Адміністративне право і процес; фінансове право; інформаційне право

УДК 340+342.4+351

DOI https://doi.org/**10.5281/zenodo.15253981**

Гібридна агресія проти України як виклик модернізації правової політики у сфері інформаційної безпеки

Ряполов Антон Павлович

аспірант, кафедра теорії держави та права,

Дніпровський державний університет внутрішніх справ,

м. Дніпро, 49005, Україна,

ORCID: https://orcid.org/0009-0007-1693-507X

Прийнято: 07.04.2025| Опубліковано: 18.04.2025

Анотація. *У статті досліджено особливості гібридної агресії російської федерації проти України в інформаційному вимірі та обґрунтовано необхідність модернізації національної правової політики у сфері інформаційної безпеки. Наголошується, що інформаційна складова сучасних конфліктів стала одним із ключових інструментів впливу, а інформаційна війна – невід'ємною частиною гібридної агресії. З 2014 року, а особливо після початку повномасштабного вторгнення у 2022 році, Україна зіткнулася з потужною хвилею дезінформації, пропаганди, маніпуляцій у соціальних мережах, кібератак, а також спроб ворога підривати морально-психологічну стійкість суспільства. Аналіз показує, що чинна правова політика України залишається фрагментарною, реактивною та недостатньо ефективною в умовах динамічних інформаційних загроз. У роботі розкрито основні недоліки чинної правової політики: відсутність кодифікованого законодавства у сфері інформаційної безпеки, розмежованості між суб'єктами її забезпечення, нестачі ефективних інструментів боротьби з дезінформацією, недостатньої*

уваги до медіаграмотності та відсутності чітких процедур захисту інформаційних прав громадян. У статті запропоновано конкретні напрями модернізації правової політики: створення Інформаційного кодексу України, вдосконалення санкційного механізму, оновлення повноважень інституцій, запровадження обов'язкової медіаосвіти, імплементація європейських стандартів у діяльність онлайн-платформ, посилення судового захисту у сфері інформаційних відносин. Зроблено висновок, що стратегічна модернізація правової політики в інформаційній сфері є критично необхідною умовою для забезпечення інформаційного суверенітету держави, ефективної протидії гібридним загрозам та утвердження цінностей демократичного правопорядку в умовах воєнного часу. В умовах нових викликів держава зобов'язана перейти від фрагментарного реагування до стратегічного й цілісного підходу, що передбачає кодифікацію законодавства, ефективну координацію суб'єктів, розвиток превентивних механізмів, забезпечення прав і свобод людини та впровадження міжнародних стандартів.

Ключові слова: *гібридна агресія, інформаційна безпека, дезінформація, правова політика, інформаційна війна, національна безпека, кібербезпека, медіаграмотність, санкції, інформаційні загрози.*

Hybrid aggression against Ukraine as a challenge for modernizing legal policy in the field of information security

Riapolov Anton Pavlovych
postgraduate student, Department of theory of state and law,
Dnipro State University of Internal Affairs,
Dnipro, 49005, Ukraine,
ORCID: https://orcid.org/0009-0007-1693-507X

Abstract. *The article examines the specific features of the hybrid aggression of the russian federation against Ukraine in the information domain and substantiates the*

necessity of modernizing the national legal policy in the field of information security. It emphasizes that the informational dimension of modern conflicts has become one of the key tools of influence, while information warfare constitutes an integral part of hybrid aggression. Since 2014, and especially following the full-scale invasion in 2022, Ukraine has faced a powerful wave of disinformation, propaganda, manipulation via social media, cyberattacks, and attempts by the enemy to undermine the moral and psychological resilience of society. The analysis shows that the current legal policy of Ukraine remains fragmented, reactive, and insufficiently effective under the conditions of dynamic informational threats. The paper outlines the main shortcomings of the existing legal framework: the absence of a codified legislative act in the field of information security, lack of coordination between responsible actors, insufficient legal instruments to combat disinformation, low attention to media literacy, and the absence of clear procedures for the protection of citizens' information rights. The article proposes specific directions for the modernization of legal policy: adoption of an Information Code of Ukraine, improvement of the sanction mechanism, revision of institutional powers, implementation of mandatory media education, integration of European standards into the regulation of online platforms, and strengthening of judicial protection in information-related legal relations. It concludes that a strategic modernization of legal policy in the field of information security is a critical prerequisite for ensuring the state's informational sovereignty, effectively countering hybrid threats, and affirming the values of democratic rule of law under wartime conditions. In the face of new challenges, the state is obliged to move from a fragmented response to a strategic and holistic approach, which involves codification of legislation, effective coordination of actors, development of preventive mechanisms, ensuring human rights and freedoms, and implementation of international standards.

Keywords: *hybrid aggression, information security, disinformation, legal policy, information warfare, national security, cybersecurity, media literacy, sanctions, informational threats.*

Постановка проблеми. У XXI столітті війни дедалі рідше ведуться виключно на полі бою. Натомість дедалі більшого значення набувають нетрадиційні, комплексні форми протистояння, які поєднують військові, політичні, економічні, соціальні та інформаційні впливи. Однією з таких форм є гібридна агресія, яка становить системну та приховану діяльність держави-агресора з використанням широкого спектра інструментів впливу. Водночас одним із головних об'єктів гібридної агресії є інформаційний простір, що перетворився на ключовий інструмент досягнення стратегічних цілей ворога без формального оголошення війни.

З початком агресії російської федерації проти України у 2014 році, а особливо після повномасштабного вторгнення у 2022 році, інформаційна складова війни набула виняткового значення. Пропагандистські кампанії, фейкові новини, кібератаки, інформаційно-психологічні операції, деструктивний вплив через соціальні мережі та месенджери – все це стало інструментами ураження свідомості громадян, дестабілізації суспільства, зниження довіри до державних інституцій і послаблення міжнародної підтримки України. Особливістю інформаційної складової гібридної агресії є її масованість, тривалість і багаторівневість. Ворог одночасно працює в кількох напрямках: формування альтернативної реальності в очах світової спільноти, вплив на внутрішню політику України через інформаційні канали, створення паніки або апатії серед населення, дискредитація Збройних Сил, влади, волонтерського руху. При цьому використовуються як відкриті платформи (медіа, соціальні мережі), так і приховані механізми (бот-мережі, контрольовані блогери, маніпулятивні повідомлення під виглядом новин). Такий підхід виявив значні слабкості у традиційній системі забезпечення інформаційної безпеки, яка не була готова до протистояння із системною, добре спланованою і технологічно підтриманою агресією.

Аналіз останніх досліджень і публікацій. Питання інформаційної безпеки в умовах гібридної війни привернули увагу багатьох українських і зарубіжних науковців. Серед авторів, які досліджували цю тематику, варто

відзначити Бурдак А. [7], Власика А. [8], Горбуліну В. [12], Курбана О. [10], Марущак А. [4], Наливайко Л. [5], Присяжнюка С. [2], Сенченко О. [1], а також таких дослідників, як Зайченко В., Калакуру Я. [6], Кибіча Я. [9], Лалак О. [14], Меренича О. [11], Наливайко І. [3], Шепітько Т. [15] та ін. Їхні праці становлять важливу теоретичну й аналітичну базу для формування цілісного уявлення про специфіку інформаційних загроз, об'єктів та суб'єктів інформаційної безпеки, принципи інформаційної політики в умовах гібридної агресії. Однак, попри наявність значного масиву напрацювань, проблематика модернізації саме правової політики держави у цій сфері залишається недостатньо систематизованою, що і зумовлює актуальність запропонованого дослідження.

Виділення невирішених раніше частин загальної проблеми. Досвід України став безпрецедентним для всієї Європи, адже вперше на практиці показав, наскільки потужною може бути інформаційна війна в межах класичного збройного конфлікту. На цьому тлі виникає об'єктивна потреба в глибокому оновленні правової політики держави у сфері інформаційної безпеки, яка має стати не лише реакцією на загрози, а й стратегічно орієнтованою системою превентивного захисту, адаптованою до умов гібридного протистояння. Сучасна війна вимагає не лише фізичної стійкості, а й інформаційної витривалості – здатності протидіяти дезінформації, зберігати інформаційну автономію та гарантувати безпечний і правдивий інформаційний простір для своїх громадян.

Формулювання цілей статті (постановка завдання). Мета дослідження – аналіз впливу гібридної агресії російської федерації на інформаційний простір України як ключового чинника, що обумовлює необхідність модернізації національної правової політики у сфері інформаційної безпеки. У межах дослідження буде розглянуто характер гібридних загроз, виявлено недоліки чинної системи правового регулювання та запропоновано напрями її вдосконалення з урахуванням сучасних викликів.

Виклад основного матеріалу дослідження. Гібридна агресія російської федерації проти України є багатокомпонентною і включає системне використання інформаційних, психологічних, кібернетичних та медійних

інструментів, спрямованих на дестабілізацію суспільства, підрив державного суверенітету та ослаблення здатності до спротиву. Особливої інтенсивності вона набула з початком повномасштабного вторгнення у 2022 році, що супроводжувалося потужною хвилею дезінформації, інформаційно-психологічних операцій (ІПсО), фейкових наративів, спрямованих на внутрішній і зовнішній інформаційний фронт. Одним із головних інструментів гібридної агресії є дезінформація та пропаганда, яка реалізується через контрольовані рф інформаційні ресурси, соціальні мережі та навіть окремі «нейтральні» міжнародні платформи. Основна мета – вплинути на громадську думку, посіяти панічні настрої, підірвати довіру до українських інституцій, армії та міжнародних партнерів. Російські медіа систематично поширюють викривлену або відверто фейкову інформацію щодо ситуації на фронті, внутрішньополітичної ситуації, економічного стану країни та ролі західних союзників. Такі дії є прикладом свідомого втручання у внутрішні справи суверенної держави та порушення норм міжнародного права [1, с. 41-45].

Важливою складовою є кіберагресія – атаки на інформаційні ресурси державних органів, об'єкти критичної інфраструктури, банківську систему, медіа тощо. У 2022–2024 роках було зафіксовано десятки масштабних кібератак, які паралізували електронні сервіси, порушували функціонування державних реєстрів, викрадали персональні дані або поширювали шкідливе ПЗ. Наприклад, у січні 2022 року кібератака на сайти уряду України була визнана найбільш скоординованою за останні роки [2, с. 192-198]. Ще одним вектором є маніпуляція через соціальні мережі, які стали майданчиком для поширення проросійських наративів через анонімні акаунти, ботоферми та псевдоблогерів. У цьому контексті особливу небезпеку становить використання генеративного штучного інтелекту для створення глибоких фейків (deepfakes), маніпулятивних відео, фальшивих новин, які важко ідентифікувати та спростувати. За даними Міністерства цифрової трансформації, у другій половині 2024 року було виявлено низку інформаційних кампаній, які реалізовувалися із застосуванням GPT-моделей для масового генерування фейкових текстів, спрямованих на

деморалізацію населення [3, с. 179-186]. Крім технологічних атак, ворог активно використовує історичні та культурні наративи як засіб м'якої сили для ідеологічного обґрунтування своєї агресії. Через концепт «русского міра» пропагандисти намагаються переконати, що українська державність – штучне утворення, а території України нібито історично належать росії. Така риторика, підкріплена маніпулятивним використанням фактів, має на меті делегітимізацію самої ідеї української нації [4, с. 5-9]. Не менш небезпечною є інформаційна атака на зовнішньополітичному фронті, де рф через інформаційні агентства та дипломатичні структури поширює дезінформацію на міжнародному рівні. Вона намагається впливати на громадську думку в Європі та США, викликати сумніви у доцільності допомоги Україні, поширюючи наративи про «корумповану українську владу», «військові злочини» ЗСУ, «неонацизм» тощо [5, с. 28-34]. Гібридна агресія в інформаційному вимірі є системною, багатоетапною та стратегічно організованою. Її особливістю є поєднання відкритого впливу, прихованих операцій та високотехнологічних засобів, що вимагає від України не лише оперативного реагування, а й модернізації всієї правової політики у сфері інформаційної безпеки з урахуванням міжнародних стандартів і поточних викликів.

З початком гібридної агресії російської федерації правова політика України у сфері інформаційної безпеки набула особливого значення. Саме нормативно-правові засади формують основу протидії інформаційним загрозам, визначають механізми реагування та координують діяльність відповідних державних інституцій. У перші роки конфлікту державна політика у цій сфері залишалася переважно декларативною та фрагментарною, однак із 2022 року спостерігається зростання динаміки правотворчості, посилення ролі окремих суб'єктів інформаційної безпеки, а також спроби формування більш цілісного правового підходу [6, с. 69-84]. Проте цей процес супроводжується низкою проблем, що вказують на потребу у глибокій модернізації відповідної політики.

Передусім варто зазначити, що чинна законодавча база України у сфері інформаційної безпеки не є систематизованою. Норми, які регулюють

інформаційні відносини в умовах воєнного стану, кібербезпеку, діяльність ЗМІ, протидію дезінформації, розкидані по різних нормативно-правових актах – Конституції України, законах «Про національну безпеку України», «Про інформацію», «Про основні засади забезпечення кібербезпеки України», «Про санкції», «Про телебачення і радіомовлення», «Про захист персональних даних» тощо [8, с. 32-36]. Відсутність єдиного кодифікованого акту, який би унормовував принципи, поняття, цілі, суб'єктів, форми та методи забезпечення інформаційної безпеки, значно ускладнює практичне правозастосування, спричиняє дублювання повноважень та правову невизначеність.

Серйозною проблемою залишається неузгодженість між суб'єктами, що реалізують політику у сфері інформаційної безпеки. Повноваження в цій сфері поділені між Службою безпеки України, Радою національної безпеки і оборони України, Міністерством оборони, Держспецзв'язку, Національною радою з питань телебачення і радіомовлення, Міністерством культури та інформаційної політики, Міністерством цифрової трансформації, окремими органами судової та виконавчої влади. Проте механізм міжвідомчої координації виявляється недостатньо ефективним, а подекуди й суто формальним. Як наслідок, держава демонструє реактивну модель реагування на інформаційні виклики, замість того щоб вибудовувати превентивну, гнучку та стратегічно спрямовану політику [9, с. 94-111].

Іншим вразливим аспектом є нестача правових інструментів для боротьби з дезінформацією. Україна не має спеціального закону про дезінформацію або фейкові новини, а спроби законодавчого врегулювання (зокрема проєкт Закону України «Про дезінформацію» 2020 року) викликали серйозні дискусії в суспільстві та серед правозахисників. Наразі єдиним ефективним інструментом боротьби з проросійською інформаційною агресією залишаються санкції, які запроваджуються рішеннями РНБО та вводяться в дію указами Президента України [10, с. 55-66]. Проте санкційний механізм – це здебільшого реакція на вже скоєні порушення, а не спосіб запобігання їм. Окремо варто наголосити на тому, що правова політика у сфері інформаційної безпеки не враховує належною

мірою освітній та культурний компоненти. Державна стратегія щодо медіаграмотності населення – хоча і декларується як пріоритет – досі не має чіткої законодавчої підтримки. У чинних законах відсутні норми про обов'язкове включення медіаосвіти до навчальних програм, а на рівні шкільної та вищої освіти ця тематика часто представлена у вигляді факультативів або разових ініціатив. У результаті громадяни залишаються вразливими до інформаційних маніпуляцій, фейків та пропаганди, а отже – зростає ризик внутрішнього розколу та зниження опірності суспільства. Потребує перегляду і стан захисту прав громадян у сфері інформаційної безпеки. В умовах воєнного стану низка прав і свобод – зокрема свобода слова, доступ до інформації, свобода ЗМІ – зазнає обмежень [11, с. 417-422]. Хоча такі обмеження допустимі згідно з Конституцією України та міжнародними стандартами, вони повинні мати чітке нормативне обґрунтування, бути пропорційними та тимчасовими. Водночас в Україні відсутній механізм незалежного моніторингу за дотриманням таких обмежень, що може призводити до зловживань та недовіри до рішень держави в інформаційній сфері.

Попри зусилля держави у протидії інформаційній агресії та розвиток окремих елементів нормативно-правової системи, правова політика України у сфері інформаційної безпеки залишається такою, що потребує концептуального оновлення. Актуальними є завдання з формування єдиного кодифікованого акту, удосконалення міжвідомчої координації, створення правових механізмів боротьби з дезінформацією, запровадження медіаосвіти як елементу державної політики, а також – створення системи захисту інформаційних прав людини [12, с. 383]. Без виконання цих завдань неможливо забезпечити належний рівень інформаційної безпеки в умовах тривалої гібридної агресії.

Реалії повномасштабної гібридної агресії проти України висунули перед державою потребу не лише оперативно реагувати на інформаційні загрози, а й формувати стратегічно вивірену, цілісну та ефективну правову політику у сфері інформаційної безпеки. Актуальність модернізації цієї політики зумовлена як внутрішніми чинниками (нормативна фрагментарність, неузгодженість

суб'єктів, брак профілактичних механізмів), так і зовнішніми – зокрема, новими методами інформаційної війни, широким використанням штучного інтелекту та поглибленням інформаційної взаємозалежності світу. У цьому контексті визначаються низка ключових напрямів, що потребують законодавчого вдосконалення, інституційного оновлення та концептуального переосмислення.

Першочерговим завданням є розробка та прийняття комплексного кодифікованого акту, який би унормував сферу інформаційної безпеки – зокрема, Інформаційного кодексу України. Такий акт має не лише систематизувати чинні норми, що містяться у понад десятку різних законів, а й закріпити основні поняття, принципи, суб'єктів, механізми реалізації політики у цій сфері. Аналогічний досвід існує в низці держав – наприклад, Франції, де функціонує Кодекс внутрішньої безпеки, або Литви, де відповідні положення зведені в Національну стратегію кібер- та інформаційної безпеки [13, с. 95]. В українському контексті така кодифікація дозволить підвищити передбачуваність та ефективність правозастосування, усунути дублювання норм, спростити міжвідомчу координацію.

Наступним важливим кроком є оновлення санкційної політики у сфері інформаційної безпеки. Санкції залишаються ключовим інструментом нейтралізації проросійських інформаційних ресурсів, однак потребують більш прозорих і чітких процедур. Необхідно нормативно визначити підстави, критерії, порядок виявлення інформаційних загроз, роль уповноважених суб'єктів у ініціюванні санкцій, гарантії захисту прав суб'єктів, проти яких застосовуються обмежувальні заходи. Водночас санкції мають супроводжуватися інформаційною кампанією для суспільства – з поясненням причин їх запровадження, правових підстав і очікуваного ефекту.

Також потребує вдосконалення інституційне забезпечення інформаційної безпеки. Доцільно розширити повноваження Центру протидії дезінформації, перетворивши його на повноцінний координаційний орган із міжвідомчими функціями та правом ініціювати нормативні зміни. Усі державні органи, дотичні до сфери інформаційної безпеки, повинні діяти в межах чітко визначених

компетенцій, з урахуванням принципу субсидіарності та необхідності уникнення дублювання функцій [14]. До системи суб'єктів має бути також включено громадянське суспільство – профільні НУО, незалежні медіа, асоціації журналістів – як рівноправних партнерів у забезпеченні прозорості та демократичності інформаційної політики.

У межах модернізації правової політики важливе значення має розвиток інструментів превентивного впливу. Йдеться, зокрема, про необхідність запровадження обов'язкового вивчення основ медіаграмотності та критичного мислення в закладах освіти всіх рівнів. Для цього слід внести зміни до законів «Про освіту» та «Про повну загальну середню освіту», доповнивши їх положеннями про інформаційно-аналітичну безпеку учнів і студентів. Крім того, варто підтримати реалізацію державних програм із підвищення цифрової грамотності дорослого населення – із залученням місцевих громад, бібліотек, освітніх центрів.

Окремого правового врегулювання потребує питання відповідальності онлайн-платформ за поширення дезінформації. Доцільно імплементувати елементи європейських підходів, зокрема положення Директиви (ЄС) 2018/1808 про аудіовізуальні медіапослуги, яка покладає на провайдерів обов'язок запобігати розповсюдженню мови ворожнечі, недостовірної інформації, а також забезпечувати прозорість власності й редакційної політики [15, с. 138-144]. В Україні ж донині відсутні правові норми, які б регулювали відповідальність таких платформ у межах внутрішньої юрисдикції.

Ще одним важливим напрямом є розвиток судового захисту прав у сфері інформаційних відносин. У контексті воєнного стану та обмеження доступу до інформації зростає потреба в ефективних, швидких і незалежних процедурах захисту прав на свободу вираження поглядів, право на доступ до публічної інформації, захист честі, гідності, ділової репутації. Для цього доцільно створити спеціалізовані палати або підрозділи у складі адміністративних судів, що спеціалізуватимуться на інформаційних спорах. Крім того, необхідно

законодавчо встановити чіткі критерії законності обмежень прав під час війни – з урахуванням практики Європейського суду з прав людини.

Висновки. Узагальнюючи викладене, модернізація правової політики у сфері інформаційної безпеки вимагає не лише оновлення окремих законодавчих норм, а цілісного переосмислення підходів до інформаційного суверенітету держави, ролі суспільства у протидії інформаційним загрозам, а також визначення нових стандартів взаємодії держави, медіа та громадян у цифровому середовищі. Така модернізація має ґрунтуватися на засадах верховенства права, поваги до прав людини та демократичного врядування, що є водночас і ключовими орієнтирами для українського шляху до Європейського Союзу. Гібридна агресія російської федерації продемонструвала вразливість інформаційного простору України та виявила системні недоліки чинної правової політики у сфері його захисту. В умовах нових викликів держава зобов'язана перейти від фрагментарного реагування до стратегічного й цілісного підходу, що передбачає кодифікацію законодавства, ефективну координацію суб'єктів, розвиток превентивних механізмів, забезпечення прав і свобод людини та впровадження міжнародних стандартів. Модернізована правова політика в інформаційній сфері є необхідною умовою збереження національної єдності, демократичного розвитку та інформаційного суверенітету України.

Отже, внесок цієї статті спрямований на розробку сучасних підходів до протидії впливу гібридної агресії російської федерації на інформаційний простір України як ключового чинника, що обумовлює необхідність модернізації національної правової політики у сфері інформаційної безпеки, враховуючи пропозиції з її вдосконалення з урахуванням сучасних викликів.

Список використаних джерел

1. Сенченко О. Новий виклик людству – гібридна війна. *Вісник Книжкової палати*. 2017. № 5. С. 41-45 (дата звернення: 03.04.2025)

2. Присяжнюк С. Модернізація механізмів реалізації гуманітарної політики України. *Вісник Львівського університету. Серія філос.-політолог. студії.* 2023. № 51. С. 192-198 (дата звернення: 03.04.2025).

3. Наливайко І. О. Теоретико-правова характеристика соціального захисту учасників бойових дій в Україні. *Аналітичне-порівняльне правознавство*. 2023. № 2. С. 179-186. URL : http://journalapp.uzhnu.edu.ua/ article/view/282699/276886 (дата звернення: 03.04.2025).

4. Марущак А. І. Дослідження проблем інформаційної безпеки у юридичній науці. *Інформація і право*. 2021. № 3(36). С. 5-9 (дата звернення: 03.04.2025).

5. Наливайко Л. Р. Громадська експертиза як форма громадського контролю: проблеми теорії та практики. *Університетські наукові записки*. 2014. № 2. С. 28-34. URL : https://er.dduvs.in.ua/bitstream/123456789/2028/1/12.pdf (дата звернення: 03.04.2025).

6. Калакура Я. Методологічні засади інформаційного менеджменту в умовах окупаційно-гібридної війни Росії проти України. *Український інформаційний простір*. 2021. № 1(7). С. 69-84 (дата звернення: 03.04.2025).

7. Бурдак А. А. Інформаційна безпека України в умовах викликів сьогодення. *Молодий вчений*. 2024. № 30. С. 32-36 (дата звернення: 03.04.2025).

8. Власик А. С. Національна безпека України: еволюція проблем внутрішньої політики: монографія. К. : НІСД, 2016. 528 с. (дата звернення: 03.04.2025).

9. Кибіч Я. В. Особливості формування кібернетичної безпеки в умовах гібридної війни. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2018. № 6. С. 94-111 (дата звернення: 03.04.2025).

10. Курбан О. В. Основи сучасної національної інформаційної безпеки України. *Вісник Харківської державної академії культури. Серія: Соціальні комунікації*. 2017. № 50. С. 55-66 (дата звернення: 03.04.2025).

11. Меренич О. С. Структурні елементи нормативно-правового механізму забезпечення національної безпеки України: роль оборонно-стратегічних документів. *Право і суспільство*. 2024. № 5. С. 417-422 (дата звернення: 03.04.2025).

12. Горбуліна В. П. Світова гібридна війна: український фронт: монографія. К. : НІДС, 2017. 496 с. (дата звернення: 03.04.2025).

13. Зайченко В. В. Стратегічні пріоритети забезпечення технологічної конкурентоспроможності економіки України. *Регіональна економіка*. 2020. № 1. С. 95 (дата звернення: 03.04.2025).

14. Лалак О. А. Ризики і виклики кібербезпеки: досвід України та Польщі. *International relations*. 2017. № 13 (дата звернення: 03.04.2025).

15. Шепітько Т. В. До питання про сутнісні виміри гібридної війни: класичні і новітні уявлення. Політикус. 2021. № 1. С. 138-144 (дата звернення: 03.04.2025).