

8. Spalding, R. (2019). *Stealth War: How China Took Over While America's Elite Slept*, *Portfolio*, 256 p. (in English).

9. There are 548 "Confucius" Institutes in the world. *Telegraph*. URL: <https://telegraph.com/en/there-are-548-Confucius-Institutes-in-the-world/> (in English).

Матеріал надійшов до редакції 17.06.2025 р.

УДК 355.01:316.776.23]:355.48(477:470)"2014..."

Борис Роговий,

аспірант факультету міжнародних відносин спеціальності
291Міжнародні відносини, суспільні комунікації та регіональні студії,
Волинський національний університет імені Лесі Українки,
Rohovyi.Borys@vnu.edu.ua,
ORCID ID: 0009-0003-1560-9900,
DOI 10.29038/2524-2679-2025-02-106-121

ІНФОРМАЦІЙНІ ЗАГРОЗИ ТА ВЕКТОРИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ ПІД ЧАС РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Досліджено сучасні загрози для медіа та інформаційних систем, тенденції розвитку методів ведення інформаційних воєн у контексті російсько-української війни ХХІ ст. Детально розглянуто історію розвитку процесу інформаційно-психологічних операцій російської федерації проти України, ресурсну базу та інституції, задіяні в реалізації деструктивних інформаційних впливів. Описано методологію ведення інформаційних операцій, їх особливості й характерні риси в період із початку 2014 року до 2022 р. Проаналізовано загрози й виклики, пов'язані зі стрімким розвитком технологій штучного інтелекту, та досліджено методи застосування ШІ в інформаційних операціях деструктивного характеру. Описано шляхи використання російською федерацією технологій штучного генерування зображень, аудіо-, відео- й тестового матеріалу для здійснення інформаційно-психологічних атак перед і під час повномасштабного вторгнення росії до України. Доведено, що інтенсивність і складність деструктивних

впливів, направлених на дискредитацію України, значно зросли після початку вторгнення 2022 р. Деталізовано потенційні шляхи розвитку таких впливів у подальшому з метою посилення інформаційного тиску на Україну та міжнародне товариство зі сторони рф. Визначено, що одним із ключових загроз і викликів для інформаційного простору України є низька медіаграмотність населення. Досліджено дії держави, спрямовані на покращення обізнаності суспільства, запропоновано можливі покращення нормативної й інституційної бази.

Уточнено нормативно-правову базу українського законодавства для стратегічного захисту інформаційних систем і шлях її розвитку за останнє десятиліття. Запропоновано перспективні зміни в нормотворчій базі України для всеосяжної та детальної розробки стратегії захисту вітчизняних інформаційних, медіа та соціальних мереж. Розкрито необхідність термінового створення ефективних механізмів захисту шляхом використання наявних правоохоронних органів й інституцій для оперативного реагування на новітні інформаційні загрози зі сторони російської федерації. З'ясовано критичну необхідність подальшого вдосконалення вітчизняної системи захисту інформаційних мереж від деструктивних впливів, шляхом покращення внутрішньої, національної складової частини та співпраці з міжнародними партнерами. Мета статті – дослідити сучасні тенденції розвитку інформаційних загроз і векторів розвитку відповідних систем безпеки та методів захисту від деструктивних впливів, які можуть бути запозичені й використані для створення ефективної моделі захисту від ворожих, деструктивних впливів.

Ключові слова: деструктивний вплив, штучний інтелект, ЗМІ, медіа та інформаційні системи, пропаганда, державна політика.

Borys Rohovyi,

Lesya Ukrainka Volyn National University,

ORCID ID: 0009-0003-1560-9900

INFORMATION THREATS AND VECTORS FOR PROTECTING UKRAINE'S INFORMATION SPACE DURING THE RUSSO-UKRAINIAN WAR

The study explores contemporary threats to media and information systems, trends in the development of methods of conducting information warfare in the context of the 21st-century Russian-Ukrainian war. The history of the development of information and psychological operations conducted by the Russian Federation against Ukraine, including the resource base and institutions involved in implementing destructive information influences, is examined in detail. The

methodology of conducting information operations, their peculiarities, and distinguishing features during the period of the Russian-Ukrainian military confrontation are described.

The threats and challenges posed by the rapid development of artificial intelligence (AI) technology are analyzed, and methods of using AI in destructive information operations are explored. The study describes how the Russian Federation employs technologies for generating synthetic images, audio, video, and textual content to conduct information and psychological attacks both prior to and during its full-scale invasion of Ukraine. It is proven that the intensity and complexity of destructive influences aimed at discrediting Ukraine significantly increased after the invasion began in 2022. Potential future developments in such influences, aimed at intensifying informational pressure on Ukraine and the international community from the Russian Federation, are detailed.

It is established that one of the key threats and challenges for Ukraine's information space is the population's low level of media literacy. The actions of the state aimed at raising public awareness are analyzed, and possible improvements to the regulatory and institutional framework are proposed. The study clarifies the legal framework of Ukrainian legislation for the strategic protection of information systems and outlines its development trajectory over the past decade.

Prospective changes to Ukraine's regulatory framework are suggested for the comprehensive and detailed development of a strategy to protect national information, media, and social networks. The necessity of urgently creating effective protection mechanisms through the use of existing law enforcement agencies and institutions for rapid response to new information threats from the Russian Federation is emphasized. The critical need to further improve the domestic system for protecting information networks from destructive influences is identified, focusing on enhancing the national component and fostering cooperation with international partners. The article aims to investigate modern trends in the development of information threats and vectors for improving security systems and protection methods against destructive influences. These findings can be used to develop an effective model for countering hostile and destructive actions.

Key words: destructive influence, artificial intelligence, media, information systems, propaganda, state policy.

1. ВСТУП

Постановка проблеми. Інститут медіа та інформаційних систем є доволі критичним і водночас чутливим аспектом державної політики безпеки й складовою частиною доволі розгалуженого комплексу нормативно-правових актів, органів та організацій, покликаних контролювати здійснення охорони суверенітету тієї чи іншої країни в сучасних умовах

інформаційного протистояння й постійно зростаючих загроз, які надходять з інформаційних, медіа та соціальних мереж. Протягом останніх десяти років кількість і технологічність деструктивних впливів на інформаційні мережі й медіа зросли не лише в обсязі, а й кардинально змінили якість. У тому ж числі й розвиток технології штучного інтелекту, який дає змогу спотворювати інформаційні матеріали на рівні з реальними фото, відео- й аудіоматеріалами. Особливо загострилася ситуація з початком повномасштабного вторгнення російської федерації в Україну в лютому 2022 р. й одночасним колосальним збільшенням кількості дезінформації, агресивної пропаганди та всіх можливих деструктивних, інформаційних впливів проти України й країн НАТО, і так званого «колективного Заходу» загалом. Сьогодні проблематика полягає в надзвичайній турбулентності подій та потребі державного апарату й регулювання мати можливість не відставати від новітніх тенденцій у боротьбі з деструктивними впливами задля забезпечення стабільності та інформаційного поля, суверенітету й національних інтересів.

Для України це питання є найбільш гострим, зважаючи на дуже складну геополітичну та військову ситуацію, спричинену вторгненням росії, що супроводжується колосальними атаками на всі інформаційні, соціальні й медіамережі. Отож ще з 2014 р. Україна стала наріжним каменем для російської машини пропаганди та дезінформації, спрямованої насамперед на західну аудиторію. До того ж в Україні сьогодні, попри активний розвиток законодавчої й інституційної бази, досі не існує ефективного механізму захисту вітчизняних інформаційних систем від деструктивних впливів, інформаційно-психологічних операцій (далі – ІПСО) і нових методів пропаганди, що постійно вдосконалюються. Тому дослідження дій держави під дією постійних деструктивних впливів сприяло б визначенню слабких місць, що потребують покращення з метою ефективної протидії, насамперед російській, інформаційній війні проти України, що на сьогодні є надзвичайно актуальним.

Аналіз досліджень та публікацій. Теоретико-методологічний концепт теми дослідження становлять такі категорії, як «безпека медіа та інформаційних систем», «деструктивні впливи», «інформаційне протистояння», «російсько-українська війна».

Посилаючись на визначення М. Гаврильців у праці «Інформаційна безпека держави в системі національної безпеки України», у статті трактуватимемо поняття «безпека медіа та інформаційних систем» як стан захищеності важливих інтересів держави й суспільства, за якого забезпечується якісне інформування, доступ до джерел інформації, захист від дезінформації та деструктивних впливів, кіберзагроз [1].

«Деструктивні впливи» детально розглянули в колективній монографії науковці ВНУ ім. Лесі Українки «Стратегічні комунікації ЄС: протидія деструктивним впливам», визначили їх як цілеспрямовані дії, спрямовані на дестабілізацію, підривно діяльність, маніпуляцію суспільною думкою за допомогою дезінформації, пропаганди та емоційно забарвленої інформації для тиску на суспільство, державу, групу осіб для досягнення політичних чи військових цілей [2].

«Інформаційне протистояння» у нашому дослідженні розуміємо як маніпулювання інформацією, що провокує порушення цілісності суспільства, його стабільного, зокрема емоційного стану, підлив цілей, поглядів і світогляду соціуму, а також розпалювання конфліктів (міжособистісних, етнічних, міжнародних). Таке визначення можемо сформулювати зі статті Христини Максим. «Феномен інформаційної агресії в умовах повномасштабної війни Росії проти України» [3].

«Російсько-українська війна» має такі хронологічні рамки: 2014–2025 рр. – початок пов'язаний із 2014 р., коли російська федерація розпочала агресію проти України, незаконно анексувавши Крим і підтримуючи збройні формування на сході України, що спричинило початок війни на Донбасі. У 2022 р. РФ здійснила повномасштабне вторгнення, намагаючись захопити ключові території України, включаючи Київ, і використовуючи масовані ракетні удари по цивільних об'єктах. Обидва етапи агресії супроводжуються воєнними злочинами, пропагандою та грубими порушеннями міжнародного права, друга дата – теперішній час.

Українські дослідники сфери інформаційних впливів, пропаганди й деструктивних впливів доволі детально вивчають елементи цього напрямку. Особливу увагу приділяють російсько-українській інформаційній війні. Для розуміння варто навести декілька прикладів вітчизняних досліджень. Детальний аналіз інструментарію російської інформаційної машини, опис методів ведення пропаганди шляхом поширення неправдивої інформації серед населення за допомогою «інтернет-ресурсів і порталів виконано в статті Б. Іваницької та С. Гусєвої «Основні методи пропаганди в російському інтернет-змі Pravda.ru» [4]. Проаналізовано та розкрито основні етапи проведення інформаційної пропаганди, охарактеризовано процеси й черговість здійснення тих чи інших операцій і надано рекомендації для запобігання деструктивним впливам у статті І. Малик «Механізми протидії негативним впливам інформаційної пропаганди» [5].

Деталізовано результати впливу на суспільну думку та обізнаність населення шляхом здійснення інформаційного-деструктивного тиску на медіа й соціальне поле країни, наведено приклади зміни суспільно-

політичної свідомості громадян під час інформаційної війни та механізми впливу ЗМІ на громадську думку в посібнику В. Хорошко й Ю. Хохлачової «Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство» [6].

Також досліджено вразливі місця української інформаційної системи та населення до дезінформації й деструктивних впливів, описано проблеми інституційної неготовності протистояти проросійським наративам і пропаганді та надано пропозиції щодо підвищення рівня обізнаності суспільства й процесів, які допоможуть у покращенні медіаграмотності, у статті Н. Еляшевської «Вразливість України до інформаційної війни» [7].

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Інформаційна війна, як зазначає І. Фещенко в статті «Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту», – це засіб пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях із метою послаблення матеріальних і моральних сил, ресурсів супротивника та посилення власних [8]. Цей вид протистояння включає пропаганду, дезінформацію, деструктивні впливи, інформаційно-психологічні операції, створення негативного інформаційного іміджу України на міжнародній арені й інші заходи агресивного характеру.

У літературі існує безліч класифікацій інформаційних війн, проте особливу увагу потрібно приділити класифікації М. Лібіцького [9]. Він виокремлює такі форми інформаційної війни:

- управлінська війна – це форма інформаційної війни, яка спрямована на вплив на системи управління супротивника через інформаційні або технічні методи. Її мета – порушення або дезорганізація процесів прийняття рішень та координації дій у ворожій системі;
- розвідувальна війна – це інформаційна діяльність, спрямована на збір даних про супротивника для подальшого їх використання в стратегічному плануванні й операціях. Вона включає використання розвідувальних технологій для створення «картини» поля бою та виявлення слабких місць противника;
- радіоелектронна боротьба – це застосування електромагнітної енергії для впливу на засоби зв'язку, озброєння й бойові системи противника. Вона також уключає радіоелектронний захист власних систем і перешкоджання використанню супротивником електронних засобів;
- психологічна війна – це діяльність, спрямована на вплив на емоції, мотиви та поведінку супротивника за допомогою вибраної інформації. Її

мета – деморалізація супротивника, маніпуляція громадською думкою й зниження ефективності його дій;

- хакерська війна – це форма інформаційної війни, яка використовує атаки на комп'ютерні системи для порушення їхньої роботи або отримання доступу до інформації. Основна мета – зламати, змінити чи знищити інформацію на вебресурсах супротивника;

- економіко-інформаційна війна – це конфлікт, у якому інформація про економічні процеси, компанії або ресурси застосовується для послаблення економічного потенціалу супротивника. Часто включає економічне шпигунство та використання конфіденційної інформації для досягнення конкурентних переваг;

- кібервійна – це застосування наступальних й оборонних заходів у кіберпросторі для знищення або зламу інформаційно-комунікаційних систем противника. Її мета – порушити критичну інфраструктуру, створити хаос або отримати стратегічну перевагу.

Ці форми тісно взаємопов'язані та часто застосовуються в комплексі, наприклад, для досягнення ширших цілей інформаційної війни супроводжуються кібервійною, психологічною війною, а також використанням радіоелектронної боротьби й мережевих технологій.

У період 2014–2022 рр. кількість так званих інформаційно-психологічних операцій (ІПСО), спрямованих на дестабілізацію України, розхитування суспільства та розпалювання ворожнечі, збільшилась у геометричній прогресії. Можна також натрапити на доволі доцільну думку, що процес був повністю запущений після «Мюнхенської промови» у 2007 р., де президент росії в. путін проголосив промову, яка вказувала на початок нової «холодної війни» [10]. Зокрема, тези про «неприйнятність однополярного світу», «тисячолітню історію росії», «недопустимість розширення НАТО». Для цього дослідження такі твердження є важливими, оскільки вказують на черговий поділ світу, який спонукав більшість країн здійснити вибір між двома політичними блоками чи таборами – західним й, відповідно, східним. Україна внаслідок цього вибору на користь демократичного «західного» курсу розвитку зіткнулась із колосальною інформаційною, а згодом і військовою агресією проти української незалежності та суверенітету зі сторони російської федерації і її союзників.

Апарат та інструментарій, яким послуговується російський режим у веденні інформаційної війни, є досить широким. Проаналізуємо декілька напрямів: використання засобів масової інформації для поширення дезінформації, створення хибного уявлення про стан речей щодо тієї чи іншої ситуації. До цього ж інструменту можна віднести інформаційні

впливи декількох видів. Як зазначають В. Хорошко та Ю. Хохлачова, ці впливи можуть бути декількох видів: «білий», тобто зі сторони офіційного джерела, уряду чи організації; «сірий» – такий, що просуває певні наративи через неурядові засоби поширення інформації та «чорний» – це поширення абсолютно вигаданої, неправдивої інформації, котра надходить від третіх осіб [6].

Серед напрямів – використання заяв офіційних осіб, організацій чи установ задля маніпулювання суспільною думкою; створення уявлення про чіткий та цілеспрямований намір до певної дії. Чудовим прикладом може слугувати заява президента російської федерації перед початком повномасштабного вторгнення для створення картини невідворотності події, усеосяжності та неспроможності України протистояти. [11].

Використання соціальних мереж для поширення фейків, неправдивої інформації й пропаганди на всіх рівнях – від викривлення заяв офіційних осіб України до поширення дезінформації про стан оборони та українську армію. Прикладом застосування такого інструменту є навала російських ботоферм у колишній мережі «Twitter» (наразі «X»). Десятки тисяч підставних акаунтів поширювали дезінформацію про «нацизм» в Україні; видавали російські воєнні злочини такими, які здійснені українською армією, просували наратив зупинки підтримки України в коментарях у статтях великих інтернет-видань. 10 липня 2024 р. департамент юстиції США викрив і зупинив роботу російської ботоферми, яка провадила діяльність на території США та за кордоном, основними завданнями якої були дискредитація України й насадження переконань про припинення підтримки України та нелегітимність українського суверенітету. За даними департаменту юстиції США, кількість активних ботів становила близько десяти тисяч [12].

Штучний інтелект – це останній у списку технологічних інновацій інформаційних інструментів деструктивних впливів, але не останній за важливістю, а можливо й перший. Ця нова технологія є дуже небезпечною у світі інформаційної війни. Вона дає змогу в максимально короткий термін створювати реалістичні відео-, аудіо- та графічні матеріали для дезінформації. Є низка прикладів, коли згенеровано звернення Президента України В. Зеленського, у якому він нібито оголошує капітуляцію, звернення колишнього Головнокомандувача ЗСУ В. Залужного із закликами до української армії здаватись у полон [13]. Звісно, абсурдність цих матеріалів відразу дала змогу їх спростувати, проте динамічний розвиток технології ШІ створює матеріали, які все складніше відрізнити від реальної, правдивої, істинної інформації [14].

Як приклад постійності та сили російських ІІСО, пропаганди варто згадати катастрофу з малайзійським авіалайнером МН-17 17 липня 2014 р. Попри існування розслідувань різних країн й організацій, а також рішення Міжнародного кримінального суду, росія продовжує постійно поширювати різні наративи про свою непричетність до катастрофи [15, 16]. Тобто понад 10 років постійної, безперервної брехні та дезінформації. Потрібно визнати, що кількість зусиль і постійність цих ІІСО ставить росію чи не на перше місце в рейтингу країн із потужним, впливовим та розвинутим апаратом, спрямованим на ІІСО, деструктивні впливи й пропаганду.

Для розуміння прогресії сил і ресурсів, яких докладає росія для розвитку «машини пропаганди», можемо навести статистику Національного проєкту медіаграмотності Міністерства культури «Фільтр» про витрати рф на пропаганду для формування негативного образу України. Агресивність і масовість інформаційних атак не є чимось новим, що з'явилося із початком повномасштабного вторгнення. Наприклад, у 2020 р. в бюджеті рф було передбачено 1,3 млрд євро для фінансування державних пропагандистських ЗМІ [17]. На 2023 р. у держбюджеті закладено 1,6 млрд доларів США. Тож можемо чітко зрозуміти масштаби докладених зусиль, ресурсів та можливостей, які рф використовує лише для пропаганди проти України на державному рівні.

Як Україна реагує на ці постійні атаки та нові загрози? Оскільки посправжньому екзистенційність проблеми усвідомлена лише з початком повномасштабного вторгнення, імпульс до розвитку система інформаційної безпеки України отримала лише у 2022 р. Звісно, не можна забувати про фундаментальні зміни, які відбулись у 2014 р., а саме низку нормативно-правових змін, направлених на визначення й розробку нових механізмів інформаційної безпеки. Зокрема, це рішення РНБО «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 р., Закон України «Про інформацію» [18, 19]. Ці два нормативно-правових акти (далі – НПА) регулювали ключові визначення щодо інформації, її поділ та рівні захисту, доступу до неї. Не лише ці два НПА створено з початком російської агресії 14-го року, проте вони були одними з ключових у подальшому розвитку.

Наступним важливим етапом можна вважати прийняття «Стратегії інформаційної безпеки» України від 28 грудня 2021 р. [20]. Це був важливий ступінь розвитку інформаційної безпеки. Розроблено інформаційні заходи оборони держави та визначено суб'єкти національної безпеки в цій сфері. Цей етап також визначав комплекси заходів щодо урядових, антикризових, стратегічних комунікацій, де зазначалася необхідність проводити діалог із суспільством щодо можливих загроз зі сторони ворожих наративів і

деструктивних інформаційних впливів. Саме цей документ визначив на законодавчому рівні загрозу, яка надходить саме від російської федерації та необхідність інформаційного протистояння їй. Було надзвичайно важливо чітко вказати на головне джерело інформаційних загроз не лише для України, а й для решти демократичного світу. Окремої уваги заслуговує визнання недоліків і слабких місць в інформаційній обороноздатності, як-от недостатній рівень медіаграмотності населення, оскільки усвідомлення проблеми – це перший етап на шляху її розв’язання. Звісно, стратегія не була позбавлена недоліків. Документ визначає соціальні мережі, як нове джерело небезпечних впливів, проте не надає докладного опису заходів чи стратегії дій держави в напрямі реагування на ці загрози.

Окремо зауважимо про відсутність згадок про регуляцію та будь-яку стратегію дій у напрямі штучного інтелекту. Єдина спроба держави почати роботу із ШІ – це «Дорожня карта» з регулювання штучного інтелекту, яка презентована 7 жовтня 2023 р. Міністерством цифрової трансформації України. Вона передбачає майбутні заходи з регуляції сфери ШІ, оцінку ризиків та процедуру ознайомлення населення з можливостями й загрозами, що їх становить технологія штучного інтелекту [21]. Проте досі цей процес не був запущений, жодних законодавчих, активних ініціатив, які стоять на порядку денному, не запущено. Це становить колосальну загрозу для інформаційної безпеки України, оскільки технологія розвивається щогодини та, відповідно, держава вже запізнюється з рішеннями щодо контролю й заходів безпеки.

Якщо ж узагальнити ключові недоліки національної інформаційної безпеки, то їх є декілька. Передусім, низький рівень медіаграмотності населення, що дає змогу маніпулювати суспільною думкою та фактами за допомогою джерел і засобів масової інформації, мережі «Інтернет». На жаль медіаграмотність більше опрацьована різними громадськими організаціями та ініціативами, проте повинна мати й державну підтримку, програму з розвитку обізнаності населення. Звісно, є приклади й національних рівнів, як-от: «Національний проєкт із медіаграмотності Фільтр», що організований Міністерством культури та інформаційної політики України, проте він не набув масштабного поширення та залишається доволі невеликим інструментом покращення.

Повільність у реакції державного апарату на наявні загрози інформаційної безпеки, такі як досі ЗМІ із сумнівною репутацією та фактами роботи на проросійські інформаційні сили «Страна.UA.» [22], що, безумовно, є фактором внутрішнього інформаційного саботажу, який розколює суспільство та насаджує недовіру до офіційних джерел

інформації, у тому числі проштовхуючи ворожу російську пропаганду на внутрішню аудиторію.

Ігнорування проблеми розвитку штучного інтелекту як інструменту якісно нового рівня, що дає змогу створювати покращенні матеріали для дезінформації та деструктивного впливу як на українську аудиторію, так і на зовнішню, що може шкодити репутації України на міжнародному рівні й загострювати соціальну, політичну та економічну напругу всередині держави. Розробка програм і стратегій із регулювання ШІ має бути кращою. Є локальні ініціативи та рекомендації того, як розпізнати матеріали, згенеровані штучним інтелектом, та відфільтровувати цю інформацію, проте потрібно створити національні проєкти, або додати цей функціонал до наявних, оскільки ця загроза продовжує розвиватися стрімкими темпами.

Існує декілька векторів розвитку захисту українського інформаційного простору від російських деструктивних впливів. Насамперед треба розвивати інструментарій освіти населення щодо потенційних загроз зі сторони дезінформації, пропаганди тощо. Саме постійна робота із суспільством задля покращення медіаграмотності дасть змогу відфільтровувати та виявляти загрози на початках і запобігти масовому поширенню та, як результат – впливу на людей. Другим кроком можна з упевненістю назвати зменшення бюрократії й збільшення практичних кроків у сфері інформаційної безпеки. Україна має та продовжує створювати багато нормативно-правових актів, покликаних контролювати цю сферу, проте з реалізацією на практиці маємо проблеми. Розтягнутість у часі, паперова робота та заангажованість державного апарату не сприяють чіткому адмініструванню наряду інформаційного захисту. Звісно, не можна забувати про необхідність постійної стимуляції й громадського контролю за діяльністю правоохоронних органів у темі боротьби з дестабілізуючими та відверто проросійськими інформаційними майданчиками як в Україні, так і на міжнародній арені, оскільки це завдає значної шкоди репутації й іміджу держави у світовому інформпросторі. Також корисним буде переглянути перелік поточних нормативних актів та інституцій, що працюють у цій сфері, оскільки бувають випадки дублювання роботи різних служб і правових колізій. Завершальним етапом є прийняття факту авангардизму у сфері боротьби з російськими деструктивними впливами. Україна переймає багато, беззаперечно, корисних практик від західних партнерів у напрямі охорони інформаційного простору, проте останні роки показали, що багато інструментів країн Європи й західного світу в цілому

є застарілими. Тому державі потрібно сприяти креативному та новітньому підходу до розробки й практики в напрямі захисту та регулювання української інформаційної сфери.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Агресія російської федерації проти України стала шоковим етапом нашої історії, проте вона не була раптовою. Розвиток негативного ставлення мав найкращі відображення саме в інформаційному просторі рф. Пропаганда, дезінформація, деструктивні впливи передували повномасштабному вторгненню й анексії територій за довгі роки. На жаль, Україна довгий час ігнорувала ці загрози. Тому маємо зробити висновки з цього уроку та підготуватися до всіх можливих варіантів подій інформаційної боротьби, оскільки війна за розум і свідомість громадян України та партнерів тільки набирає обертів.

Ефективна протидія інформаційним впливам пропаганди можлива лише за умови залучення всіх рівнів, на яких відбувається це протистояння – державного, суспільного й індивідуального. Тільки скоординовані зусилля державних інституцій, громадських організацій та особиста відповідальність кожного громадянина здатні забезпечити формування стійкого імунітету для боротьби в інформаційному середовищі. Подальші дослідження у сфері протидії пропаганді мають бути спрямовані на глибше вивчення об'єкта інформаційного впливу, зокрема його емоційно-вольового стану, інтелектуального рівня, вікових, статевих й індивідуальних особливостей.

Інститут медіа та інформаційних систем є одним із ключових елементів національної безпеки, особливо в умовах гібридної війни, що триває в Україні. Дослідження підтверджує, що інформаційна війна є невід'ємною складовою частиною сучасних збройно-політичних конфліктів та активно використовується російською федерацією як засіб впливу на українське суспільство й міжнародну спільноту.

За останнє десятиліття зросла не лише кількість деструктивних впливів у медіапросторі, але і їх технологічна складність. Використання штучного інтелекту, маніпулятивних медіатехнологій і соціальних мереж створює нові загрози для національної безпеки. Україна стала епіцентром інформаційних атак із боку росії, яка поширює дезінформацію, пропаганду та інформаційно-психологічні операції, спрямовані на дестабілізацію суспільства, дискредитацію державних інституцій і вплив на міжнародну думку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гаврильців, М. Т. (2020). Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*, с. 201. URL: http://lsej.org.ua/2_2020/54.pdf.
2. Стратегічні комунікації ЄС: протидія деструктивним впливам: кол. моногр. / Н. П. Карпчук, Б. М. Юськів, А. М. Шуляк, С. В. Федонюк, Н. О. Шуляк; за заг. ред. Н. Карпчук. Луцьк: Вежа-Друк, 2023. ISBN 978-966-940-489-3.
3. Максим, Х. (2023). Феномен інформаційної агресії в умовах повномасштабної війни Росії проти України. *Вісник Національного університету «Львівська політехніка»*. Серія: «Юридичні науки», УДК 340:1. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2023/nov/31660/13.pdf>.
4. Іваницька, Б., Гусєва, С. (2018). Основні методи пропаганди в російському інтернет-ЗМІ. PRAVDA.RU. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/16167/ivanytska3.pdf>.
5. Малик, І. (2015). Механізми протидії негативним впливам інформаційної пропаганди. *Політичні науки*. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&p;S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=hv_2015_1_2_10.
6. Хорошко, В., Хохлячова, Ю. (2016). Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство, ч. 1. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=bezin_2016_22_3_9
7. Еляшевська, Н. (2015). Вразливість України до інформаційної війни. *Теле- та радіожурналістика*, вип. 14, с. 165–169. URL: <http://publications.lnu.edu.ua/collections/index.php/teleradio/article/view/732/738>.
8. Фещенко, І. В. (2021). Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту. *Філософія та політологія в контексті сучасної культури*. URL: <https://fip.dp.ua/index.php/FIP/article/view/1056/1181>.
9. Libicki, M. C. (1995). What Is Information Warfare? National defense university: Center for Advanced Concepts and Technology Institute for National Strategic Studies. URL: <https://apps.dtic.mil/sti/citations/ADA367662>.
10. Попович, Т. Мюнхен з Путіним і без: ідеї «руського міра» проголошені 14 років тому. *Укрінформ*. URL: <https://www.ukrinform.ua/rubric-world/3197052-munhen-z-putinim-i-bez-idei-russkogo-mira-progoloseni-14-rokiv-tomu.html> (дата звернення: 06.02.2025).
11. Коріновська, А. Путін оголосив війну Україні. Президент РФ підтримав звернення «Л/ДНР» про введення військ. URL: https://suspilne.media/210077-putin-pidtrimav-zvernenna-ldnr-pro-vvedenna-vijsk/?utm_source=copylink&utm_medium=ps.
12. US Justice Department says it disrupted Russian social media influence operation. Reuters. URL: <https://www.reuters.com/world/us/us-justice-dept-says-it-disrupted-russian-social-media-influence-operation-2024-07-09/>.
13. Для чого російська пропаганда використовує дипфейк В. Залужного. *Центр протидії дезінформації*. URL: <https://cpd.gov.ua/main/dlya-chogo-rosijska-propaganda-vykorystovuye-dipfejk-v-zaluzhnogo/>

14. Фабрика брехні. Як штучний інтелект допомагає в інформаційній війні проти України. *Новинарня*. URL: <https://novynarnia.com/2024/08/13/fabryka-brejni-yak-shtuchnyj-intelekt-dopomagaє-v-informacijnij-vijni-proty-ukrayiny/>
15. Що означає вирок по справі МН17 для України, росії та світу. *Центр протидії дезінформації*. URL: <https://cpd.gov.ua/articles/shho-oznachaye-vyrok-po-spravi-mn17-dlya-ukrayiny-rosiyi-ta-svitu/>.
16. МН17: десять років російської брехні й заперечення – EU vs Disinfo. *EU vs Disinfo*. URL: <https://euvdisinfo.eu/ua/mh17-десять-років-російської-брехні-й-зап/>
17. Скільки Росія витрачає на пропаганду? *Національний проєкт з медіаграмотності*. URL: <https://filter.mkip.gov.ua/skilky-rosiya-vytrachaye-na-propagandu>.
18. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Рішення Ради нац. безпеки і оборони України від 28.04.2014: станом на 1 трав. 2014 р. URL: <https://zakon.rada.gov.ua/laws/show/n0004525-14#Text>
19. Про інформацію: Закон України від 02.10.1992 № 2657-XII редакція від 15.11.2024: станом на 15 листоп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
20. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: УКАЗ ПРЕЗИДЕНТА УКРАЇНИ від 28.12.2021. URL: <https://www.president.gov.ua/documents/6852021-41069>.
21. Регулювання штучного інтелекту в Україні: презентуємо дорожню карту. Міністерство цифрової трансформації України. 07.10.2023. URL: <https://thedigital.gov.ua/news/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu>
22. Довженко, О., Зубченко, Я. (2022). Що не так із виданням «Страна.ua» і чому ми не віримо, що воно стало проукраїнським. *Детектор медіа*. 30.09.2022. URL: <https://detector.media/infospace/article/203301/2022-09-30-shcho-ne-tak-iz-vydanyam-strana-ua-i-chomu-my-ne-virymo-shcho-vono-stalo-proukrainskym/>

REFERENCES

1. Havryltsiv, M. T. (2020). Informatsiina bezpeka derzhavy v systemi natsionalnoi bezpeky ukrainy. *Yurydychni naukovyi elektronnyi zhurnal*, p. 201. URL: http://lsej.org.ua/2_2020/54.pdf (in Ukrainian).
2. Stratehichni komunikatsii YeS: protydiia destruktivnym vplyvam: kol. monohr. / N. P. Karpchuk, B. M. Yuskiv, A. M. Shuliak, S. V. Fedoniuk, N. O. Shuliak; za zah. red. N. Karpchuk. Lutsk: Vezha-Druk, 2023. ISBN 978-966-940-489-3 (in Ukrainian).
3. Maksym, Kh. (2023). Fenomen informatsiinoi ahresii v umovakh povnomasshtabnoi viiny Rosii proty Ukrainy. *Visnyk Natsionalnoho universytetu «Lvivska politehnika»*. Seria: «Yurydychni nauky», UDK 340:1. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2023/nov/31660/13.pdf>. (in Ukrainian).
4. Ivanytska, B., Husieva, S. (2018). Osnovni metody propahandy v rosiiskomu internet-ZMI. PRAVDA.RU. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/16167/ivanytska3.pdf> (in Ukrainian).

5. Malyk, I. (2015). Mekhanizmy protydyi nehatyvnyvym vplyvam informatsiinoi propahandy. *Politychni nauky*. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=hv_2015_1_2_10 (in Ukrainian).

6. Khoroshko, V., Khokhlachova, Yu. (2016). Informatsiina viina. *ZMI yak instrument informatsiinoho vplyvu na suspilstvo*, ch. 1. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=bez_2016_22_3_9 (in Ukrainian).

7. Eliashevskaya, N. (2015). Vrazlyvist Ukrainy do informatsiinoi viiny. *Tele- ta radiozhurnalistyka*, vyp. 14, p. 165–169. URL: <http://publications.lnu.edu.ua/collections/index.php/teleradio/article/view/732/738> (in Ukrainian).

8. Feshchenko, I. V. (2021). Informatsiina viina yak orhanichna skladova suchasnoho zbroino-politychnoho konfliktu. *Filosofia ta politolohiia v konteksti suchasnoi kultury*. URL: <https://fip.dp.ua/index.php/FIP/article/view/1056/1181> (in Ukrainian).

9. Libicki, M. C. (1995). What Is Information Warfare? National defense university: Center for Advanced Concepts and Technology Institute for National Strategic Studies. URL: <https://apps.dtic.mil/sti/citations/ADA367662> (in Ukrainian).

10. Popovych, T. Miunkhen z Putynym i bez: idei «russkoho mira» proholosheni 14 rokiv tomu. *Ukrinform*. URL: <https://www.ukrinform.ua/rubric-world/3197052-miunkhen-z-putynim-i-bez-idei-russkoho-mira-progoloseni-14-rokiv-tomu.html> (data zvernennia: 06.02.2025) (in Ukrainian).

11. Korinivska, A. Putin oholosyv viinu Ukraini. Prezydent RF pidtrymav zvernennia «L/DNR» pro vvedennia viisk. URL: https://susplne.media/210077-putin-pidtrimav-zvernennia-ldnr-pro-vvedennia-vijsk/?utm_source=copylink&utm_medium=ps (in Ukrainian).

12. US Justice Department says it disrupted Russian social media influence operation. *Reuters*. URL: <https://www.reuters.com/world/us/us-justice-dept-says-it-disrupted-russian-social-media-influence-operation-2024-07-09/> (in Ukrainian).

13. Dlia choho rosiiska propahanda vykorystovuie dipfeik V. Zaluzhnoho. *Tsentr protydyi dezinformatsii*. URL: <https://cpd.gov.ua/main/dlya-chogo-rosijska-propaganda-vykorystovuye-dipfeik-v-zaluzhnogo/> (in Ukrainian).

14. Fabryka brekhni. Yak shtuchnyi intelekt dopomahaie v informatsiinii viini proty Ukrainy. *Novynarnia*. URL: <https://novynarnia.com/2024/08/13/fabryka-brekhni-yak-shtuchnyj-intelekt-dopomagaye-v-informacijnij-vijni-proty-ukrayiny/> (in Ukrainian).

15. Shcho oznachaie vyrok po spravi MN17 dlia Ukrainy, rosii ta svitu. *Tsentr protydyi dezinformatsii*. URL: <https://cpd.gov.ua/articles/shho-oznachaye-vyrok-po-spravi-mn17-dlya-ukrayiny-rosiyi-ta-svitu/> (in Ukrainian).

16. MH17: desiat rokiv rosiiskoi brekhni y zaperechennia – EU vs Disinfo. *EU vs Disinfo*. URL: <https://euvsdisinfo.eu/ua/mh17-десять-років-російської-брехні-й-зап/> (in Ukrainian).

17. Skilky Rosiia vytrachaie na propahandu? Natsionalnyi proiekt z mediahramotnosti. URL: <https://filter.mkyp.gov.ua/skilky-rosiya-vytrachaye-na-propagandu> (in Ukrainian).

18. Pro zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy: Rishennia Rady nats. bezpeky i oborony

Ukrainy vid 28.04.2014: stanom na 1 trav. 2014 r. URL: <https://zakon.rada.gov.ua/laws/show/n0004525-14#Text> (in Ukrainian).

19. Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 № 2657-XII redaktsiia vid 15.11.2024: stanom na 15 lystop. 2024 r. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (in Ukrainian).

20. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky»: UKAZ PREZYDENTA UKRAINY vid 28.12.2021. URL: <https://www.president.gov.ua/documents/6852021-41069> (in Ukrainian).

21. Rehuliuвання shtuchnoho intelektu v Ukraini: prezentuiemo dorozhniu kartu. Ministerstvo tsyfrovoi transformatsii Ukrainy. 07.10.2023. URL: <https://thedigital.gov.ua/news/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu> (in Ukrainian).

22. Dovzhenko, O., Zubchenko, Ya. (2022). Shcho ne tak iz vydanniam «Strana.ua» i chomu my ne virymo, shcho vono stalo proukrainskym. *Detektor media*. 30.09.2022. URL: <https://detector.media/infospace/article/203301/2022-09-30-shcho-ne-tak-iz-vydanniam-stranaua-i-chomu-my-ne-virymo-shcho-> (in Ukrainian).

Матеріал надійшов до редакції 29.05.2025 р.

УДК 327:004

Ганна Озернюк,

кандидат юридичних наук,

доцент кафедри міжнародних відносин та права,

Національний університет «Одеська політехніка»,

ozernuk@ukr.net

ORCID ID: 0000-0001-5030-6356,

DOI 10.29038/2524-2679-2025-02-121-135

ЦИФРОВА ДИПЛОМАТІЯ ТА ДИПЛОМАТІЯ ДАНИХ: ІСТОРИЧНІ ПЕРЕДУМОВИ Й КОНЦЕПТУАЛЬНІ ВІДМІННОСТІ

У статті на основі дослідження етапів становлення дипломатичних комунікацій від традиційних до цифрових висвітлено історичні передумови становлення цифрової дипломатії й дипломатії даних. Обстоюється думка, що цифрова дипломатія з'явилася завдяки популяризації цифрових технологій та інтенсифікувалася в період усесвітньої пандемії. Дипломатія