacra-and-Simulation%3A-The-Impact-of-ICT-Upon-of-Kasza/e6a97d2831fc4df5ed849dbfd492ea1a52a02b82 [in English].

Дата першого надходження статті до видання: 03.02.2026
Дата прийняття статті до друку після рецензування: 13.03.2026
Дата публікації (оприлюднення) статті: 20.04.2026