УДК 316.485.26:316.77(477)
DOI https://doi.org/10.24144/2307-3322.2025.90.3.52

ПРОБЛЕМНІ ПИТАННЯ ПРОТИДІЇ РОСІЙСЬКІЙ ІНФОРМАЦІЙНІЙ АГРЕСІЇ

Петренко С.,
науковий співробітник науково-організаційного центру
Національної академія Служби безпеки України,
ORCID: 0000-0003-1219-2401
e-mail: sveta.iris.av@gmail.com

Ільченко Ю.,
науковий консультант науково-організаційного центру
Національної академія Служби безпеки України,
ORCID: 0009-0006-9592-3642
e-mail: yposst66@gmail.com

Петренко С.В., Ільченко Ю.О. Проблемні питання протидії російській інформаційній агресії.

Інформаційна агресія в умовах гібридної війни перетворилася на потужний інструмент державного впливу, що дозволяє досягати політичних, військових і соціальних цілей без прямого застосування сили. В умовах повномасштабного вторгнення російської федерації проти України інформаційний тиск набув безпрецедентного масштабу, охоплюючи як внутрішній, так і міжнародний інформаційний простір. Основними цілями таких дій є дестабілізація українського суспільства та органів влади, підрив довіри до державних інституцій, дискредитація Збройних сил України, поширення панічних настроїв, а також формування вигідного для агресора наративу на міжнародному рівні через іноземні ЗМІ та інформаційні майданчики, що широко охоплюють аудиторію.

У статті здійснено всебічний аналіз ключових викликів, що ускладнюють ефективну протидію інформаційній агресії росії. Виокремлено такі проблеми: високий рівень технологічної складності сучасних атак; відсутність сталої міжвідомчої координації між державними структурами; фрагментарність та неузгодженість законодавчого регулювання у сфері інформаційної безпеки; низький рівень критичного мислення та медіаграмотності населення; зовнішній контроль над глобальними цифровими платформами, що обмежує можливості оперативного реагування на загрози; політична вразливість процесів, пов'язаних із регулюванням інформаційної політики.

Проаналізовано еволюцію методів російського інформаційного впливу від поодиноких кібератак до системних багаторівневих інформаційно-психологічних операцій із використанням бот-мереж, соціальних медіа, проксі-ресурсів та контрольованих медіа. Розглянуто основні елементи української нормативно-правової бази у сфері інформаційної політики та безпеки (Кримінальний кодекс України, закони «Про інформацію», «Про медіа»), а також відповідні міжнародні акти – директиви Європейського Союзу, рекомендації Ради Європи, документи ОБСЄ.

На основі проведеного аналізу обґрунтовано необхідність комплексного підходу до протидії інформаційній агресії. Запропоновано низку практичних заходів: розвиток стратегічних комунікацій, підвищення рівня медіаграмотності населення, впровадження систем верифікації контенту, посилення цифрового суверенітету України та модернізація інституційної інфраструктури інформаційної безпеки з урахуванням новітніх технологічних викликів і загроз.

Ключові слова: інформаційна агресія, дезінформація, інформаційна безпека, фейкові новини, стратегічні комунікації, Україна, росія.

Petrenko S.V., Ilchenko Y.O. Critical aspects of countering russian information aggression.

In the context of hybrid warfare, information aggression has evolved into a powerful instrument of state influence, enabling the achievement of political, military, and social objectives without the direct

use of force. During the full-scale invasion of Ukraine by the russian federation, information pressure has reached an unprecedented scale, encompassing both the domestic and international information space. The primary goals of such actions include destabilizing Ukrainian society and government, undermining public trust in state institutions, discrediting the Armed Forces of Ukraine, spreading panic and uncertainty, and shaping a favorable narrative for the aggressor in the global media environment with wide audience reach.

This article presents a comprehensive analysis of the key challenges impeding effective resistance to russian information aggression. The most critical issues identified include: the technological complexity of modern information attacks; the lack of consistent interagency coordination among state institutions; fragmented and inconsistent legal regulation in the field of information security; a low level of critical thinking and media literacy among the population; external control over global digital platforms, which limits the ability to respond promptly to threats; and the political vulnerability of information policy regulation processes.

The paper examines the evolution of Russian information influence methods – from isolated cyberattacks to complex, multi-level information and psychological operations involving bot networks, social media platforms, proxy websites, and controlled media outlets. It also analyzes the main components of Ukraine's regulatory framework in the field of information policy and security (the Criminal Code of Ukraine, the Laws "On Information" and "On Media"), as well as relevant international legal instruments, including European Union directives, Council of Europe recommendations, and OSCE documents.

Based on this analysis, the study substantiates the need for a comprehensive approach to countering information aggression. The authors propose a set of practical measures, including the development of strategic communications, improvement of media literacy, implementation of content verification systems, strengthening of Ukraine's digital sovereignty, and modernization of institutional information security infrastructure in response to emerging technological challenges and threats.

Key words: information aggression, disinformation, information security, fake news, strategic communications, Ukraine, russia.

Постановка проблеми. У сучасних умовах повномасштабної збройної агресії російської федерації проти України особливого значення набуває інформаційна безпека держави. Російська інформаційна агресія стала потужним інструментом підривної діяльності російських спецслужб, метою якої є дестабілізація внутрішньополітичної ситуації, підрив довіри до українських інституцій, деморалізація суспільства та формування викривленої картини реальності як в Україні, так і за її межами. Масовані кампанії дезінформації, фейкові новини, маніпуляції в соціальних мережах і контрольованих медіа – усе це створює серйозні загрози національній безпеці держави.

Попри зусилля державних структур і громадянського суспільства, протидія російській інформаційній агресії залишається складним завданням через постійне оновлення методів інформаційного впливу, використання штучного інтелекту, бот-мереж і високотехнологічних платформ для поширення пропаганди. У зв'язку з цим постає необхідність комплексного аналізу наявних проблем у сфері інформаційної безпеки та вироблення ефективних механізмів протидії деструктивним впливам.

Мета дослідження полягає у всебічному аналізі основних проблем та викликів, пов'язаних із протидією російській інформаційній агресії, визначенні її основних форм і методів, а також у розробці напрямів щодо вдосконалення національної системи інформаційної безпеки України. Особливу увагу приділено виявленню вразливих місць у вітчизняному інформаційному середовищі, оцінці ефективності чинних механізмів реагування та обґрунтуванню напрямів посилення інформаційного спротиву в умовах повномасштабного вторгнення.

Стан опрацювання проблематики. У сучасному науковому дискурсі питання протидії російській інформаційній агресії набули особливої уваги у зв'язку з російською агресією проти України. Так, Гурковський В. аналізує основні методи інформаційного впливу, включно з маніпулятивними повідомленнями, фейками та цілеспрямованими кампаніями дезінформації, що формують хибні уявлення у масовій свідомості та дестабілізують суспільство [1].

У статті Гребенюка М. та Леонова Б.Д. розглянуто досвід країн Європейського Союзу у сфері боротьби з деструктивною пропагандою в період виборчих кампаній. Автори підкреслюють значення правового регулювання та важливість проактивних інформаційних стратегій, що можуть бути адаптовані до українських реалій [2].

Коруц У. акцентує увагу на правових механізмах протидії інформаційній війні, трактуючи її як складову пропаганди війни. У дослідженні наведено ключові аспекти міжнародного гуманітарного та інформаційного права, що регламентують допустимі межі інформаційного впливу у період конфліктів [3].

Малик І. у своїй статті розглядає механізми протидії інформаційній пропаганді на державному та громадському рівнях. Авторка пропонує підходи до підвищення інформаційної стійкості суспільства, зокрема через освіту, медіаграмотність та розвиток критичного мислення [4].

Окрему увагу інституційному виміру протидії інформаційній агресії приділяє Панченко О.В своїй роботі автор аналізує діяльність національних і міжнародних інституцій, таких як Ради національної безпеки, центри стратегічних комунікацій, регуляторні органи ЄС та НАТО, наголошуючи на необхідності консолідації зусиль для нейтралізації пропагандистського впливу рф [5].

Виклад основного матеріалу. Починаючи з 2014 року, коли рф розпочала агресивні дії проти України, інформаційна війна стала одним із ключових інструментів у реалізації її повномасштабного вторгнення. Основною метою таких дій є систематичний підрив довіри до державних інституцій України, розхитування внутрішньополітичної стабільності та формування негативного іміджу України на міжнародній арені.

Росія активно використовує широкий арсенал засобів інформаційного впливу: поширення фейків і маніпулятивних наративів у соціальних мережах, кампанії з дезінформації, підтримку прокремлівських медіаресурсів, діяльність бот-мереж і тролів для нав'язування антиукраїнських поглядів. Паралельно з цим ведеться цілеспрямована робота з підтримки проросійських груп всередині країни з метою створення соціальної напруги.

Значну роль у структурі інформаційної агресії відіграють кібератаки, які з 2014 року еволюціонували від прямого знищення даних до складних кампаній з витоку конфіденційної інформації, що може використовуватись як інструмент політичного та економічного тиску. Серед сучасних тактик – фішинг, соціальна інженерія, впровадження шпигунського ПЗ та атаки на канали постачання. Особливу загрозу становлять атаки на критичну інфраструктуру – енергетичну, банківську, інформаційну та урядову [6, с. 83].

Однією з небезпечних тенденцій є поступова зміна пріоритетів із короткотермінового порушення роботи систем до реалізації довготривалих стратегічних операцій, спрямованих на створення хаосу, поширення паніки та послаблення обороноздатності держави через інформаційний вплив.

Україна опинилася в умовах багаторівневої інформаційної агресії, яка вимагає не лише реагування на окремі інциденти, а й формування стійкої системи кібер- та інформаційної безпеки з урахуванням новітніх форм атак і інформаційного впливу [6, с. 83].

Протидія інформаційній агресії рф є надзвичайно складним і багатоаспектним завданням, яке охоплює не лише безпековий, а й соціально-політичний, правовий, гуманітарний і технологічний виміри. Водночас в українському контексті актуалізується низка системних проблем, які суттєво ускладнюють ефективну протидію цьому явищу.

Однією з найсерйозніших проблем у сфері протидії російській інформаційній агресії є високий рівень адаптивності та технологічної складності ворожих інформаційних атак. Рф активно впроваджує сучасні технології, зокрема штучний інтелект, машинне навчання, нейромережі для створення deepfake-контенту, а також методи соціальної інженерії, які дозволяють маніпулювати емоційним станом людей, підривати їхню довіру до офіційних джерел інформації та формувати альтернативну, викривлену картину реальності. Особливо небезпечним є поширення дезінформації через бот-мережі, фейкові акаунти в соціальних мережах, підконтрольні ЗМІ, Telegram-канали та YouTube-платформи. Наприклад, у 2022–2024 роках зафіксовано масштабні інформаційні кампанії, спрямовані на дискредитацію Збройних Сил України, штучне нагнітання панічних настроїв серед населення під час масованих обстрілів енергетичної інфраструктури та формування ворожого ставлення до міжнародних партнерів України. Складність таких атак полягає не лише в їхньому обсязі, а й у високому рівні персоналізації – багато повідомлень цілеспрямовано адаптуються під конкретні аудиторії за географією, віком, політичними поглядами, що ускладнює їх нейтралізацію традиційними засобами.

Ще однією критичною проблемою є недостатній рівень координації між державними структурами, відповідальними за захист інформаційного простору. На сьогодні в Україні немає централізованого міжвідомчого органу або національного центру стратегічних комунікацій, який би здійс-

нював оперативне управління процесом виявлення, аналізу та протидії інформаційним загрозам. Відповідні повноваження частково розподілені між Міністерством оборони, Службою безпеки України, Центром протидії дезінформації при РНБО, Національною поліцією, Держспецзв'язку, Міністерством культури та інформаційної політики, однак відсутність чіткої ієрархії, уніфікованих протоколів обміну інформацією та швидкої координації дій призводить до дублювання функцій, затримок у реагуванні та зниження загальної ефективності інформаційного захисту. Наприклад, у випадках масштабних кібератак на державні сайти в січні 2022 року (напередодні повномасштабного вторгнення рф) було виявлено, що реагування різних інституцій відбувалося паралельно, без належної взаємодії, що призвело до затримок у відновленні ресурсів і публічному інформуванні громадян.

Окремою проблемою виступають обмежені можливості правового регулювання у сфері протидії дезінформації. Хоча українське законодавство містить окремі положення, які можуть бути використані для реагування на поширення фейкових новин, нормативна база залишається фрагментарною й не повністю адаптованою до реалій сучасного інформаційного середовища. Значна частина дезінформаційної діяльності відбувається в цифровому просторі, що створює труднощі для застосування традиційних юридичних норм. Крім того, спроби ухвалення закону про дезінформацію (як-от законопроєкт 2020 року, запропонований Міністерством культури) викликали значну суспільну і професійну критику через побоювання щодо обмеження свободи слова, цензури та надмірної концентрації повноважень в одному органі. Водночас відсутність чітко окреслених правових механізмів і критеріїв оцінки достовірності інформації створює прогалини, які використовують ворожі інформаційні структури. Залишається неврегульованим також питання відповідальності глобальних цифрових платформ (Meta, Google, Telegram тощо), через які активно поширюється деструктивний контент, що ускладнює міжнародну співпрацю в сфері інформаційної безпеки. Також, така платформа як Telegram широко використовується спеціальними спецслужбами рф для віддаленого вербування українських громадян та зв'язку зі своєю агентурою.

Серйозним бар'єром на шляху до ефективної протидії дезінформації в Україні залишається низький рівень медіаграмотності серед широких верств населення. Значна частина громадян не володіє достатніми навичками критичного осмислення інформації, не вміє розрізняти достовірні джерела від маніпулятивних, а отже – легко піддається впливу інформаційних кампаній, спрямованих на формування хибної картини дійсності. Це особливо небезпечно в умовах воєнного часу, коли поширення панічних настроїв, викривлених повідомлень про ситуацію на фронті, обстріли або економічні труднощі може мати деструктивний ефект. Наприклад, упродовж 2023–2024 років було зафіксовано численні випадки поширення фейкових новин про «зраду» українського командування, «здачу» міст чи перебої в постачанні гуманітарної допомоги, які викликали суспільну напругу, але виявилися дезінформацією. Відсутність системного підходу до навчання медіаграмотності в загальноосвітніх закладах, університетах та для дорослого населення лише посилює вразливість до подібного впливу.

Не менш суттєвою проблемою залишається недосконалість інфраструктури інформаційної безпеки. Україна поки що не має повноцінної, технічно оснащеної системи, яка б забезпечувала оперативний моніторинг, аналіз і нейтралізацію інформаційних загроз. У багатьох державних установах відсутні алгоритми кризової комунікації, системи попередження фейкових кампаній, а інструменти кіберзахисту не завжди відповідають рівню загроз, що постійно зростає. На цьому тлі виникають затримки у реагуванні на інформаційні атаки, а також складнощі в комунікації з громадськістю під час інформаційних інцидентів. У 2023 році низка атак на урядові сайти та платформи електронних послуг засвідчила, що Україна потребує масштабної модернізації у сфері цифрової безпеки та створення єдиної системи стратегічних комунікацій на базі сучасних технологій та аналітики.

Окрему загрозу становить вплив глобальних цифрових платформ, через які реалізується більшість інформаційних атак. Багато пропагандистських наративів поширюється через такі ресурси, як Facebook, YouTube, Telegram, TikTok, які перебувають поза межами прямої дії українського законодавства. Це створює серйозні труднощі в питанні контролю, блокування або обмеження доступу до шкідливого контенту. Наприклад, Telegram, який активно використовується як канал поширення фейкових новин та деструктивних повідомлень, зберігає значну автономію і слабко реагує на звернення українських органів щодо видалення ворожого контенту. Відсутність чітких міжнародних механізмів співпраці з платформами або обмеженість їх дії в Україні зумов-

лює фрагментарність впливу на цифрове середовище. Це унеможливлює ефективне припинення трансляції ворожої інформації або просування пропагандистських меседжів за межами державної юрисдикції.

Крім того, значною перешкодою у формуванні дієвої політики протидії інформаційній агресії є інституційна вразливість та політизація боротьби з дезінформацією. У багатьох випадках заходи щодо протидії фейкам та інформаційним атакам сприймаються суспільством не як питання безпеки, а як інструмент внутрішньої політичної боротьби. Це знижує довіру громадян до офіційних ініціатив і може сприяти зростанню пасивного або навіть вороже налаштованого ставлення до заходів держави у сфері інформаційної безпеки. Наприклад, під час суспільних обговорень законопроєкту щодо протидії дезінформації в 2020 році низка експертів та журналістів висловила побоювання, що державна боротьба з фейками може перетворитися на цензуру і переслідування опозиційних медіа. У такій ситуації навіть об'єктивно необхідні кроки, спрямовані на захист інформаційного простору, можуть отримати негативну оцінку з боку суспільства. Це, у свою чергу, послаблює політичну волю до ухвалення важливих рішень у сфері кібер– та інформаційної безпеки.

У відповідь на ці виклики в Україні активізувалася розробка нормативно-правових інструментів для протидії поширенню інформаційної агресії.

Ключові положення щодо регулювання та обмеження інформаційних загроз викладені в Законі України «Про інформацію» [7], який визначає правові засади доступу до достовірної інформації, передбачає захист від поширення неправдивих відомостей, що можуть загрожувати громадському порядку, безпеці та правам громадян. Особливу увагу приділено забезпеченню права суспільства на правдиву інформацію та обмеженню маніпулятивних інформаційних впливів.

Положення Кримінального кодексу України також можуть застосовуватися для кваліфікації інформаційних злочинів, зокрема поширення свідомо неправдивих відомостей, що спричиняють паніку, дестабілізують ситуацію або створюють загрозу громадській безпеці. Наприклад, стаття 259 КК України передбачає відповідальність за завідомо неправдиве повідомлення про загрозу безпеці громадян, що часто використовується в межах дезінформаційних кампаній [8].

Суттєвий крок у напрямку оновлення правового поля був зроблений з ухваленням Закону України «Про медіа» у 2023 році [9]. Цей закон регулює відповідальність медіа та онлайн-платформ за поширення інформації, що може нести загрозу національній безпеці, а також зобов'язує власників цифрових ресурсів здійснювати контроль за контентом, що має ознаки дезінформації.

Міжнародна практика також слугує орієнтиром для формування ефективної політики протидії інформаційній агресії. Зокрема, Міжнародний пакт про громадянські та політичні права (1966 р.) у статті 19 визначає право на свободу висловлювання, але допускає обмеження в інтересах національної безпеки та захисту громадського порядку, що може бути застосоване в контексті боротьби з дезінформацією [10].

Рада Європи у своїй Рекомендації 2018 року щодо впливу фейкових новин на демократичні процеси закликала держави забезпечити баланс між свободою слова і необхідністю захисту демократичних інституцій від інформаційних атак, зокрема шляхом впровадження прозорих стандартів відповідальності.

Важливим кроком на рівні ЄС стало ухвалення Директиви про аудіовізуальні медіа-послуги [11], яка покладає на цифрові платформи відповідальність за контент, що може становити загрозу правам людини або національній безпеці, включно з фейковими новинами, що активно використовуються РФ як інструмент впливу.

НАТО, ОБСЄ та інші міжнародні організації виступають активними учасниками у сфері протидії інформаційним загрозам. Їхня діяльність охоплює як технічний моніторинг інформаційних потоків, так і напрацювання рекомендацій для національних урядів щодо ефективної побудови системи інформаційної безпеки.

У сукупності, національні й міжнародні нормативні документи формують базу для послідовної та правомірної протидії інформаційній агресії рф, проте потребують подальшого вдосконалення у відповідь на динамічний розвиток дезінформаційних технологій.

Висновки. Російська інформаційна агресія становить системну й багатоаспектну загрозу національній безпеці України, особливо в умовах військової агресії. Проведене дослідження дозволяє стверджувати, що попри активізацію зусиль держави у сфері інформаційної безпеки, залишається низка критичних проблем, які ускладнюють ефективну протидію ворожому впливу. До них, зо-

крема, належать: технологічна складність сучасних інформаційних атак, недостатня координація між державними інституціями, фрагментарність правового регулювання, низький рівень медіаграмотності населення, вразливість інфраструктури інформаційної безпеки, зовнішній контроль над інформаційними платформами та політизація процесів протидії дезінформації.

Загрози, які формуються в інформаційному просторі, не лише шкодять іміджу держави, а й прямо впливають на морально-психологічний стан суспільства, підривають довіру до державних інституцій, спричиняють соціальну напругу та політичну нестабільність. У цьому контексті ефективна протидія інформаційній агресії повинна бути не точковою, а системною, з опорою на міжгалузеву координацію, високий рівень аналітичної спроможності та активну участь громадянського суспільства.

Вирішення окреслених проблем потребує оновлення національного законодавства з урахуванням європейських підходів, створення єдиного центру стратегічних комунікацій, активізації міжнародної співпраці з цифровими платформами, масштабної програми підвищення медіаграмотності, а також модернізації системи моніторингу, виявлення і нейтралізації інформаційних загроз. Лише за умови впровадження комплексного підходу можливо досягти належного рівня інформаційної безпеки, зберегти стійкість та забезпечити ефективну оборону в інформаційному просторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Гурковський В. Механізми використання дезінформації в умовах російської гібридної агресії. *Освіта регіону.* URL: http://social-science.com.ua/article/1393 (дата звернення 22.07.2025).
2. Гребенюк М.В., Леонов Б.Д. Проблеми протидії поширенню деструктивної пропаганди та дезінформації напередодні виборів: аналіз досвіду ЄС. *Правова інформатика*. № 2(29)/2019. С. 82–89.
3. Коруц У. Інформаційна війна як інструмент пропаганди війни: правові підстави протидії. *Підприємництво, господарство і право.* 2020. № 8. С. 334–339.
4. Малик І. Механізми протидії негативним впливам інформаційної пропаганди. *Humanitarian vision*. 2015. Vol. 1. Num. 2. С. 47–54. URL: http://nbuv.gov.ua/UJRN/ hv_2015_1_2_10 (дата звернення 22.07.2025).
5. Панченко О.А. Інституційне забезпечення процесів протидії російській інформаційній експансії та пропаганді в сучасному світі. *Інформація і право.* Вип. 3. 2021. С. 28–34. URL: http://il.ippi.org.ua/article/download/243797/241769 (дата звернення 22.07.2025).
6. Галіпчак В.Д. Безпека інформаційного простору України в умовах російської агресії на сучасному етапі: основні завдання та виклики. *Регіональні студії.* Вип. 34. 2023. С. 81–85. URL: http://regionalstudies.uzhnu.uz.ua/archive/34/13.pdf (дата звернення 22.07.2025).
7. Про інформацію: Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 22.07.2025).
8. Кримінальний кодекс України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України. 2*001. № 25-26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 12.07.2025).
9. Про медіа: Закон України від 13.01.2023 № 2849-IX. Відомості Верховної Ради України. 2023. № 10. Ст. 70. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення 22.07.2025).
10. Міжнародний пакт про громадянські та політичні права від 16.12.1966. *Офіційний вісник України*. 1994. № 12. Ст. 38.
11. Рекомендації Ради Європи щодо впливу рейкових новин на демократичні процеси. Страсбург: Рада Європи. 2018. 25 с.