Медіафорум : аналітика, прогнози, інформаційний менеджмент.
Том 16. 129-138

Mediaforum: Analytics, Forecasts, Information Management.
Volume 16. 129-138

https://doi.org/10.31861/mediaforum.2025.16.129-138
УДК: [327.88:004.7]:355.48(470:477) "2022/..."

© *Іванна Макух-Федоркова*[1]

ВПЛИВ ЦИФРОВОЇ ДЕЗІНФОРМАЦІЇ НА ПЕРЕБІГ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

У статті аналізується вплив цифрової дезінформації на перебіг російсько-української війни як одного з ключових інструментів сучасної гібридної війни. Розглядаються основні етапи еволюції дезінформаційних кампаній з 2014 року до 2025 року, з особливою увагою до періоду після повномасштабного вторгнення Росії в Україну. Підкреслюється, як фейкові новини, маніпуляції в соціальних мережах, deepfake, штучний інтелект та інші цифрові технології використовуються для деморалізації українського суспільства, підриву довіри до державних інституцій, дестабілізації внутрішньої ситуації та впливу на міжнародну громадську думку. Розглядаються приклади масштабних інформаційних операцій та кіберінцидентів, які супроводжували дезінформаційні кампанії, зокрема атаки на «Київстар», державні реєстри та транспортну інфраструктуру. Аналізується протидія з боку українських і міжнародних акторів, зокрема ЄС та США, а також важливість посилення цифрової стійкості. Стаття демонструє, що цифрова дезінформація стала однією з визначальних стратегій у війні Росії проти України.

Ключові слова: *цифрова дезінформація, інформаційна війна, гібридна війна, Україна, Росія, соціальні мережі, deepfake, штучний інтелект, кібербезпека, міжнародна підтримка.*

The Impact of Digital Disinformation on the Course of the Russian-Ukrainian War

This article examines the impact of digital disinformation on the course of the Russian-Ukrainian war, positioning it as a central tool in Russia's hybrid

[1] Кандидатка політичних наук, доцент кафедри міжнародних відносин та суспільних комунікацій Чернівецького національного університету імені Юрія Федьковича, Україна. E-mail: i.makuch-fedorkova@chnu.edu.ua; https://orcid.org/0000-0003-2198-8727.

warfare strategy. Since 2014, and especially following the full-scale invasion in 2022, disinformation campaigns have intensified, targeting both Ukrainian and international audiences. The analysis explores how fake news, manipulated content, AI-generated deepfakes, and coordinated propaganda efforts have been used to undermine public morale, erode trust in institutions, distort narratives about the war, and weaken international support for Ukraine.

The article also discusses the role of cyber incidents that have supported disinformation efforts, such as the December 2023 cyberattack on the major telecom provider Kyivstar, which disrupted critical communications and public services, creating confusion and panic. Other attacks on state registries, the Ministry of Justice, and Ukrainian Railways are considered within the broader context of information operations.

Attention is given to Ukraine's evolving responses, including institutional, civic, and international initiatives aimed at countering false narratives and enhancing digital resilience. Ukraine's experience in combating Russian disinformation is supported by cooperation with Western governments, fact-checking organizations like VoxCheck, and technology platforms such as YouTube, which play a vital role in moderating harmful content.

The study also highlights shifts in international cyber cooperation, especially after the 2025 change in U.S. leadership, which led to a pause in offensive cyber collaboration. In contrast, the European Union expanded its support through cybersecurity initiatives, new satellite intelligence systems, and closer ties with Ukrainian cyber institutions via ENISA.

Ultimately, the article argues that digital disinformation has become one of the most defining weapons of the war, requiring not only technical defenses but also societal resilience, strategic communication, and international unity.

Keywords: *digital disinformation, hybrid warfare, Ukraine, Russia, fake news, deepfakes, information operations, cyberattacks, critical infrastructure, international cooperation, digital resilience, artificial intelligence.*

Постановка проблеми. У XXI столітті війна все більше виходить за межі традиційного збройного протистояння, набуваючи нових форм, серед яких ключове місце займає кіберпростір. Кібернетична війна між Україною та Росією стала одним із найважливіших фронтів сучасного конфлікту, особливо після 2014 року, коли почалася анексія Криму, і ще більше після повномасштабного вторгнення Російської Федерації у 2022 році. Цей новий тип війни охоплює широкий

спектр дій: від атак на критичну інфраструктуру, зламу державних і військових систем, шпигунства до масштабного розповсюдження дезінформації, спрямованої на підрив довіри до інституцій, деморалізацію суспільства та дестабілізацію ситуації в країні.

Росія вже понад десятиліття використовує кіберзброю як невід'ємну складову гібридної війни як проти України, так і проти західних країн, зокрема США та Європи. Однак, незважаючи на масштабність і регулярність таких атак, очікуваних результатів агресору досягти не вдалося. Однією з причин цього стала здатність України до швидкої адаптації, аналізу ворожих методів та побудови ефективної системи захисту. За роки конфлікту Київ напрацював значний досвід протидії кіберзагрозам, мобілізувавши державні ресурси, волонтерські ініціативи та заручившись підтримкою провідних західних технологічних компаній і партнерів. Це дозволило суттєво зміцнити національну кіберстійкість і вдосконалити інформаційну безпеку.

Зростаюча актуальність кібернетичного виміру війни зумовлена тим, що сучасні конфлікти дедалі частіше відбуваються у цифровому просторі. Росія активно використовує дезінформаційні кампанії як інструмент впливу, від фейків і маніпуляцій до психологічного тиску через соціальні мережі, ботоферми та підконтрольні ЗМІ. Такі дії спрямовані не лише проти України, але й мають транскордонний характер, орієнтований на підрив підтримки України за кордоном.

Водночас, Україна демонструє стійку здатність до ефективної інформаційної оборони. Вона розвиває інституційні та громадянські ініціативи у сфері фактчекінгу, цифрової грамотності, кібербезпеки та міжнародної координації, що дозволяє протидіяти загрозам нового типу. Саме інформаційно-кібернетичний фронт сьогодні є не менш вирішальним, ніж військовий, і потребує детального аналізу, щоб зрозуміти, яким чином технології, комунікація та стратегічна інформаційна боротьба впливають на хід сучасної війни.

Аналіз останніх досліджень і публікацій. Останні дослідження та публікації висвітлюють активізацію цифрової агресії Росії проти України, зокрема у вигляді кібератак та дезінформаційних кампаній. Значна увага приділяється резонансній атаці на телекомунікаційного оператора «Київстар» у грудні 2023 року, яку пов'язують з угрупованням «Солнцепек» (Кузьменко 2023) та російською розвідкою, згідно з даними СБУ (Мигаль 2024). Цей інцидент, як і напади на державні

реєстри (Dysa 2024) та «Укрзалізницю» (Reuters 2025), розглядається як частина масштабної інформаційно-кібернетичної кампанії, спрямованої на дестабілізацію критичної інфраструктури України (Тартачний 2024). Паралельно з цим відзначається зростання міжнародної уваги до цифрової безпеки України. Європейський Союз посилює співпрацю у сфері кіберзахисту (Enhanced EU-Ukraine cooperation 2023) та планує запуск супутникової розвідки після скорочення підтримки з боку США (Isayev 2025; Superville & Klepper 2025). Аналіз також фіксує поширення російських інформаційних операцій за межами України, зокрема проти військових і транспортних структур Європи (Lyngaas 2023), та зростання загроз для західних демократій загалом (Odarchenko & Davlikanova 2024). Ці публікації засвідчують системний характер дезінформаційної війни та підкреслюють потребу в консолідованій міжнародній відповіді (Takeaways from the EU's summit 2025).

Метою статті є дослідження впливу цифрової дезінформації на перебіг російсько-української війни та аналіз механізмів її поширення й засобів протидії.

Виклад основного матеріалу. Цифрова дезінформація та кіберінциденти відіграють ключову роль у перебігу російсько-української війни, особливо з моменту початку повномасштабного вторгнення у 2022 році. Росія активно використовує кібератаки як засіб гібридної війни, спрямований не лише на військову інфраструктуру, але й на цивільне населення, критичні сервіси та інформаційний простір. Одним із наймасштабніших кіберінцидентів у ході російсько-української війни стала атака на телекомунікаційного оператора «Київстар» у грудні 2023 року. Внаслідок цієї атаки мільйони українців залишилися без мобільного зв'язку та Інтернету, були порушені системи банкінгу, повітряного оповіщення, а також робота багатьох сервісів державного значення. Відповідальність за атаку взяла на себе російська хакерська група «Солнцепёк», яка заявила, що знищила 10 тисяч комп'ютерів, понад 4 тисячі серверів, усі системи хмарного зберігання даних і резервного копіювання (Кузьменко Ю 2023). Служба безпеки України (СБУ) встановила, що за атакою стоїть хакерське угруповання Sandworm, яке є підрозділом Головного управління Генерального штабу Збройних сил Російської Федерації (ГРУ РФ). Згідно з повідомленнями, хакери проникли в мережу оператора через обліковий запис одного зі співробітників, що дозволило їм за-

кріпитися в системі та знищити внутрішню мережеву інфраструктуру (Мигаль М. 2024).

У грудні 2024 року сталася атака на державні реєстри України, що належать Міністерству юстиції. Атака призвела до тимчасової зупинки роботи реєстраційних сервісів, однак витоку персональних даних вдалося уникнути. Згідно з офіційною інформацією, за атакою стояли хакери, пов'язані з російськими спецслужбами (Dysa Y. 2024).

У березні 2025 року зазнала кібератаки компанія «Укрзалізниця», внаслідок чого пасажири не могли скористатися онлайн-продажем квитків, а всі операції здійснювалися вручну. Відновлення повної роботи IT-систем тривало кілька тижнів (Ukraine's railways restore 2025).

У свою чергу, українські хакери також активно проводять кібероперації проти російської інфраструктури. Зокрема, було здійснено атаку на московського інтернет-провайдера «Інфотел», злам БТІ Москви, атаку на платіжну систему «Мир», а також втручання в систему водоканалу Севастополя, змінюючи дані про споживання води (Тартачний О. 2024).

Отже, цифрова дезінформація та кіберінциденти стали невід'ємною частиною сучасного конфлікту. Вони не лише впливають на моральний стан населення і функціонування критичної інфраструктури, а й формують новий вимір війни – інформаційно-кібернетичний фронт. Атаки на такі критично важливі об'єкти, як «Київстар», державні реєстри, «Укрзалізниця» та інші інституції, показали вразливість інформаційної інфраструктури та масштаб потенційних загроз. Росія активно застосовує кіберзброю як інструмент тиску: від фізичного знищення серверів до психологічних операцій, спрямованих на дезінформацію населення та створення паніки. Водночас Україна продемонструвала здатність до цифрової оборони та проведення ефективних кібервідповідей, атакуючи російські інформаційні системи та структури. Ці кіберінциденти не лише підкреслюють необхідність інвестицій у кібербезпеку, а й вимагають системної підготовки держави та суспільства до інформаційної війни.

Варто зазначити, що після приходу до влади адміністрації Дональда Трампа в січні 2025 року, підтримка Сполученими Штатами України в сфері кіберзахисту зазнала суттєвих змін. Так, у лютому 2025 року міністр оборони Піт Хегсет наказав призупинити всі наступальні кібероперації проти Росії, що свідчить про зміну підходу США до кіберзагроз з боку Росії. А вже у березні 2025 року адміні-

страція Трампа призупинила обмін розвідданими з Україною, позбавивши її важливої інформації для оборони (Superville D., Klepper D. 2025). Ці кроки викликали занепокоєння серед союзників США та були розцінені як послаблення підтримки України в її протистоянні з державою-агресором. Після зміни політики США щодо підтримки України в сфері кібербезпеки, Європейський Союз активізував зусилля для посилення співпраці з Україною та зміцнення власної інформаційної політики. Так, у відповідь на призупинення США обміну розвідданими з Україною, ЄС розглядає створення нової супутникової мережі для покращення військової розвідки та зменшення залежності від американської підтримки (Isayev K. 2025). Також ще в грудні 2023 року Європейське агентство з кібербезпеки (ENISA) підписало робочу угоду з українськими партнерами, спрямовану на обмін найкращими практиками, підвищення обізнаності та зміцнення кіберстійкості (Enhanced EU-Ukraine cooperation in Cybersecurity 2023). Крім того, європейські лідери погодили план збільшення оборонних витрат, що включає інвестиції в кіберсистеми та електронну війну, підкреслюючи прагнення Європи до більшої автономії в питаннях безпеки та оборони (Takeaways from the EU's landmark 2025) Ці кроки свідчать про консолідацію зусиль Європи в сфері інформаційної політики та кібербезпеки, спрямованих на підтримку України та зміцнення власної стійкості перед сучасними загрозами.

Вплив цифрової дезінформації на перебіг російсько-української війни пройшов кілька етапів, кожен з яких відзначався зміною тактики, інструментів та масштабів інформаційних операцій. Перший етап, що розпочався ще до 2014 року, характеризувався активною пропагандою через контрольовані Росією медіа та соціальні мережі. Метою було формування антиукраїнських настроїв, виправдання агресивних дій Кремля та створення образу України як «нездатної до самостійного існування держави». У цей період використовувалися традиційні методи маніпуляції, такі як фабрикація новин, перекручування історичних фактів і тиражування міфів про «громадянську війну». Другий етап почався після вторгнення Росії на Донбас і анексії Криму. Москва активно застосовувала ботоферми, тролів та фейкові акаунти, щоб посіяти паніку, розколоти українське суспільство та підірвати довіру до влади. Російські спецслужби також експериментували з більш персоналізованими атаками, такими як витоки конфіденційних даних і поширення компрометуючої інформації про

українських політиків і військових. Третій етап розпочався з повномасштабного вторгнення у 2022 році (Odarchenko K., Davlikanova E. 2024). В цей період агресор перейшов до ще більш масштабних кампаній цифрової дезінформації, спрямованих як на внутрішню аудиторію, так і на Захід. Було запущено безліч інформаційних атак з метою дискредитації українських лідерів, знецінення військової допомоги від партнерів та посилення розбіжностей між союзниками. Водночас, Україна ефективно організувала контрпропаганду, створивши власні аналітичні центри, такі як Центр протидії дезінформації та залучаючи міжнародні платформи до блокування російських пропагандистських ресурсів. Зокрема, Центр співпрацює з такими аналітичними платформами, як VoxCheck, для розробки рекомендацій щодо протидії російській пропаганді. Крім того, міжнародні технологічні компанії, такі як YouTube, обмежують доступ до російських державних медіа на своїх платформах, що сприяє зменшенню поширення дезінформації. І четвертий етап розпочався після 2023 року, коли дезінформаційні кампанії стали ще складнішими. Росія почала широко використовувати штучний інтелект для створення глибоких фейків, маніпулятивних відео та синтетичних новин.

Варто наголосити, що одним із наймасштабніших кіберінцидентів, що спричинив значні побічні наслідки за межами України, стала атака на міжнародну компанію, що надає послуги в сфері супутникового зв'язку Viasat, ще на початку повномасштабного вторгнення. Унаслідок цієї операції було порушено роботу супутникової широкосмугової послуги KA-SAT, що зачепило десятки тисяч користувачів по всій Європі. Зокрема, ця атака спричинила збій у роботі 5800 вітрових турбін у Центральній Європі та призвела до пошкоджень критичної інфраструктури.

Останнім часом країна-агресор все частіше використовує кібератаки як інструмент гібридної війни, зокрема для підриву логістичних маршрутів та організацій, що надають допомогу Україні. Особливо примітним випадком була атака із застосуванням програмного забезпечення «вимагача Prestige», яка була спрямована на логістичні компанії в Польщі (Lyngaas S. 2023). Використання цього шкідливого програмного забезпечення дозволило створити ілюзію злочинної діяльності та ускладнило ідентифікацію справжніх замовників атаки. Подібна тактика спостерігалася і в таємних російських спробах організувати диверсії на польській залізничній мережі.

Водночас Україна, за підтримки міжнародних партнерів, активно зміцнює інформаційну безпеку, співпрацюючи з великими технологічними компаніями та запроваджуючи алгоритми для виявлення маніпулятивного контенту. Отже, цифрова дезінформація стала потужною зброєю в інформаційній війні, яка безпосередньо впливає на бойові дії, міжнародну підтримку та моральний стан суспільства. Її еволюція показує, що боротьба за правду і довіру залишається критично важливим фронтом у російсько-українській війні.

Висновки. Підбиваючи підсумок, зауважимо, що цифрова дезінформація стала одним із ключових інструментів сучасної війни. Вона відіграє важливу роль у формуванні суспільної думки, дестабілізації державних інституцій, підриві довіри до влади, деморалізації населення та впливі на рівень міжнародної підтримки. Російсько-українська війна переконливо продемонструвала, що інформаційний фронт є не менш вирішальним, ніж збройний, а перемоги в цій сфері нерідко визначають стратегічні перспективи всієї кампанії.

Протягом усього конфлікту Росія систематично застосовувала дезінформаційні технології для посилення внутрішнього хаосу в Україні, дискредитації української влади та послаблення підтримки з боку партнерів. У відповідь Україна змогла сформувати ефективну систему інформаційної протидії, що ґрунтується на роботі аналітичних центрів, партнерстві з міжнародними технологічними платформами та активному залученні громадянського суспільства.

Завдяки цим зусиллям Україна не лише ефективно захищає власний інформаційний простір, але й формує потужний контрнаратив на міжнародній арені, сприяючи консолідації демократичних країн у боротьбі проти авторитарної пропаганди. Подальший розвиток технологій, зокрема штучного інтелекту, ускладнює виклики, пов'язані з інформаційною безпекою, роблячи завдання боротьби з дезінформацією ще більш актуальним.

Водночас війна в Україні показала, що кібернетичні атаки та інформаційні операції стали новим типом зброї у XXI столітті. Вони визначають не лише характер конфліктів, а й стратегії національної безпеки. Український досвід свідчить про важливість довгострокових інвестицій у кібербезпеку, розвитку цифрової політики, міжнародної співпраці та підвищення цифрової стійкості. Саме інформаційно-кібернетичний вимір може стати вирішальним у майбутньому глобальному протистоянні між демократією й авторитаризмом.

Україна вже стала прикладом для інших країн, які стикаються з викликами гібридної агресії. Її досвід є цінним внеском у розуміння сучасної війни, де боротьба за правду, довіру та цифрову безпеку є питанням не лише національного, а й міжнародного значення.

References:

1. Kuzmenko Yu. Ataka na «Kyivstar»: rosiiski khakery «Solntsepeka» vzialy vidpovidalnist za zlam. Suspilne.media. 13.12 2023. URL: https://suspilne.media/638370-ataka-na-kiivstar-rosijski-hakeri-solncepeka-vzali-vidpovidalnist-za-zlam/ (In Ukrainian) – data zvernennia: 30.03.2025.

2. Myhal M. Ataka na «Kyivstar»: SBU identyfikuvala khakeriv rosiiskoi rozvidky. Hlavkom. 4.05 2024. URL: https://glavcom.ua/country/incidents/ataka-na-kijivstar-sbu-identifikuvala-khakeriv-rosijskoji-rozvidki--994308.html (In Ukrainian) – data zvernennia: 30.03.2025.

3. Tartachnyi O. Rosiisko-ukrainska kiberviina: shcho ta chomu staie mishenniu khakeriv. Thepage. 19.11 2024. URL: https://thepage.ua/ua/it/yak-rosijsko-ukrayinska-vijna-prohodit-u-kiberprostori? (In Ukrainian) – data zvernennia: 30.03.2025.

4. Dysa Y. Ukraine says Russian cyberattack hits state registries but no data lost. Reuters. December 20, 2024. URL: https://www.reuters.com/technology/cybersecurity/ukraine-says-russian-cyberattack-hits-state-registries-no-data-lost-2024-12-20/ (date of access: 02.04.2025).

5. Enhanced EU-Ukraine cooperation in Cybersecurity. News article. 8 December 2023. URL: https://cybersecurity-centre.europa.eu/news/enhanced-eu-ukraine-cooperation-cybersecurity-2023-12-08_en (date of access: 01.04.2025).

6. Isayev K. EU plans launching intelligence satellites after US pause on Ukraine support. Caliber.Az. 16 March 2025. URL: https://caliber.az/en/post/eu-plans-launching-intelligence-satellites-to-after-us-pause-on-ukraine-support? (date of access: 02.03.2025).

7. Lyngaas S. Russian hackers targeted European military and transport organizations in newly discovered spying campaign. CNN. Wed March 15, 2023. URL: https://edition.cnn.com/2023/03/15/politics/russian-hackers-europe-military-organizations-microsoft/index.html (date of access: 28.03.2025).

8. Odarchenko K., Davlikanova E. Russia's evolving information war poses a growing threat to the West. UkraineAlert. November 26, 2024. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/russias-

evolving-information-war-poses-a-growing-threat-to-the-west/ (date of access: 29.03.2025).

9. Superville D., Klepper D. Trump administration pauses flow of intelligence to Ukraine. The Associated Press. Wednesday, Mar.5, 2025. URL: https://www.defensenews.com/global/europe/2025/03/05/trump-administration-pauses-flow-of-intelligence-to-ukraine/? (date of access: 03.04.2025).

10. Takeaways from the EU's landmark security summit after Trump said Europe must fend for itself. World News. March 7, 2025. URL: https://apnews.com/article/europe-defense-ukraine-russia-us-military-spending-dbc6133a2412ec02adf87078f2f2f5cc (date of access: 02.04.2025).

11. Ukraine's railways restore half of IT services hit by cyberattack so far. Reuters. April 9, 2025. URL: https://www.reuters.com/world/europe/ukraines-railways-restore-half-it-services-hit-by-cyber-attack-so-far-2025-04-09/ (date of access: 02.04.2025).

Надійшла до редакції / Received: 21.04.2025 *Схвалено до друку / Accepted: 02.06.2025*