УДК: 351.74:355.1(100)

https://doi.org/10.52058/2786-6300-2025-8(38)-382-390

Серветник Володимир Віталійович доктор філософії галузі публічне управління та адміністрування, доцент кафедри публічного адміністрування Навчально-наукового інституту управління, економіки та бізнесу, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», https://orcid.org/0009-0000-5936-9927

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ: РОЛЬ ДЕРЖАВИ ТА ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Анотація. Стаття ґрунтовно аналізує, як гібридна війна Російської Федерації трансформує інформаційний простір України й висуває інформаційну безпеку на рівень екзистенційного пріоритету. Автор обґрунтовує, що сучасні інформаційно-психологічні операції супроводжують збройні дії та мають на меті підірвати державність, зруйнувати суспільну єдність і делегітимізувати інститути влади. Методологічно використано контент-аналіз урядових документів (Стратегії інформаційної безпеки, постанови КМУ № 195 про телемарафон «Єдині новини»), аналітику Центру стратегічних комунікацій, Detector Media та EUvsDisinfo, а також практичні кейси волонтерських проєктів StopFake, VoxCheck і OSINT-спільнот. У результаті продемонстровано, що багаторівневу оборону формують три підсистеми: 1) державна – санкційна політика РНБО, нормативне блокування пропагандистських ресурсів, розбудова кіберзахисту СБУ і ДССЗІ; 2) громадянська – волонтерські фактчек-ініціативи, краудсорсинговий моніторинг Telegram-каналів, освітні програми медіаграмотності (Very Verified від IREX); 3) гібридна – партнерські формати, у яких держава делегує ГО виконання частини комунікаційних функцій. Виявлено, що ключовою проблемою залишається недостатня координація: відсутність єдиного стратегічного центру призводить до дублювання повноважень РНБО, МКІП та СБУ, а також до затримок у кризовому реагуванні. Вторинна проблема – правовий вакуум: законопроєкт «Про протидію дезінформації» ще не врегулював баланс між безпекою та свободою слова. Автор пропонує створити національний координаційний центр інформаційної безпеки, ухвалити збалансований закон про дезінформацію, імплементувати стандарти Digital Services Act для платформ і системно розширити цифрову освіту. Практична цінність дослідження полягає в тому, що воно окреслює конкретні механізми синергії держави й громадянського суспільства, здатні зміцнити інформаційний суверенітет України перед викликами XXI століття.

Ключові слова: гібридна війна, інформаційна безпека, дезінформація, кіберзагрози, цифрова грамотність, громадянське суспільство.

Servetnyk Volodymyr Vitaliiovych PhD in Public Administration, Associate Professor at the Department of Public Administration, Educational and Scientific Institute of Management, Economics and Business, PJSC "Higher Educational Institution 'Interregional Academy of Personnel Management'", https://orcid.org/0009-0000-5936-9927

INFORMATION SECURITY IN THE CONDITIONS OF HYBRID WARFARE: THE ROLE OF THE STATE AND CIVIL SOCIETY

Abstract. The article offers an in-depth analysis of how the Russian Federation's hybrid war has reshaped Ukraine's information environment, pushing information security to the level of an existential priority. The author argues that contemporary information-psychological operations accompany kinetic warfare and aim to undermine statehood, fracture social cohesion, and delegitimise public institutions. Methodologically, the study employs content analysis of key governmental documents (the National Information Security Strategy; Cabinet of Ministers Resolution No. 195 on the "United News" tele-marathon), analytics from the Centre for Strategic Communication, Detector Media, EUvsDisinfo, and case studies of volunteer projects such as StopFake, VoxCheck, and various OSINT communities.

Findings show that Ukraine's multi-layered defence rests on three subsystems: State level – sanctions imposed by the National Security and Defence Council, regulatory blocking of propaganda resources, and the cyber-defence work of the Security Service of Ukraine and the State Service for Special Communications; Civic level – volunteer fact-checking initiatives, crowdsourced monitoring of Telegram channels, and large-scale media-literacy programmes (e.g., IREX's Very Verified); Hybrid level – partnership formats in which the state outsources part of its communication functions to NGOs.

The principal challenge remains insufficient coordination: the absence of a single strategic centre leads to duplicated mandates across the NSDC, the Ministry of Culture and Information Policy, and the SBU, producing delays in crisis response. A secondary issue is the legal vacuum: the draft Law on Countering Disinformation has not yet reconciled security needs with freedom of expression. The author recommends establishing a National Information-Security Coordination Centre, adopting a balanced disinformation law, transposing Digital Services Act standards to online platforms, and systematically expanding digital-literacy education. The study's practical value lies in detailing specific mechanisms for state–civil-society synergy capable of reinforcing Ukraine's information sovereignty against twenty-first-century threats.

Keywords: hybrid warfare; information security; disinformation; cyber threats; digital literacy; civil society.

Постановка проблеми. Інформаційна безпека України, особливо в умовах гібридної війни, перетворилася на ключовий компонент національної безпеки. Від початку російської агресії 2014 р., а особливо після повномасштабного вторгнення 24 лютого 2022 р., «інформаційний фронт» став таким самим критичним, як і фізичний. Російська Федерація системно застосовує інформаційно-психологічні операції, кібератаки, кампанії дезінформації та фейкові новини, поширює вкиди у соціальних мережах і підриває довіру до державних інституцій [1; 2]. Головною мішенню цих атак є українське суспільство: противник прагне деморалізувати населення, сіяти паніку, роз'єднувати громадян і делегітимізувати державу. При цьому демократична модель управління не дозволяє повністю закрити інформаційний простір, тому постає завдання знайти баланс між свободою слова та безпековими потребами. У такій ситуації вирішальною стає активна участь громадянського суспільства, яке доповнює державні зусилля та підвищує стійкість інформаційного середовища.

Аналіз останніх досліджень і публікацій. Проблема інформаційної безпеки в умовах гібридної війни активно досліджується як українськими, так і зарубіжними авторами. Національний вимір окреслюють урядові рішення щодо протидії дезінформації та централізованого інформування: постанова про створення телемарафону «Єдині новини», яка задала формат кризової комунікації [1], та проєкт закону про заборону російського програмного забезпечення, що розширює інструменти кіберзахисту [2]. Теоретичний фундамент формують праці вітчизняних дослідників – зокрема, узагальнення Кузьменка про інформаційну безпеку як складову національної безпеки [3] і монографія під ред. Чепурного, присвячена гібридній війні та її інформаційному вимірові [7]. У практичній площині проблему висвітлюють методичні матеріали МКІП щодо протидії дезінформації [4] та аналітика Почепцова про сучасні інформаційні війни [5].

Системний моніторинг російських наративів забезпечує Центр стратегічних комунікацій та інформаційної безпеки [6] і незалежні медійні платформи, зокрема Detector Media, яка відстежує тенденції інформаційної війни [8]. На міжнародному рівні ключовим джерелом даних є база EUvsDisinfo [12] і звіти East StratCom Task Force Європейської служби зовнішніх справ [10], що документують дезінформаційні кампанії Кремля. Європейська комісія пропонує нормативну рамку через оновлений «Code of Practice on Disinformation» [9] та Digital Services Act [11], які визначають спільні стандарти протидії маніпулятивному контенту для онлайн-платформ.

Окрему роль відіграють дослідження міжнародних експертів: матеріал NATO Review аналізує еволюцію гібридної війни й підкреслює важливість довіри як «антидота» проти інформаційних атак [14], а стаття *The Economist* висвітлює успіхи українських «інформаційних воїнів» у цифровому середовищі [15]. Практичні інструменти підвищення медіаграмотності пропонує курс «Very Verified» від IREX, спрямований на розвиток критичного мислення у широкої аудиторії [13].

Узагальнення цих джерел засвідчує: попри значний масив досліджень щодо тактик та наслідків дезінформації, роль громадянського суспільства в координації зусиль з державою та відповідальність обох сторін за інформаційний суверенітет України залишаються недостатньо розкритими, що й визначає подальший напрям наукового пошуку.

Мета статті – проаналізувати внесок держави й громадянського суспільства у зміцнення інформаційної безпеки України в умовах гібридної війни та обґрунтувати напрями їхньої взаємодії для протидії зовнішнім і внутрішнім інформаційним загрозам.

Виклад основного матеріалу. За словами дослідника інформаційних конфліктів Г. Почепцова [5] та аналітиків *NATO Review* [14], інформаційна безпека нині перетворилася на невід'ємний компонент національної безпеки, а інформаційна війна – на повноцінний театр воєнних дій. В українському випадку, після агресії Російської Федерації 2014 р. і особливо після повномасштабного вторгнення 24 лютого 2022 р., саме інформаційний фронт нерідко визначає стійкість держави. Росія системно застосовує пропагандистські й кібернетичні інструменти – від централізованих телеефірів і клонованих медіа до мереж ботів у Facebook, Telegram та X – щоб деморалізувати населення, сіяти паніку та підривати довіру до демократичних інституцій [8; 12].

Як показують огляди Центру стратегічних комунікацій та інформаційної безпеки (SPRAVDI) [6] і *Detector Media* [8], ці атаки носять багаторівневий характер: дезінформаційні сюжети на телеканалах підкріплюються фейковими новинами в соціальних мережах, а інформаційно-психологічні операції супроводжуються хакерськими зламами урядових сайтів. EUvsDisinfo фіксує тисячі прикладів російських наративів, що намагаються розпалити мовні, релігійні та регіональні конфлікти всередині країни [12].

У відповідь держава поступово переходить від реактивних до проактивних дій. Ключовим кроком стало ухвалення Стратегії інформаційної безпеки України (2021 р.), а під час гарячої фази війни – створення єдиного телемарафону «Єдині новини», нормативно закріпленого постановою КМУ № 195 від 18.03.2022 р. [1]. Для протидії ворожому ПЗ уряд 2023 р. схвалив законопроєкт про заборону російських програмних продуктів [2], а Міністерство культури та інформаційної політики розробило концепцію закону «Про протидію дезінформації» [4].

Водночас незалежні ініціативи – StopFake, VoxCheck, курс медіаграмотності *Very Verified* від IREX [13] – підвищують критичне мислення громадян і фактично доповнюють зусилля держави.

Так, український досвід підтверджує тезу, що ефективна інформаційна оборона можлива лише за умови синергії урядових стратегій і активної участі громадянського суспільства, здатного швидко виявляти та нейтралізувати гібридні загрози.

Раду національної безпеки і оборони України вважають головним координатором у сфері протидії дезінформації: саме РНБО запроваджує санкції проти медіаресурсів і платформ, що працюють в інтересах країни-агресора [7]. Формуванням державної інформаційної політики опікується Міністерство культури та інформаційної політики, тоді як Центр стратегічних комунікацій [3] виконує аналітичну й моніторингову функції, фіксуючи та класифікуючи ворожі інформаційні операції. Кіберзахист забезпечують Державна служба спеціального зв'язку та Служба безпеки України, які оперативно реагують на злами інформаційних систем і поширення шкідливого контенту.

До помітних державних рішень належать блокування російських телеканалів і сайтів, запуск єдиного телемарафону «Єдині новини» [6] та масштабні інформаційні кампанії на підтримку ЗСУ. Однак міжвідомча взаємодія залишається фрагментарною, а процедури швидкого спростування фейків – недостатньо відпрацьованими.

Водночас однією з найсильніших переваг України є мобілізоване громадянське суспільство. На відміну від багатьох західних демократій, де протидія дезінформації покладається переважно на державу або професійні медіа, в Україні ключову роль відіграють волонтери, аналітичні центри та ініціативи «знизу», що самостійно здійснюють факт-чекінг, спростовують фейки й моніторять інформаційний простір [11]. Платформи StopFake, VoxCheck, Media Detector і Texty.org.ua вже з 2014 р. систематично перевіряють факти, публікують аналітику і глосарії російських наративів [9]. Після 24 лютого 2022 р. з'явилися сотні Telegram-каналів, чат-ботів і онлайн-платформ, що навчають користувачів методам інформаційної самооборони.

Громадські організації беруть участь у розробленні законодавчих пропозицій, проводять тренінги й кампанії з медіаграмотності. У співпраці з Internews, IREX і Deutsche Welle Akademie вони охопили навчальними програмами вчителів, держслужбовців і молодь; показовим прикладом є курс «Very Verified» від IREX [12], спрямований на розвиток критичного мислення. Крім освітньої роботи, аналітичні центри – зокрема Detector Media та Інститут масової інформації – регулярно звітують про мову ворожнечі й маніпулятивні техніки у вітчизняних та іноземних медіа, надаючи журналістам і законодавцям фактичну базу для реагування.

Суттєвим чинником стійкості стала й самоорганізація громадян: користувачі масово повідомляють про підозрілий контент, фейкові канали та ботоферми через чат-боти СБУ й форму зворотного зв'язку на сайті Центру стратегічних комунікацій. Така горизонтальна мобілізація свідчить, що інформаційна безпека в Україні ґрунтується не лише на державних інституціях, а й на активній участі суспільства, без якої неможливо ефективно протидіяти гібридним загрозам.

Українське громадянське суспільство виконує не лише оборонну, а й інноваційну функцію в інформаційній сфері, часто випереджаючи державні інституції у виявленні та спростуванні ворожих наративів. Проте, попри очевидні успіхи, координація між усіма суб'єктами інформаційної безпеки залишається недостатньою: відсутність єдиного стратегічного центру спричиняє дублювання функцій, фрагментарні рішення й затримки в кризовому реагуванні. Повноваження нині розподілені між РНБО, МКІП, ДССЗІ, СБУ, Центром стратегічних комунікацій та іншими структурами, однак законодавчо визначеного механізму їхньої взаємодії досі немає. Навіть затверджена Стратегія інформаційної безпеки не забезпечена чіткими індикаторами ефективності, системами моніторингу й належним фінансуванням. Додатковим викликом залишається відсутність сучасної правової бази: дискусійний законопроєкт «Про протидію дезінформації» [14] через ризики цензури не ухвалено, тож спеціального інструменту, що дозволив би боротися з маніпулятивними кампаніями без порушення свободи слова, Україна не має.

Гібридна війна Росії перенесла поле бою до соцмереж, месенджерів, відеоплатформ і навіть відеоігор; алгоритми цих сервісів формують інформаційні «бульбашки», а штучно згенерований deepfake-контент додає новий рівень загроз (показовим став фейковий «заклик до капітуляції» 2022 р.). Проблему ускладнює домінування приватних іноземних платформ – Facebook, TikTok, YouTube, Telegram – які не мають офісів в Україні й повільно реагують на запити щодо блокування дезінформації; їхні алгоритми просувають емоційний контент, через що навіть українські медіа інколи несвідомо ретранслюють ворожі меседжі.

Для адаптації до динамічних загроз потрібна довгострокова модель інформаційної безпеки, що поєднає централізовані механізми (державна стратегія, національний координаційний центр) і децентралізовані ініціативи громадських організацій, незалежних медіа й експертних спільнот. Першочергово необхідно оновити нормативну базу: ухвалити збалансований закон про протидію дезінформації, модернізувати правила державної комунікації та імплементувати для онлайн-платформ кодекси поведінки за зразком Digital Services Act [15]. Одночасно слід розвивати цифрову освіту – запровадити курси медіаграмотності для вчителів, держслужбовців і старшого покоління, а також обов'язкові модулі

інформаційної гігієни в школах і університетах – та підтримувати незалежні аналітичні центри, які відстежують інформаційні загрози. Важливо встановити безперервний аудит державних комунікацій під час криз, регулярно вимірювати проникнення ворожих наративів і рівень довіри до офіційних повідомлень, коригуючи стратегії в режимі реального часу. Водночас баланс між безпекою та свободою слова має залишатися незмінним принципом: лише прозорі державні комунікації, незалежні медіа й активне громадянське суспільство здатні забезпечити стійкість України до гібридних впливів.

Висновки. Інформаційна безпека в умовах гібридної війни перетворилася для України на критичний чинник національної безпеки, соціальної стійкості та демократичної цілісності: якщо після 2014 р. вона була пріоритетом, то з 2022 р. стала питанням виживання держави. Російська агресія супроводжується масованими кампаніями дезінформації, інформаційно-психологічного тиску та маніпулятивного контенту, спрямованими на підрив довіри до інституцій. У відповідь Україна вибудувала багаторівневу систему протидії – від об'єднання телеканалів у єдиний національний марафон до мобілізації громадянського спротиву в цифровому просторі. Досвід засвідчує: ефективна інформаційна оборона можлива лише за умови синергії держави і громадянського суспільства, поєднання стратегічного бачення з гнучким оперативним реагуванням та системного розвитку цифрової грамотності населення. Водночас необхідно зберігати баланс між безпекою і свободою слова, адже саме прозорість комунікацій і незалежні медіа забезпечують демократичну стійкість, не допускаючи авторитарних практик контролю. Україна вже має унікальний набір практик – від потужних OSINT-спільнот до оперативних кризових комунікаційних структур – який може слугувати фундаментом нової, актуалізованої під виклики XXI століття архітектури інформаційної безпеки.

Література:

1. Кабінет Міністрів України. (2022, 18 березня). *Постанова № 195 «Про створення єдиного телемарафону "Єдині новини"»*. https://zakon.rada.gov.ua/laws/show/195-2022-%D0%BF

2. Кабінет Міністрів України. (2023, 12 липня). *Зміцнюємо цифрову безпеку держави: уряд підтримав законопроєкт про заборону використання російських програм* [Прес-реліз]. https://www.kmu.gov.ua/news/zmitsniuiemo-tsyfrovu-bezpeku-derzhavy-uriad-pidtrymav-zakonoproekt-pro-zaboronu-vykorystannia-rosiiskykh-prohram

3. Кузьменко, О. (2020). *Інформаційна безпека як складова національної безпеки України*. Perspectives. http://perspectives.pp.ua/index.php/nauka/article/view/4271

4. Міністерство культури та інформаційної політики України. (2022). *Основні положення законопроєкту «Про протидію дезінформації»* [Презентаційні матеріали]. https://www.kmu.gov.ua/news/mkms-opublikovano-osnovni-polozhennya-zakoproektu-pro-protidiyu-dezinformaciyi

5. Почепцов, Г. (2020). *Сучасні інформаційні війни.* Experts.in.ua. http://www.experts.in.ua/baza/analitic/index.php?ELEMENT_ID=112800

6. Центр стратегічних комунікацій та інформаційної безпеки. (n.d.). *Офіційний сайт*. Отримано 6 серпня 2025 р. з https://spravdi.gov.ua/

7. Чепурний, І. Ю. (Ред.). (2017). *Гібридна війна та інформаційна безпека України*. НІСД.

8. Detector Media. (2023). *Як Росія веде інформаційну війну проти України: тенденції 2022 року*. https://detector.media/

9. European Commission. (2022). *Code of Practice on Disinformation – 2022 Strengthened Code*. https://digital-strategy.ec.europa.eu/en/library/strengthened-code-practice-disinformation

10. European External Action Service. (n.d.). *Delegation to Ukraine* [Офіційний сайт]. Отримано 6 серпня 2025 р. з https://www.eeas.europa.eu/delegations/ukraine_uk?s=232

11. European Parliament & Council. (2022). *Digital Services Act* (Regulation (EU) 2022/2065). https://prighter.com/digital-governance/eu-dsa/

12. EUvsDisinfo. (n.d.). *Official EUvsDisinfo database*. Отримано 6 серпня 2025 р. з https://euvsdisinfo.eu/

13. IREX. (n.d.). *Very Verified: Онлайн-курс із медіаграмотності*. Отримано 6 серпня 2025 р. з https://veryverified.eu/

14. NATO. (2021, 30 листопада). *Гібридна війна: нові загрози, складність, довіра як антидот*. NATO Review. https://www.nato.int/docu/review/uk/articles/2021/11/30/gbridna-vjna-nov-zagrozi-skladnst-dovra-yak-antidot/index.html

15. The Economist. (2022, April). *Ukraine's information warriors: How Kyiv is winning the online war*. https://www.economist.com/

References

1. Cabinet of Ministers of Ukraine. (2022, March 18). *Postanova № 195 «Pro stvorennia yedynoho telemarafonu "Yedyni novyny"»* [Resolution No. 195 "On the creation of the single television marathon 'United News'"]. https://zakon.rada.gov.ua/laws/show/195-2022-%D0%BF [in Ukraine]

2. Cabinet of Ministers of Ukraine. (2023, July 12). *Zmitsniuiemo tsyfrovu bezpeku derzhavy: Uriad pidtrymav zakonoproiekt pro zaboronu vykorystannia rosiiskykh prohram* [Strengthening the state's cyber security: The government supported a draft law banning the use of Russian software] [Press release]. https://www.kmu.gov.ua/news/zmitsniuiemo-tsyfrovu-bezpeku-derzhavy-uriad-pidtrymav-zakonoproekt-pro-zaboronu-vykorystannia-rosiiskykh-prohram [in Ukraine]

3. Kuzmenko, O. (2020). *Informatsiina bezpeka yak skladova natsionalnoi bezpeky Ukrainy* [Information security as a component of Ukraine's national security]. *Perspectives.* http://perspectives.pp.ua/index.php/nauka/article/view/4271 [in Ukraine]

4. Ministry of Culture and Information Policy of Ukraine. (2022). *Osnovni polozhennia zakonoproektu «Pro protydiiu dezinformatsii»* [Key provisions of the draft law "On countering disinformation"] [Presentation materials]. https://www.kmu.gov.ua/news/mkms-opublikovano-osnovni-polozhennya-zakoproektu-pro-protidiyu-dezinformaciyi [in Ukraine]

5. Pocheptsov, G. (2020). *Suchasni informatsiini viiny* [Modern information wars]. Experts.in.ua. http://www.experts.in.ua/baza/analitic/index.php?ELEMENT_ID=112800 [in Ukraine]

6. Centre for Strategic Communications and Information Security. (n.d.). *Ofitsiinyi sait* [Official website]. Retrieved August 6, 2025, from https://spravdi.gov.ua/ [in Ukraine]

7. Chepurnyi, I. Yu. (Ed.). (2017). *Hibrydna viina ta informatsiina bezpeka Ukrainy* [Hybrid warfare and information security of Ukraine]. NISD. [in Ukraine]

8. Detector Media. (2023). *Yak Rosia vede informatsiinu viinu proty Ukrainy: tendentsii 2022 roku* [How Russia is waging an information war against Ukraine: Trends of 2022]. https://detector.media/ [in Ukraine]

9. European Commission. (2022). *Code of Practice on Disinformation – 2022 Strengthened Code.* https://digital-strategy.ec.europa.eu/en/library/strengthened-code-practice-disinformation [in Ukraine]

10. European External Action Service. (n.d.). *Delegation to Ukraine* [Official website]. Retrieved August 6, 2025, from https://www.eeas.europa.eu/delegations/ukraine_uk?s=232 [in Ukraine]

11. European Parliament & Council. (2022). *Digital Services Act* (Regulation (EU) 2022/2065). https://prighter.com/digital-governance/eu-dsa/ [in Ukraine]

12. EUvsDisinfo. (n.d.). *Official EUvsDisinfo database.* Retrieved August 6, 2025, from https://euvsdisinfo.eu/ [in Ukraine]

13. IREX. (n.d.). *Very Verified: On-line course on media literacy.* Retrieved August 6, 2025, from https://veryverified.eu/ [in Ukraine]

14. NATO. (2021, November 30). *Hibrydna viina: novi zahrozy, skladnist, dovira yak antydot* [Hybrid warfare: new threats, complexity, trust as an antidote]. *NATO Review.* https://www.nato.int/docu/review/uk/articles/2021/11/30/gbridna-vjna-nov-zagrozi-skladnst-dovra-yak-antidot/index.html [in Ukraine]

15. The Economist. (2022, April). *Ukraine's information warriors: How Kyiv is winning the online war.* https://www.economist.com/ [in Ukraine]