УДК 342.35
DOI https://doi.org/10.24144/2307-3322.2025.89.3.12

НОРМАТИВНО-ПРАВОВІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ АГРЕСІЇ

Ряполов А.П.,
аспірант кафедри теорії держави і права
Дніпровського державного університету внутрішніх справ
ORCID: 0009-0007-1693-507X

Ряполов А.П. Нормативно-правові основи інформаційної безпеки України в умовах гібридної агресії.

У статті досліджено нормативно-правові основи інформаційної безпеки України в умовах гібридної агресії російської федерації. Визначено, що інформаційна безпека, як складова національної безпеки, набула особливого значення в умовах сучасного збройного конфлікту, у межах якого активно застосовуються інструменти інформаційного впливу, дезінформації, пропаганди та кібератак. Автором проаналізовано чинну законодавчу та нормативну базу, зокрема, Конституцію України, закони «Про національну безпеку України», «Про інформацію», «Про основні засади забезпечення кібербезпеки України», стратегії, укази Президента України, рішення Ради національної безпеки і оборони України, а також інші спеціальні акти, що формують систему нормативного регулювання у сфері захисту національного інформаційного простору. Окрему увагу приділено впливу гібридної агресії на зміст, структуру та динаміку правового регулювання. Показано, що російська агресія стала каталізатором змін у законодавстві, спричинила посилення державного контролю, створення нових інституцій (зокрема Центру протидії дезінформації), розширення повноважень органів публічної влади та запровадження особливих правових режимів. Виокремлено ключові виклики, пов'язані з необхідністю збереження балансу між забезпеченням інформаційної безпеки та дотриманням конституційних прав і свобод, зокрема свободи слова, права на інформацію та приватність. Сформульовано пропозиції щодо вдосконалення законодавства у цій сфері, зокрема шляхом систематизації норм, чіткого розмежування повноважень суб'єктів інформаційної безпеки, удосконалення процедур судового захисту, підвищення рівня правової та медіаграмотності населення, а також імплементації міжнародних стандартів. Враховуючи динаміку інформаційних загроз, автор підкреслює необхідність гнучкого, прозорого та стратегічно скоординованого підходу до нормативно-правового забезпечення інформаційної безпеки України, що має враховувати швидко змінювані технології та глобальні тенденції у сфері кібербезпеки. Наголошується, що ефективна реалізація державної інформаційної політики потребує не лише вдосконалення законодавства, а й належного ресурсного забезпечення, міжвідомчої координації та активної взаємодії з громадянським суспільством.

Ключові слова: інформаційна безпека, гібридна агресія, правове регулювання, дезінформація, національна безпека, медіаграмотність, законодавство, кібербезпека, свобода слова, нормативно-правова база.

Riapolov A.P. Legal and regulatory foundations of information security in Ukraine under conditions of hybrid aggression.

The article examines the regulatory and legal foundations of information security in Ukraine in the context of the Russian Federation's hybrid aggression. It is determined that information security, as a component of national security, has acquired special importance in the context of a modern armed conflict, within which tools of information influence, disinformation, propaganda, and cyberattacks are actively used. The author analyzed the current legislative and regulatory framework, in particular, the Constitution of Ukraine, the laws «On National Security of Ukraine», «On Information», «On the Basic Principles of Ensuring Cybersecurity of Ukraine», strategies, decrees of the President of Ukraine, decisions of the National Security and Defense Council of Ukraine, as well as other special acts, that

form the system of regulatory regulation in the field of protection of the national information space. Special attention is paid to the impact of hybrid aggression on the content, structure, and dynamics of legal regulation. It is demonstrated that Russian aggression has become a catalyst for legislative changes, resulting in increased state control, the establishment of new institutions (notably, the Center for Countering Disinformation), the expansion of public authorities' powers, and the introduction of special legal regimes. Key challenges related to the need to maintain a balance between ensuring information security and respecting constitutional rights and freedoms, in particular freedom of speech, the right to information, and privacy, are highlighted. Proposals have been formulated to improve legislation in this area, in particular by systematizing norms, clearly delimiting the powers of information security entities, improving judicial protection procedures, increasing the level of legal and media literacy of the population, as well as implementing international standards. Given the dynamics of information threats, the author emphasizes the need for a flexible, transparent, and strategically coordinated approach to the regulatory and legal support of information security in Ukraine, which should take into account rapidly changing technologies and global trends in the field of cybersecurity. It is emphasized that the effective implementation of state information policy requires not only improving legislation, but also proper resource provision, interdepartmental coordination, and active interaction with civil society.

Key words: information security, hybrid aggression, legal regulation, disinformation, national security, media literacy, legislation, cybersecurity, freedom of speech, legal framework.

Постановка проблеми. В умовах сучасних глобальних викликів інформаційна безпека стала ключовим елементом національної безпеки держави. Особливо це стосується України, яка з 2014 року стикається з безпрецедентною гібридною агресією з боку російської федерації. Ця агресія включає не лише військові дії, але й потужні інформаційні атаки, спрямовані на дестабілізацію суспільства, підрив довіри до державних інституцій та маніпулювання громадською думкою. Використання дезінформації, кібератак, пропаганди та інших засобів інформаційного впливу стало невід'ємною складовою сучасних конфліктів, що підкреслює необхідність формування ефективної системи нормативно-правового забезпечення інформаційної безпеки.

Метою дослідження є аналіз чинної нормативно-правової бази України у сфері інформаційної безпеки в контексті гібридної агресії, виявлення її недоліків та розробка рекомендацій щодо її вдосконалення для ефективної протидії сучасним інформаційним загрозам.

Стан опрацювання проблематики показує, що дослідження зумовлена тим, що в умовах гібридної війни інформаційний простір перетворюється на поле бою, де відбувається боротьба за свідомість та лояльність громадян. Недостатня правова регламентація та відсутність чітких механізмів протидії інформаційним загрозам можуть призвести до серйозних наслідків, таких як посилення соціальної напруги, розкол у суспільстві та підрив державного суверенітету. Тому дослідження та вдосконалення нормативно-правових основ інформаційної безпеки України є надзвичайно важливим завданням для забезпечення стійкості та стабільності держави.

Проблематика інформаційної безпеки в умовах гібридної війни стала предметом уваги багатьох вітчизняних та зарубіжних науковців. Серед дослідників, які зробили значний внесок у вивчення цієї тематики, можна відзначити: Арістову І., Кормича Б., Ментух Н., Олійника О., Сулацького Д. та ін. Їхні праці присвячені різним аспектам інформаційної безпеки, включаючи організаційно-правові основи, політику інформаційної безпеки, захист інформаційних ресурсів та інші ключові питання. Незважаючи на значний внесок цих дослідників, питання нормативно-правового забезпечення інформаційної безпеки України в умовах гібридної агресії потребує подальшого комплексного аналізу з урахуванням сучасних викликів та загроз. Це обумовлює необхідність детального вивчення та вдосконалення правових механізмів, спрямованих на захист національного інформаційного простору

Виклад основного матеріалу. Нормативно-правове регулювання інформаційної безпеки в Україні базується на системному підході, який охоплює як стратегічне бачення національної безпеки в цілому, так і конкретні правові інструменти, спрямовані на запобігання інформаційним загрозам, що загострилися в умовах гібридної агресії російської федерації. Загальні засади такого регулювання формуються в межах Конституції України, законів, підзаконних нормативно-правових актів, указів Президента України, рішень РНБО, а також міжнародних договорів, ратифікованих Верховною Радою України.

Важливою базою правового забезпечення інформаційної безпеки є Конституція України, яка проголошує свободу думки і слова, вільний доступ до інформації (ст. 34), а також закріплює обов'язок держави захищати національні інтереси, включно з безпековими аспектами (ст. 17) [1]. Законодавчим підґрунтям нормативного регулювання виступає Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII, який визначає інформаційну безпеку як складову національної безпеки та передбачає необхідність її забезпечення у сферах інформаційних ресурсів, кібербезпеки, інформаційного простору, протидії пропаганді та маніпулятивному впливу [2].

Одним із ключових документів, який визначає стратегічні орієнтири у цій сфері, є Стратегія інформаційної безпеки України, затверджена Указом Президента України від 14 травня 2021 року № 187/2021. У Стратегії наголошено на необхідності посилення протидії дезінформації, розвитку медіаграмотності, забезпеченні кіберзахисту, охороні критичної інформаційної інфраструктури, захисті журналістів та свободи слова, а також створенні ефективної системи реагування на загрози в інформаційній сфері [3]. Крім того, правове регулювання інформаційної безпеки здійснюється за допомогою спеціальних законів, серед яких важливе місце займає Закон України «Про інформацію», який визначає правові основи доступу до інформації, її захисту та класифікації, а також регулює обіг інформації у суспільстві [4].

Значну роль у забезпеченні кібербезпеки, як складової інформаційної безпеки, відіграє Закон України «Про основні засади забезпечення кібербезпеки України», який закріплює принципи кіберзахисту, визначає суб'єктів у сфері кібербезпеки та встановлює їхні повноваження [5]. У сфері діяльності медіа та захисту інформаційного простору працюють положення Закону України «Про телебачення і радіомовлення», «Про друковані засоби масової інформації (пресу) в Україні», «Про доступ до публічної інформації». Вони формують правові основи для функціонування незалежних ЗМІ, визначають правила розповсюдження інформації та встановлюють межі дозволеного, зокрема в умовах воєнного або надзвичайного стану [6-7]. Розгалужена структура нормативно-правових актів у сфері інформаційної безпеки доповнюється численними актами Президента України, рішеннями РНБО, постановами Кабінету Міністрів України, які регламентують порядок реалізації окремих повноважень, особливо у період воєнного стану. У цьому контексті особливе значення має практика застосування рішень РНБО, введених у дію указами Президента щодо санкцій, блокування інформаційних ресурсів, протидії деструктивному інформаційному впливу тощо [8].

Засади нормативно-правового регулювання інформаційної безпеки в Україні становлять комплексну систему правових норм, що функціонують у межах загальнонаціональної стратегії безпеки. Вони забезпечують юридичне підґрунтя для реалізації державної політики у сфері захисту інформаційного простору, особливо в умовах гібридної агресії з боку російської федерації, яка потребує оперативного та ефективного реагування [9]. Водночас ця система потребує подальшого вдосконалення, зокрема в аспектах кодифікації, чіткого розподілу компетенції між суб'єктами, а також імплементації міжнародних стандартів інформаційної безпеки.

Вплив гібридної агресії на правове регулювання інформаційної безпеки в Україні є визначальним чинником трансформації нормативно-правової системи, що охоплює як зміст, так і динаміку правотворчих процесів. Починаючи з 2014 року, після незаконної анексії Автономної Республіки Крим та частини територій Донецької і Луганської областей, російська федерація послідовно застосовує широкий арсенал засобів інформаційного впливу проти України. З початком повномасштабного вторгнення у 2022 році ці процеси набули ще більшого масштабування, а інформаційний простір перетворився на одне з головних полів бою. Це, у свою чергу, зумовило необхідність термінового перегляду підходів до правового регулювання сфери інформаційної безпеки.

Одним із найбільш показових проявів впливу гібридної агресії стало значне посилення правових механізмів державного реагування на загрози в інформаційному середовищі. Зокрема, в умовах воєнного стану було активовано практику прийняття рішень Ради національної безпеки і оборони України, які набувають юридичної сили після введення їх у дію Указами Президента. У цих рішеннях часто містяться заходи з блокування інформаційних ресурсів, пов'язаних з державою-агресором, або таких, що поширюють проросійську дезінформацію, розпалюють ворожнечу чи підривають обороноздатність держави [8]. Також було посилено кримінально-правові механізми, зокрема, введено додаткову відповідальність за колабораціонізм, поширення недостовірної інформації в умовах війни, публічне виправдовування збройної агресії проти України, передачу

ворогові інформації про розташування Збройних Сил України тощо. Ці положення були закріплені у змінах до Кримінального кодексу України, ухвалених після 24 лютого 2022 року [10]. У відповідь на масштабну дезінформаційну кампанію було створено Центр протидії дезінформації, що діє при РНБО України, основним завданням якого є виявлення фейків, інформаційних маніпуляцій і координація заходів протидії інформаційним загрозам. Діяльність цього органу не лише потребувала нормативного оформлення, а й стала стимулом для розробки додаткових підзаконних актів, методичних рекомендацій і протоколів взаємодії між суб'єктами безпеки.

В умовах гібридної війни держава була змушена балансувати між забезпеченням свободи слова та реалізацією функції самозахисту. З цією метою Національна рада України з питань телебачення і радіомовлення отримала розширені повноваження щодо тимчасового або постійного припинення мовлення телеканалів, діяльність яких створює загрозу національній безпеці, а також вживає заходів щодо недопущення в ефір проросійських наративів або прихованої пропаганди [6]. Водночас важливою зміною, викликаною гібридною агресією, стало посилення ролі громадянського суспільства у забезпеченні інформаційної безпеки. Були запущені освітні й просвітницькі кампанії, спрямовані на підвищення рівня медіаграмотності, зокрема з ініціативи Міністерства культури та інформаційної політики, а також завдяки участі громадських організацій. Така активність отримала підтримку і на нормативному рівні – положення про формування критичного мислення і протидію фейкам дедалі частіше включаються до національних стратегій і державних програм.

Гібридна агресія російської федерації мала суттєвий вплив на зміст і структуру нормативно-правового регулювання інформаційної безпеки в Україні. Відбулося оперативне оновлення законодавства, розширення повноважень відповідних органів, активізація співпраці між державою та суспільством. Водночас залишається актуальним завданням удосконалення правових механізмів в аспекті дотримання стандартів прав людини, демократичного врядування та забезпечення належного контролю за реалізацією повноважень у сфері інформаційної безпеки.

У сучасних умовах, коли інформаційна сфера перетворилася на простір жорсткої боротьби за вплив на свідомість громадян, нормативно-правове забезпечення інформаційної безпеки постає одним із головних інструментів захисту суверенітету та демократичного розвитку України. Проведений аналіз дає підстави зробити висновок, що вітчизняна правова система продемонструвала здатність до адаптації до нових викликів, які зумовлені гібридною агресією російської федерації. Законодавча база зазнала значного розширення, було створено нові інститути, запроваджено спеціальні процедури реагування на інформаційні загрози [13]. Водночас, на тлі надзвичайного режиму воєнного стану, виникають і нові виклики, пов'язані із дотриманням балансу між безпековими цілями та захистом прав людини, свободою слова, прозорістю діяльності органів публічної влади.

Висновки. У контексті перспектив подальшого вдосконалення законодавства вбачається доцільним звернути увагу на кілька ключових напрямів. По-перше, необхідна систематизація правових норм у сфері інформаційної безпеки, з урахуванням того, що вони сьогодні розпорошені у великій кількості актів різної юридичної сили. Це ускладнює їх застосування та ефективне правозастосування. Виходом може бути розробка та прийняття єдиного кодифікованого акту – наприклад, Інформаційного кодексу України.

По-друге, варто переглянути підходи до визначення повноважень суб'єктів забезпечення інформаційної безпеки, зокрема у частині чіткої регламентації механізмів взаємодії між державними органами та суб'єктами громадянського суспільства. Необхідно також удосконалити законодавчі положення, що стосуються оперативного інформування населення в умовах надзвичайних ситуацій, алгоритмів спростування дезінформації та правової відповідальності за її поширення. У цьому контексті доцільно враховувати міжнародний досвід, зокрема директиви Європейського Союзу, як-от Директива (ЄС) 2018/1808 щодо аудіовізуальних медіапослуг, яка посилює вимоги до прозорості медіа та відповідальності онлайн-платформ [11].

По-третє, потрібно підвищити якість правового регулювання у сфері медіаграмотності, оскільки критичне мислення громадян є не менш важливим елементом інформаційної безпеки, ніж технічні засоби захисту. Варто передбачити в освітньому законодавстві України обов'язкове включення тематики медіаграмотності до навчальних програм різного рівня – від загальної середньої освіти до вищої.

По-четверте, необхідно удосконалити інструменти судового захисту в разі порушення прав осіб у сфері інформаційних відносин. Показовими є приклади судової практики Європейського

суду з прав людини, зокрема рішення у справах «Шмідт проти Австрії» (Schmid v. Austria) або «Сатакуннан Маркетінтімі і Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland), які підкреслюють важливість дотримання балансу між свободою вираження поглядів і захистом прав інших осіб на приватність [12].

У підсумку можна констатувати, що правове забезпечення інформаційної безпеки України значною мірою відповідає сучасним викликам, однак потребує подальшої глибокої модернізації – не тільки у відповідь на зовнішні загрози, але й для зміцнення засад демократичної правової держави. Зміцнення нормативної бази, підвищення правової обізнаності громадян, координація між державними та громадськими суб'єктами інформаційної безпеки – це ключові орієнтири для подальшого руху України у цьому напрямі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр.
2. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
3. Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента України від 14.05.2021 р. № 187/2021. *Президент України*. URL: https://zakon.rada.gov.ua/laws/show/187/2021.
4. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
6. Про телебачення і радіомовлення: Закон України від 21.12.1993 р. № 3759-XII. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/3759-12.
7. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2939-17.
8. Про рішення Ради національної безпеки і оборони України від 19.03.2021 р. «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 23.03.2021 р. № 109/2021. *Президент України*. URL: https://zakon.rada.gov.ua/laws/show/109/2021.
9. Nalyvaiko, L. R. (2014). Transparency as a democratic standard of the government functioning. *Evropský politický a právní diskurz*, 4, 51–61. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/evrpol_2014_1_4_5.pdf.
10. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2341-14.
11. Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018. *EUR-Lex*. URL: https://eur-lex.europa.eu/eli/dir/2018/1808/oj.
12. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Grand Chamber Judgment of 27 June 2017. *HUDOC.* URL: https://hudoc.echr.coe.int/fre?i=001-175121.
13. Наливайко О.І. Порівняльно-правовий аналіз реалізації процедури імпічменту. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2011. № 3. С. 61–70.