Рекомендації щодо розроблення механізмів спільного моніторингу та реагування на інформаційно-психологічні атаки противника в умовах війни: очікуваний ефект та шляхи реалізації

Recommendations for Developing Mechanisms for Joint Monitoring and Responding to Enemy Information and Psychological Attacks in Wartime: Expected Effect and Ways of Implementation

Володимир Гурковський [A]
Corresponding author: доктор наук з держ .упр. професор, начальник відділу, e-mail: volodymyr.gurkovskyi@gmail.com, ORCID ID: https://orcid.org/0000-0003-2021-5204

Геннадій Шаповалов [B]
доктор філософії, командувач Сухопутних військ Збройних Сил України, e-mail: volodymyr.gurkovskyi@gmail.com, ORCID ID: https://orcid.org/0000-0002-8979-0648

Юзеф Добровольський [D]
кандидат технічних наук, доцент, заступник начальника кафедри військової підготовки з навчальної роботи – начальник навчальної частини, e-mail: kataza@i.ua, ORCID ID: https://orcid.org/0000-0002-1077-1402

Володимир Коваль [A]
кандидат військових наук, старший науковий співробітник, науковий співробітник, e-mail: vladimerkoval69@gmail.com, ORCID ID: https://orcid.org/0000-0002-6209-6779

Володимир Ремез [C]
доктор філософії, доцент кафедри територіальної оборони, e-mail: remezv93145@gmail.com, ORCID ID: https://orcid.org/0000-0002-2561-1081

Марія Ярмольчик [D]
доктор філософії, начальник науково-дослідної лабораторії, e-mail: LinkinFan357@ukr.net, ORCID ID: https://orcid.org/0000-0001-9917-0189

Volodymyr Gurkovskyi [A]
Corresponding author: Doctor of Public Administration Professor, Head of the Department, e-mail: volodymyr.gurkovskyi@gmail.com, ORCID ID: https://orcid.org/0000-0003-2021-5204

Gennadiy Shapovalov [B]
Doctor of Philosophy, Commander of the Land Forces of the Armed Forces of Ukraine, e-mail: volodymyr.gurkovskyi@gmail.com, ORCID ID: https://orcid.org/0000-0002-8979-0648

Yuzef Dobrovolskyi [D]
Candidate of Technical Sciences, Associate Professor Deputy Chief of the Military Education Department for the Educational Work – Chief of the Educational Unit, e-mail: kataza@i.ua, ORCID ID: https://orcid.org/0000-0002-1077-1402

Volodymyr Koval [A]
Candidate of Military Sciences, Senior Researcher, research fellow e-mail: vladimerkoval69@gmail.com, ORCID ID: https://orcid.org/0000-0002-6209-6779

Volodymyr Remez [C]
Doctor of Philosophy, Associate Professor of the Department of Territorial Defense, e-mail: remezv93145@gmail.com, ORCID ID: https://orcid.org/0000-0002-2561-1081

Mariia Yarmolchyk [D]
Doctor of Philosophy, head of the research laboratory, e-mail: LinkinFan357@ukr.net, ORCID ID: https://orcid.org/0000-0001-9917-0189

[A] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна
[B] Сухопутні війська Збройних Сил України, м. Київ, Україна
[C] Національний університет оборони України, м. Київ, Україна
[D] Кафедра військової підготовки Державного університету "Київський авіаційний університет", м. Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] Ground Forces of the Armed Forces of Ukraine, Kyiv, Ukraine
[C] National Defense University of Ukraine, Kyiv, Ukraine
[D] Department of Military Training, State University "Kyiv Aviation University", Kyiv, Ukraine

Received: April 19, 2026 | Revised: April 28, 2026 | Accepted: April 30, 2026

УДК 351.86:004.77:355.4

DOI: https://doi.org/10.33445/sds.2026.16.2.6

Мета роботи. Розробити рекомендації щодо формування інтегрованого механізму спільного моніторингу та реагування на інформаційно-психологічні атаки противника в умовах війни, з урахуванням інституційних обмежень, багаторівневості управління, балансу оперативної ефективності та легітимності, оцінкою очікуваного ефекту та шляхів реалізації.

Метод дослідження. Змішаний підхід з домінуванням якісних методів: системний аналіз (реконструкція циклу реагування), інституційний аналіз (розбір взаємодій суб'єктів), порівняльний аналіз (український контекст vs. моделі EEAS, OECD, NATO, DISARM), сценарний аналіз (моделювання ситуацій); емпірика на відкритих джерелах

Purpose. To develop recommendations for forming an integrated mechanism of joint monitoring and response to adversary information-psychological attacks in wartime conditions, considering institutional constraints, multi-level governance, balance between operational efficiency and legitimacy, with evaluation of expected effects and implementation pathways.

Method. Mixed-methods approach with qualitative dominance: systemic analysis (reconstruction of response cycle), institutional analysis (examination of subjects' interactions), comparative analysis (Ukrainian context vs. EEAS, OECD, NATO, DISARM models), scenario analysis (modeling situations); empirical basis on open sources (reports 2023–

(звіти 2023–2026 рр., OSINT), з гіпотетичними корекціями через обмежений доступ до даних.

Результати. Запропоновано циклічну модель з 5 елементами (аналітичне ядро, класифікація, протокол реагування, платформа обміну, оцінювання ефективності); гіпотетичне скорочення циклу реагування, зменшення кумулятивного впливу атак; схема багаторівневої структури; кейс-ілюстрація (атака 2023 р.); ризики: фрагментація, витоки, ілюзія вимірюваності.

Теоретична цінність. Обґрунтовано ІПА як системний виклик когнітивній стійкості та управлінській цілісності; інтеграція FIMI та resilience в український контекст; війна як конкуренція управлінських моделей; гіпотези для подальших досліджень (інтеграція AI, вимір когнітивних ефектів).

Тип статті. Аналітична, прикладна.

Ключові слова: інформаційно-психологічні атаки; спільний моніторинг; реагування; гібридні загрози; FIMI; стратегічна стійкість; державне управління.

2026, OSINT), with hypothetical adjustments due to limited data access.

Results. Proposed cyclical model with 5 elements (analytical core, classification, response protocol, exchange platform, effectiveness evaluation); hypothetical reduction of response cycle, mitigation of cumulative attack impacts; multi-level structure scheme; case illustration (2023 attack); risks: fragmentation, leaks, illusion of measurability.

Theoretical value. Conceptualized IPA as a systemic challenge to cognitive resilience and managerial integrity; integration of FIMI and resilience into Ukrainian context; war as competition of governance models; hypotheses for further research (AI integration, measuring cognitive effects).

Article type. Analytical, applied.

Key words: Information-Psychological Attacks; Joint Monitoring; Response; Hybrid Threats; FIMI; Strategic Resilience; Public Administration.

Вступ

У другому кварталі 2022 року в одному з оперативних командувань виникла ситуація, яку важко віднести виключно до інформаційної або управлінської проблеми, а радше до їхнього перетину і цей перетин, до речі, не завжди очевидний на перший погляд. За 48 годин у локальних каналах Telegram та закритих військових чатах поширювався наратив про непідготовленість резерву та приховування втрат. Первинний моніторинг зафіксував аномальну динаміку репостів, проте не існувало формалізованої процедури для передачі цього сигналу на рівень стратегічних комунікацій. Рішення приймалися фрагментарно: деякі структури готували спростування, інші утримувалися, побоюючись розкриття чутливої інформації. Цей випадок ілюструє внутрішню напругу в системі реагування, але чи є він типовим? Можливо, в інших контекстах, як у 2024 році, динаміка інша.

Емпіричний факт, заснований на доступних джерелах, свідчить: у звітах EEAS за 2023–2025 роки зафіксовано системні кампанії FIMI, спрямовані на підрив довіри до військового керівництва держав-мішеней, зокрема через теми втрат, мобілізації та внутрішньої напруги [1]. Аналітичний висновок EEAS полягає в тому, що операції впливу все частіше комбінують відкриті канали з таргетованими в напівзакритих середовищах [1]. Водночас виникає питання про універсальність цього підходу: чи стосується він лише певних контекстів, як у Європі? Наприклад, у третьому звіті EEAS за 2025 рік із матрицею експозиції FIMI підкреслюється ескалація в Молдові та Африці, де російські актори використовують мережі з 16 сайтів і каналів у шести мовах. Це ілюструє гібридність загроз, але чи адаптується такий підхід до українських реалій – тут сумніви, бо наші месенджери додають локальний шар. Український досвід частково відображає цю тенденцію, але з власними акцентами. Дослідження вітчизняних авторів щодо механізмів протидії інформаційно-психологічному впливу на особовий склад фіксують розрив між аналітичним виявленням загрози та процедурою прийняття управлінського рішення [2], хоча не завжди пояснюють причини стійкості цього розриву – можливо, через брак даних. В інших роботах акцент робиться на недостатній формалізації міжвідомчої взаємодії в сфері ІПО, що знижує ефективність у кризовій динаміці [3], проте це радше спостереження, ніж повний аналіз, і в 2025 році з оновленими звітами CSIS про потроєння атак з 2023 по 2024, виникає сумнів: чи не недооцінюємо ми роль гібридних інструментів, як кібератаки на критичну інфраструктуру?

Повертаючись до випадку 2022 року, який є визначальним, оскільки без нього абстракції втрачають ґрунт. Проблема полягала не тільки у виявленні контенту, сигнал було зафіксовано. Складність виникла на рівні узгодження: хто ініціює стратегічне реагування, у які строки, з яким обсягом інформації, і чи можуть комунікаційні підрозділи діяти автономно від оперативного командування? Тут проявляється управлінська дилема, яка не зникає

самостійно. Розглядаючи подібні випадки з 2024–2025 років, як атаки на транспорт і урядові об'єкти в Європі за даними CSIS, стає очевидним, що проблема еволюціонує, включаючи фізичний саботаж, але чи стосується це безпосередньо інформаційно-психологічних атак (далі-ІПА), чи це ширше? З одного боку, швидкість реагування зменшує когнітивний ефект атаки: OECD в доповіді за 2024 рік вказує, що затримка створює інформаційний вакуум, заповнюваний маніпуляціями [4].

З іншого боку, в умовах війни передчасна комунікація може порушити операційну безпеку або підірвати довіру, якщо дані неточні. Це не теоретична суперечність, а практична, як у згаданому випадку і додаючи дані OECD про понад 500 інцидентів FIMI у 2024 році з використанням 25 платформ і 38 000 акаунтів, виникає питання: чи не потребує це перегляду часових меж реагування, хоча в українських умовах це може бути не так просто. Отже, проблема не обмежується браком технічного моніторингу, принаймні не тільки ним; вона має інституційний характер, особливо в умовах воєнного стану. Механізм спільного моніторингу та реагування або відсутній, або діє як паралельні процедури без єдиного контуру, хоча це узагальнення, і в деяких структурах можуть бути винятки. З огляду на ескалацію, описану в третьому звіті EEAS за 2025 рік, де росія та Китай будують цифрові арсенали, це узагальнення може бути недооціненим.

Теоретичні основи дослідження

Початкове припущення, яке часто зустрічається в політичних документах, полягає в ототожненні інформаційно-психологічного впливу з дезінформацією. Однак аналіз матеріалів EEAS показує ширший підхід: FIMI охоплює маніпуляцію, координацію мереж впливу, створення псевдоекспертних платформ, використання дипломатичних і медійних інструментів у комплексі [1]. Це ключове джерело, оскільки воно структурує аналіз як системний, а не ізольований, але в третьому звіті EEAS за 2025 рік з матрицею експозиції FIMI фокус на зовнішніх акторах може ігнорувати внутрішні вразливості. Отже, ІПВ у сучасному воєнному конфлікті це не лише зміст повідомлення, а й інфраструктура поширення та алгоритмічна оптимізація впливу, хоча у воєнних умовах, як в Україні, акцент може зміщуватися на психологічний ефект. Передусім зазначимо термін "FIMI", офіційно введений та активно використовуваний EEAS (дипломатичною службою ЄС). FIMI це офіційний європейський термін для опису скоординованих іноземних маніпуляцій інформацією як інструменту гібридної агресії. FIMI це переважно незаконна модель поведінки, яка загрожує або потенційно може негативно вплинути на цінності, процедури та політичні процеси. Вона характеризується маніпулятивним характером, навмисністю та скоординованістю дій. Але чи завжди навмисність очевидна в українських випадках? Актори: державні або недержавні суб'єкти (часто з проксі всередині чи поза своєю країною), які проводять скоординовані кампанії для маніпуляції інформаційним середовищем.

Фреймворк DISARM як відкритий набір інструментів для аналізу, картографування та протидії дезінфформації, пропонує таксономію операцій впливу, що дозволяє класифікувати дії за фазами від створення активів до експлуатації наративів [5]. DISARM розбиває процеси дезінформацйних кампаній на етапи, подібно до «ланцюгів атак» у кібербезпеці, дозволяючи координувати відповіді. Аналітично це корисно, оскільки розмежовує підготовку і активну фазу, але рамка менш чутлива до політико-інституційного виміру, тобто пояснює "що", але не "як" організувати державну відповідь це обмеження, яке не ігнорується. Оновлення DISARM до версії 2.0 (прототип 2026 року) додає спостереження за активами, як акаунти та платформи, що робить його гнучкішим, але чи не ускладнює застосування в реальному часі воєнних умов? Українські дослідження ІПО, зосереджені на впливі на особовий склад, підкреслюють психологічну складову – деморалізацію, зниження довіри до командування, підрив ідентичності [2].

Цей фокус важливий, але в окремих роботах є тенденція розглядати вплив переважно як зовнішню загрозу, без достатнього аналізу внутрішньої інституційної спроможності реагування [3], що створює певну неповноту. Додаючи дані з CSIS за 2025 рік про ескалацію саботажу (потроєння атак з 2023 по 2024 рік), ця неповнота стає помітнішою. У 2021-2023 рр. в аналітичних матеріалах NATO та його інституцій, зокрема NATO Innovation Hub, сформульовано підхід до Cognitive Warfare як форми боротьби за контроль над когнітивною сферою людини. На відміну від класичного розуміння інформаційних операцій, когнітивна війна трактується як довгостроковий процес впливу на сприйняття, прийняття рішень та поведінкові моделі населення і військовослужбовців, але в українських умовах це може бути не так довгостроково, як у мирний час. Концепція NATO зміщує акцент із реактивного спростування дезінформації на управління когнітивним середовищем. У центрі уваги перебувають нейропсихологічні механізми, цифрова екосистема платформ та вразливості суспільної довіри. Українські підходи до ІПВ традиційно фокусуються на виявленні та нейтралізації інформаційних атак, тоді як підхід NATO передбачає превентивне формування стійкості і ця розбіжність не знімається просто.

Запропонована в статті модель спільного моніторингу та реагування поєднує обидві логіки. Вона зберігає операційний компонент протидії ІПА, але водночас інтегрує елемент стратегічного прогнозування та оцінки когнітивних ефектів, що відповідає рамці Cognitive Warfare. Таким чином, модель може розглядатися як адаптивний варіант імплементації західної концепції в умовах війни високої інтенсивності. Хоча в документах NATO, зокрема StratCom COE, наголос на міжсекторальній інтеграції [11], а запропонований механізм орієнтований насамперед на державну координацію в умовах воєнного стану, що обмежує горизонтальність, але підвищує керованість.

Виникає методологічне напруження: якщо ІПВ трактувати лише як зовнішню атаку, відповідь зводиться до контрпропаганди, і це працює в деяких сценаріях, але не в усіх. Якщо ж бачити його як системний виклик когнітивній стійкості та управлінській цілісності, то в центрі опиняється організація державного механізму, хоча це узагальнення валідне переважно для гібридних конфліктів, як нинішній. З урахуванням доповіді OECD за 2024 рік про необхідність багаторівневих відповідей, це напруження не знімається, а посилюється і повертаючись, OECD пропонує “whole-of-government” підхід [4], формально релевантний для України, але в воєнному стані централізація може знижувати адаптивність на місцях. Отже, виникає суперечність між централізованою моделлю координації та оперативною автономією військових підрозділів. Вирішення не може бути суто адміністративним, воно потребує процедурного балансу, хоча у інтенсивних фазах війни цей баланс хиткий. Додаючи аналіз з доктрини NATO AJP-10.1 за 2023 рік [8], де наголошується на інтеграції StratCom, ця суперечність не зникає. Поняття resilience активно використовується в документах ЄС [1]: воно передбачає не лише реагування, а й здатність системи поглинати удари без втрати функціональності. Аналітично це корисно для оцінки довгострокового ефекту, але в умовах інтенсивних інформаційних атак resilience не може замінити оперативний механізм реагування: стійкість формується роками, тоді як атака розгортається протягом годин. У третьому звіті EEAS за 2025 рік resilience пов’язується з матрицею експозиції FIMI, але це не знімає питання про короткострокове управління. Таким чином, “resilience” – це стратегічна мета, але не інструмент короткострокового управління, і це розмежування важливе, бо інакше можна переоцінити пасивну стійкість. З огляду на звіт CSIS за 2025 рік про фізичні атаки, resilience може потребувати розширення на гібридні загрози. Теоретичний аналіз дозволяє сформулювати кілька робочих положень не як остаточні, а як гіпотези для подальшого розвитку:

ІПА є багаторівневою операцією, що поєднує контент, мережу поширення та когнітивний ефект [1], [5], але в українських умовах мережевий аспект може домінувати через месенджери, як у випадках 2024 року.

Ефективна відповідь потребує міжвідомчого механізму, а не лише інформаційної протидії [4], хоча це не виключає локальних дій, як у оновленому DISARM.Централізація управління підвищує узгодженість, але створює ризик втрати адаптивності, і це напруження не зникає просто, особливо з ескалацією саботажу.

Resilience є необхідною умовою, проте без процедур швидкого реагування вона не забезпечує оперативного ефекту, повертаючись до вступу, як у випадку 2022 року, і додаючи дані 2025 року. Подальший аналіз потребує переходу від теоретичних рамок до методологічного інструментарію дослідження механізму спільного моніторингу, хоча деякі положення вже натякають на методологічні виклики, як інтеграція нових матриць. Мета цієї статті полягає в розробленні рекомендацій щодо формування інтегрованого механізму спільного моніторингу та реагування на ІПА противника в умовах війни, з урахуванням обмежень держави, багаторівневості управління та конфлікту між оперативною ефективністю та інституційною легітимністю.

Це амбітне завдання, і не все вдасться охопити, особливо з урахуванням нових тенденцій 2024–2025 років важливо застерегти: стаття не претендує на побудову завершеної доктрини, частина висновків гіпотетична та потребує емпіричної перевірки. В умовах війни повна відкритість даних обмежена, тому узагальнення спираються на часткові спостереження. З урахуванням нових даних з EEAS та CSIS, гіпотези можуть потребувати корекції вже на 2026-2027 роки.

Методологія дослідження

У 2023 році під час аналізу хвиль інформаційних атак навколо мобілізації стало ясно: виявлення координаційних ознак кампанії не дає відповіді на те, чи була державна реакція структурно адекватною. Дані моніторингу були, рішення ухвалювалися, але без чіткої процедури оцінювання, де саме виникає затримка в управлінському ланцюгу. Додаючи дані з третього звіту EEAS за 2025 рік про ескалацію в 2024 році (понад 500 інцидентів), це спостереження стає ще актуальнішим.

Це спостереження визначило вибір методології не універсальної, а адаптованої до доступних джерел, з урахуванням нових тенденцій. Дослідження спирається на поєднання трьох підходів: системного аналізу для реконструкції циклу реагування від виявлення до стратегічного рішення; інституційного аналізу, щоб розібрати формальні й неформальні правила взаємодії суб'єктів; порівняльного аналізу, зіставляючи український контекст з моделями ЄС та NATO, бо без цього гіпотези залишаться абстрактними.

З інтеграцією матриці експозиції FIMI, порівняння стає глибшим, але чи не надто залежним від західних даних. Це обмеження, яке не знімається. Вихідна гіпотеза полягає в тому, що головний розрив виникає на етапі аналітичної інтерпретації, але після зіставлення з процедурами FIMI EEAS стало очевидно: проблема частіше локалізується на стадії пріоритизації та управлінського рішення [6], і це корекція, яка змінює акцент. В деяких сценаріях, як у третьому звіті EEAS за 2025 рік з прикладами з Африки, це може бути інакше. У звітах EEAS за 2023–2025 роки простежується циклічність: виявлення, аналіз, атрибуція, скоординована відповідь [1, 6] – етапи формалізовані, з розподілом відповідальності; саме ця формалізація створює стійкість, на відміну від технологій самі по собі.

Додаючи матрицю, цикл стає інструментом для експозиції мереж – але в українських умовах це може не працювати так само гладко. Емпіричну основу складають звіти EEAS щодо FIMI [1, 6] як опис процедур, ключовий бо показує, як формалізація перемагає хаос; доповідь OECD за 2024 рік про "whole-of-government" [4], але її ідеалізм для воєнного стану сумнівний;

брифінг ЄП про маніпуляцію онлайн-інформацією [7]; доктрина NATO AJP-10.1 [8] з акцентом на синхронізацію, але обмежена для воєнних умов; українські дослідження ІПО [2], [3] як вторинні, для локальних інсайтів. З CSIS за 2025 рік додаються дані про саботаж, розширюючи емпірику, але з обмеженням на доступність.

Окремо матеріали про російські операції впливу [9], що ілюструють адаптивність противника, поєднуючи інформаційні, кібер- та політичні інструменти, але без повного доступу до деталей, як у тіньовій війні з потроєнням атак це джерело важливе для ілюстрації, але не для повної атрибуції.

Емпіричні факти відокремлено від інтерпретацій: звіти ЄС та NATO як базис для процедур, висновки про застосовність авторський аналіз, не універсальний. З матрицею це розмежування чіткіше, але все ж неповне. Фокус на чотирьох елементах механізму: процедура первинного виявлення; алгоритм класифікації та пріоритизації; модель міжвідомчої координації; система оцінювання ефективності, бо саме вони визначають, де ламається цикл.

Додаючи агентську операціоналізацію DISARM (2026 рік), фокус розширюється на автоматизацію. Технологічні аспекти (великі дані, OSINT) розглядаються лише як впливи на управлінський процес. Самі інструменти не гарантують успіху без інституційного контуру. З даних EEAS про 38 000 акаунтів, це стає критичним, але в українських мережах цифри можуть відрізнятися.

Для оцінки механізму елементи сценарного аналізу: моделювалися короткострокова дезінформаційна хвиля з обмеженим охопленням; кампанія з міжнародним виміром через іноземні медіа; тривала операція з деморалізацією особового складу.

Аналіз показав варіативність ефективності однієї структури в різних сценаріях, ставлячи під сумнів універсальність централізованої моделі. З прикладами з CSIS, як атаки на транспорт, сценарії реалістичніші, але гіпотетичні корекції не знімають сумнівів. У межах статті ефективність механізмів спільного моніторингу визначається як здатність системи забезпечити своєчасне виявлення, узгоджене реагування та вимірюваний вплив на інформаційне середовище. Для операціоналізації цього поняття запропоновано систему показників:

Час ідентифікації загрози (T1) – інтервал між первинною появою ІПА та її фіксацією в системі моніторингу.

Час ухвалення рішення (T2) – період від аналітичної класифікації до формалізованого управлінського рішення.

Час комунікаційного реагування (T3) – інтервал між рішенням і публічним поширенням контрнаративу.

Коефіцієнт координаційної узгодженості (K_c) – частка синхронізованих повідомлень між залученими суб'єктами.

Індекс когнітивного впливу (I_c) – зміна тональності та поведінкових індикаторів цільової аудиторії протягом визначеного періоду.

Ефективність системи пропонується оцінювати інтегральним показником:

$$E = f\,(T1 + T2 + T3,\ K_c,\ I_c).$$

Зменшення часових параметрів при одночасному зростанні K_c та I_c свідчить про підвищення результативності механізму. Така модель дозволяє перейти від декларативного розуміння ефективності до вимірюваної управлінської категорії. хоча I_c часто непрямий, і це створює ілюзію точності.

Результати

На 2024–2025 роки фактично існує кілька паралельних центрів моніторингу та комунікації: військові підрозділи StratCom, СБУ, ЦПД, урядові пресслужби. Формально все регламентовано, але єдиної інструкції чи протоколу щодо ІПА як комплексної події немає. Чому так? Бо кожна

структура фіксує свій фрагмент: одна бачить локальну хвилю, інша – елемент ширшої кампанії. З даних третього звіту EEAS за 2025 рік про 500 інцидентів, фрагментація посилює вразливість, але в українських реаліях це може бути не такою гострою, як у Європі. Досвід ЄС показує інше: Rapid Alert System діє як платформа обміну сигналами між державами-членами [6, 7] ключ не тільки в обміні даними, а в узгодженні інтерпретації загрози.

В українському випадку асинхронність саме тут: відсутність єдиного алгоритму класифікації призводить до розбіжностей у рівні реакції, і це не технічна проблема, а інституційна. Матриця експозиції FIMI додає інструмент для узгодження, але чи інтегрується в нашу систему сумнівно без адаптації. Під час активних фаз бойових дій централізація зростає це об'єктивно, бо воєнний стан вимагає швидких вертикальних рішень. Водночас інформаційні атаки часто локальні, вимагають реакції на місцях. Інакше вакуум заповнюється маніпуляціями за лічені години.

Із звіту CSIS за 2025 рік про потроєння атак, локальність стає критичною, але чи не переоцінюємо ми її в порівнянні з стратегічним рівнем? Доктрина NATO AJP-10.1 (2023 рік з UK Change 1) підкреслює синхронізацію StratCom з оперативним плануванням [8], але доктрина також наголошує на делегуванні на тактичному рівні. В українських умовах ця рівновага хитка: надмірна централізація уповільнює, надмірна автономія ризикує неузгодженими меседжами, і знайти баланс не просто. Оновлення в AJP-10.1 додають акцент на інформаційні операції, але чи достатньо для гібридних загроз не завжди. Звіти про російські операції проти Заходу вказують: відкритість щодо викриття маніпуляцій підвищує довіру до держави [9].

Проте в воєнному контексті розкриття джерел чи деталей може мати зворотний ефект – порушити операційну безпеку. Отже, механізм спільного моніторингу мусить включати критерії рівня публічності реагування, без них кожне рішення ситуативне.

Аналіз підводить до висновку: ключова проблема не в відсутності моніторингу, а в розриві між виявленням і інституційно оформленим рішенням, особливо в умовах високої динаміки. Міжнародні моделі демонструють цінність формалізованого циклу [1, 6, 8], але їхнє механічне перенесення в українські реалії може порушити баланс між централізацією та адаптивністю, бо війна додає змінні, яких у мирних моделях просто немає.

Модель механізму спільного моніторингу та реагування. Практика показує, що спроба повністю централізованої моделі реагування на ІПА неминуче стикається з вимогами оперативної адаптивності, особливо в польових умовах. Збереження фрагментованої системи зберігає розриви між аналітикою та рішенням. Вихід не в крайнощах, а в структурованому, але гнучкому механізмі, який фіксує критичні етапи циклу, залишаючи простір для делегування. З урахуванням третього звіту EEAS за 2025 рік, де експозиція мереж показує ескалацію, модель потребує адаптації до гібридних атак.

Наукова новизна тут в інтеграції матриці FIMI з українським контекстом воєнного стану, що дозволяє гіпотетично скоротити часові лаги за рахунок гібридного військово-цивільного підходу, якого не пропонують існуючі моделі повністю.

Запропонована модель будується на п'яти взаємопов'язаних елементах не як жорстка схема, а як цикл з корекціями.

Перший елемент: інтегроване аналітичне ядро когнітивної безпеки. Його роль не обмежується моніторингом медіа: поєднання OSINT, класифікації за таксономією впливу та первинної оцінки стратегічного ризику. Досвід EEAS (зокрема, матриця в третьому звіті за 2025 рік) демонструє, як систематизація зменшує розбіжності в інтерпретації [6], але в українських умовах центр мусить бути змішаним (військово-цивільним), бо виключно цивільний або виключно військовий не витримає вимог операційної безпеки.

Другий елемент: стандартизована процедура класифікації. DISARM як технічна рамка допомагає уникнути довільних оцінок, встановлюючи фази атаки [5], проте сама таксономія не вирішує пріоритетності. Тому вводиться трирівнева шкала ризику, де ключовий показник –

потенційний вплив на оперативну спроможність чи суспільну довіру; це частково корелює з оцінкою стратегічного ефекту в EEAS [1], але адаптовано до воєнного стану, бо в інтенсивних фазах пріоритети змінюються швидко.

Третій елемент: координаційний протокол реагування. Саме тут найчастіше виникає затримка. Доктрина NATO AJP-10.1 наголошує: синхронізація StratCom з оперативним плануванням має бути процедурною, а не залежати від особистих зв'язків [8].

Тому фіксуються чіткі часові межі передачі сигналу від аналітики до рішення, але не кожна атака автоматично йде в публічну фазу. Рішення про форму відповіді враховує баланс прозорості та операційної безпеки інакше ризикуємо або надто повільно, або надто відкрито.

З AJP-10.1, це включає інформаційні операції, але в українських умовах може бути обмежено. Четвертим елементом є інтегрована цифрова платформа обміну. Rapid Alert System ЄС доводить: спільна база сигналів прискорює узгодження оцінок [12-13].

В українському контексті платформа мусить мати багаторівневий доступ обмежувати чутливі дані, бо інакше або надмірна закритість, або витік [14, 16] це ризик, який не знімається повністю. П'ятий елемент: система оцінювання ефективності. Тут найбільша складність: OECD наголошує на вимірюванні результативності [4], але індикатори когнітивних змін непрямі. Тому комбінуємо кількісні (динаміка поширення наративу, часовий лаг реагування) з якісною експертною оцінкою впливу на цільові аудиторії.

Це не дає повної точності, але створює зворотний зв'язок, якого зараз бракує. Очікуваний ефект: не повне нейтралізування інформаційних атак (це в сучасному середовищі малоймовірно), а зменшення їх кумулятивного впливу. Матеріали про російські операції проти Заходу показують: стійкість визначається швидкістю виявлення та скоординованою відповіддю [9, 19-21].

Отже, головний результат – скорочення циклу "атака – рішення – реакція", але реалізація несе ризики: посилення централізації може послабити автономію на місцях; розширення обміну підвищити вразливість до витоків; ключові показники ефективності створити ілюзію вимірюваності там, де ефект частково латентний. Ці суперечності не знімаються. Їх треба враховувати в нормативному закріпленні.

Модель відображає логіку, обґрунтовану в розділі "Результати дослідження", та базується на п'яти взаємопов'язаних елементах із розподілом за рівнями відповідальності – але ця логіка не ідеальна, бо в реальних умовах війни розподіл може зміщуватися.

Циклічність забезпечує безперервну адаптацію системи та інтеграцію аналітичного зворотного зв'язку у стратегічне планування комунікаційних заходів. Але в інтенсивних фазах це може ламатися.

Представлена модель відображає багаторівневу архітектуру спільного моніторингу та реагування на ІПА в умовах воєнного конфлікту. Її логіка побудована не як ієрархічна замкнена система, а як циклічна структура з елементами постійного коригування рішень. Ключовим є поєднання централізованого стратегічного управління з операційною адаптивністю на рівні виконання.

Схема моделі спільного моніторингу та реагування на інформаційно-психологічні атаки.

1. **Стратегічний Рівень:** РНБО України; Кабінет Міністрів України; Генеральний штаб ЗС України: Функції: формування політики, визначення пріоритетів, нормативне регулювання.

2. **Координаційний (Міжвідомчий) Рівень:** Центр стратегічних комунікацій та інформаційної безпеки (як окрема державна установа); представники силових структур; СБУ, МОУ, Міністерство культури України, експертна рада з питань розбудови в Україні системи державних стратегічних комунікацій, неурядовий Центр стратегічних комунікацій "StrarCom Ukraine". Функції: узгодження дій, обмін інформацією, верифікація загроз.

СТРАТЕГІЧНИЙ РІВЕНЬ Координаційно-управлінський центр (міжвідомча інтеграція, нормативне забезпечення, розподіл повноважень) хоча в практиці це може бути фрагментовано
↓
АНАЛІТИЧНИЙ РІВЕНЬ Моніторинг інформаційного простору (OSINT, SOCMINT, автоматизований збір даних)
↓
Аналітична обробка та класифікація (верифікація, типологізація атак, оцінювання ризику) з ризиком суб'єктивності
↓
ОПЕРАЦІЙНИЙ РІВЕНЬ Прийняття управлінських рішень (визначення сценарію реагування)
↓
Комунікаційне реагування (контрнаративи, стратегічні повідомлення, оцінювання ефективності ↺ повернення до моніторингу)

Рисунок: Інтегрована модель спільного моніторингу та реагування
Джерело: розроблено авторами

3. **Операційний Рівень:** Аналітичні підрозділи; OSINT-групи; Центри інформаційно-психологічної безпеки, підрозділи з стратегічних комунікацій, підрозділи ІПСО. Функції: моніторинг, ідентифікація наративів, оцінка впливу.

4. **Рівень Реагування:** Публічні комунікації; Контрнаративи; Інформаційно-психологічні операції; Технічне блокування деструктивного контенту.

5. **Зворотний Зв'язок:** Оцінка ефективності; Корекція алгоритмів; Оновлення протоколів; взаємодії.

Запропонована схема демонструє, що ефективність протидії визначається не лише швидкістю реагування, а здатністю інституцій забезпечити узгодженість між стратегічними установками та польовими діями. Наявність зворотного зв'язку виступає механізмом інституційного навчання, що дозволяє мінімізувати накопичення управлінських помилок в умовах високої динаміки інформаційного середовища. Хоча навчання не завжди швидке. Водночас модель залишає відкритими питання балансу між централізацією та гнучкістю. Надмірна регламентація може знизити адаптивність реагування, тоді як надмірна децентралізація створює ризики фрагментації комунікаційної позиції держави. Практична реалізація механізму потребує чітких протоколів координації, визначення відповідальності та ресурсного забезпечення на кожному рівні.

Проведемо кейс-ілюстрацію координації реагування на ІПА на прикладі "втрати довіри до військово-політичного керівництва" (2023 р.) [19].

У другій половині 2023 року в українському та міжнародному інформаційному просторі фіксувалося системне поширення наративів про нібито “конфлікт між військовим і політичним керівництвом України”, що супроводжувалося маніпулятивними інтерпретаціями кадрових рішень і фрагментарних публічних заяв. Кампанія активно тиражувалася через мережу анонімних телеграм-каналів, проксі-медіа та російські державні ресурси.

Аналітичні звіти ISW та ICDS фіксували синхронність меседжів і повторюваність формулювань, що свідчило про централізовану координацію.

Мета атаки полягала не у створенні нової інформації, а у когнітивному посиленні внутрішньої недовіри, деморалізації військовослужбовців та впливі на міжнародну підтримку [20-21] це джерела важливі для ілюстрації, але обмежені західним поглядом. Розглянемо, як би спрацювала запропонована модель спільного моніторингу гіпотетично, бо реальні дані часткові.

1. Моніторинг (T1) OSINT-моніторинг фіксує:

різке зростання частоти згадувань ключових слів;

однакові формулювання у різних джерелах;

синхронний запуск меседжів на різних платформах.

Скорочення T1 (часу ідентифікації) є критичним, оскільки перші 24-48 годин визначають масштаб когнітивного ефекту, але в реальності це може бути довше.

2. Аналітична класифікація (T2) Аналітичний блок встановлює:

наратив має ознаки скоординованої ІПА;

аудиторія впливу: внутрішня та міжнародна;

стратегічна мета: підрив довіри та формування образу “нестабільності управління”. Паралельно формується прогноз вторинних ефектів:

деморалізація;

зниження довіри партнерів;

активізація бот-мереж – прогноз не завжди точний.

3. Управлінське рішення Координаційний рівень визначає сценарій реагування:

уніфікована позиція державних органів;

синхронізація публічних коментарів;

превентивне інформування міжнародних партнерів, але синхронізація ризикує затримками.

4. Комунікаційне реагування (T3) Реалізується багаторівнева стратегія:

офіційні заяви;

роз’яснювальні матеріали;

включення незалежних експертів;

адресна робота з іноземними медіа.

Одночасно здійснюється повторний моніторинг тональності інформаційного середовища (I_c) – I_c непрямий. Емпіричний ефект (умовна ілюстрація на основі відкритих даних). За відкритими оцінками аналітичних центрів, пікове зростання згадувань відповідного наративу тривало 5-7 днів, після чого інтенсивність поширення знизилась. Це свідчить про часткову нейтралізацію когнітивного ефекту через швидке публічне реагування, але чи повна нейтралізація?

У рамках запропонованої моделі можна було б зафіксувати: T1 – до 6 годин; T2 – до 12 годин; T3 – до 24 годин; зниження негативної тональності на 30-40 % протягом тижня; · відсутність довготривалого ефекту в міжнародному інформаційному полі – гіпотетично.

Для нашого дослідження кейс має таке аналітичне значення: ІПА була спрямована не на дезінформацію фактичного характеру, а на когнітивну інтерпретацію реальних подій. Реагування вимагало міжвідомчої координації, а не лише спростування.

Швидкість синхронізації повідомлень стала ключовим фактором стабілізації інформаційного поля, але в інших кейсах це може не працювати. Цей приклад продемонстрував, що ефективність механізму протидії визначається не лише здатністю виявити атаку, а й здатністю узгодити позицію різних центрів впливу та зменшити когнітивну невизначеність, хоча невизначеність лишається.

Обговорення

Отримані результати підтверджують гіпотезу про визначальну роль інтегрованого механізму спільного моніторингу та реагування на інформаційно-психологічні атаки, однак їх інтерпретація потребує уточнення з урахуванням інституційних та методологічних обмежень. Зокрема, запропонована модель демонструє потенціал скорочення часових лагів реагування (T1–T3) та підвищення координаційної узгодженості, що корелює з підходами “whole-of-government” та FIMI. Водночас припущення про універсальність ефективності централізованої координації є частково спрощеним, оскільки в умовах воєнного стану зростає напруження між централізацією та операційною автономією.

Критичним аспектом є ризик редукції складного когнітивного впливу до вимірюваних показників, що може створювати ілюзію точності оцінювання ефективності. Крім того, запропонована модель недостатньо враховує роль неформальних комунікаційних мереж і поведінкових факторів, які суттєво впливають на динаміку ІПА. Альтернативно, механізм слід розглядати не як завершену систему, а як адаптивну рамку, чутливу до контексту та типу загроз.

Таким чином, результати дослідження узгоджуються з сучасними міжнародними підходами, але водночас виявляють необхідність їх подальшої адаптації до умов високої інтенсивності гібридного конфлікту та емпіричної верифікації.

Висновки

Проведене дослідження підтвердило, що ефективність протидії ІПА у воєнний період прямо залежить від інституціоналізованого механізму спільного моніторингу, який інтегрує аналітичні, управлінські та комунікаційні функції в єдиний цикл прийняття рішень. Розрізнені системи спостереження без координаційного центру не забезпечують скорочення часу реагування та не формують стабільного зворотного зв’язку.

Запропонована модель демонструє, що результативність підвищується за наявності трьох умов: нормативно закріпленого розподілу відповідальності; стандартизованої процедури оцінювання загроз; інтегрованої системи вимірювання комунікаційного ефекту. Відсутність хоча б одного з цих компонентів призводить до фрагментації реагування та втрати керованості інформаційного середовища.

Аналітичний блок повинен функціонувати як окреме ядро із доступом до міжвідомчих даних. Його завдання полягає не лише у фіксації атак, а й у прогнозуванні сценаріїв розвитку інформаційних кампаній противника. Це дозволяє переходити від реактивної моделі до проактивної.

Практична реалізація запропонованих механізмів передбачає створення постійного координаційного органу з чітко визначеними повноваженнями, інтеграцію OSINT-інструментів, впровадження KPI ефективності комунікацій та регулярну міжвідомчу оцінку ризиків. За таких умов система здатна скоротити час реагування, підвищити узгодженість повідомлень та мінімізувати когнітивний вплив противника на цільові аудиторії.

Отримані результати можуть бути використані під час удосконалення комунікаційної стратегії ЗС України, розроблення стандартів міжвідомчої взаємодії та формування національної системи інформаційно-психологічної стійкості, але з корекціями на нові дані 2026 року.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Council of the European Union. A Strategic Compass for Security and Defence. Brussels, 2022. 47 p. URL: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.
2. CSIS. Russia's Shadow War Against the West. Washington, DC: Center for Strategic and International Studies, 2025. 54 p. URL: https://www.csis.org/analysis/russias-shadow-war-against-west.
3. EEAS. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats, March 2025 (with FIMI Exposure Matrix). URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf
4. EEAS. 2nd and 3rd EEAS FIMI Threat Reports, 2023–2025. URL: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en (дата доступу: 24.02.2026).
5. European External Action Service. EU vs Disinformation Annual Report 2023. Brussels: EEAS, 2024. 112 p. URL: https://www.eeas.europa.eu/eeas/annual-reports_en (дата доступу: 24.02.2026).
6. European Parliament. Online Information Manipulation and Information Integrity, Briefing, 2024. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI(2024)762416_EN.pdf (дата доступу: 24.02.2026).
7. Helmus T. C., Bodine-Baron E., Radin A. Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe. Santa Monica, CA: RAND Corporation, 2022. 96 p. URL: https://www.rand.org/pubs/research_reports/RR2237.html (дата доступу: 24.02.2026).
8. Institute for the Study of War. Russian Offensive Campaign Assessment. Washington, DC, 2025. URL: https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-december-31-2025 (дата доступу: 24.02.2026).
9. Ministry of Defence of Ukraine. Strategic Communications Doctrine of the Armed Forces of Ukraine. Kyiv, 2023. 64 p. URL: https://mod.gov.ua/en/about-us/ministry-staff-en/department-of-strategic-communications (дата доступу: 24.02.2026).
10. NATO. Allied Joint Doctrine for Strategic Communications (AJP-10.1), Edition A Version 1 with UK Change 1, 2023. URL: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf (дата доступу: 24.02.2026).
11. NATO Strategic Communications Centre of Excellence. Countering Disinformation: Lessons from Ukraine. Riga: NATO StratCom COE, 2023. 78 p. URL: https://stratcomcoe.org/publications?tid%5B%5D=30 (дата доступу: 24.02.2026).
12. OECD. Disinformation and Russia's War of Aggression Against Ukraine: Threats and Governance Responses. Paris: OECD Publishing, 2023. 84 p. URL: https://www.oecd.org/en/publications/2022/11/disinformation-and-russia-s-war-of-aggression-against-ukraine_8b596425.html (дата доступу: 24.02.2026).

13. OECD. Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity, 2024. URL: https://www.oecd.org/en/publications/2024/03/facts-not-fakes-tackling-disinformation-strengthening-information-integrity_ff96d19f.html.
14. Salnikova O., Pavlenko V., Tverdokhlib O. Strategic communications in countering hybrid threats. Information & Security: An International Journal. 2019. Vol. 43, No. 2. P. 153–168. URL: https://www.researchgate.net/publication/350063259_Strategic_communications_as_a_key_factor_in_countering_hybrid_threats.
15. DISARM Framework. Taxonomy of Influence Operations, arXiv:2601.15109v2, February 2026. URL: https://arxiv.org/abs/2601.15109.
16. Інформаційно-психологічні операції в контексті інформаційної безпеки України. Науковий журнал, PDF. 2025. URL: http://il.ippi.org.ua/article/view/324704.
17. Кузьменкова К. С. Дезінформація як інструмент гібридної війни: теоретико-методологічний аналіз. Держава та регіони. Серія: Державне управління. 2025. № 1. С. 45–55.
18. Механізм протидії негативному інформаційно-психологічному впливу на особовий склад ЗС України. Наукове видання, PDF. 2020. URL: https://journal-hnups.com.ua/index.php/nitps/article/view/154 (дата доступу: 24.02.2026).
19. Institute for the Study of War. URL: https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment_10-11/.
20. Institute for the Study of War. URL: https://understandingwar.org.
21. Russia's War in Ukraine: Russia's Attempts to Undermine Mobilisation. International Centre for Defence and Security. URL: https://icds.ee/en/russias-attempts-to-undermine-mobilisation.

References

1. Council of the European Union. A Strategic Compass for Security and Defence. Brussels, 2022. 47 p. URL: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.
2. CSIS. Russia's Shadow War Against the West. Washington, DC: Center for Strategic and International Studies, 2025. 54 p. URL: https://www.csis.org/analysis/russias-shadow-war-against-west.
3. EEAS. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats, March 2025 (with FIMI Exposure Matrix). URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.
4. EEAS. 2nd and 3rd EEAS FIMI Threat Reports, 2023–2025. URL: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en (accessed: 24.02.2026).
5. European External Action Service. EU vs Disinformation Annual Report 2023. Brussels: EEAS, 2024. 112 p. URL: https://www.eeas.europa.eu/eeas/annual-reports_en (accessed: 24.02.2026).
6. European Parliament. Online Information Manipulation and Information Integrity, Briefing, 2024. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI(2024)762416_EN.pdf (accessed: 24.02.2026).
7. Helmus T. C., Bodine-Baron E., Radin A. Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe. Santa Monica, CA: RAND Corporation, 2022. 96 p. URL: https://www.rand.org/pubs/research_reports/RR2237.html (accessed: 24.02.2026).
8. Institute for the Study of War. Russian Offensive Campaign Assessment. Washington, DC, 2025. URL: https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-december-31-2025 (accessed: 24.02.2026).
9. Ministry of Defence of Ukraine. Strategic Communications Doctrine of the Armed Forces of Ukraine. Kyiv, 2023. 64 p. URL: https://mod.gov.ua/en/about-us/ministry-staff-en/department-of-strategic-communications (accessed: 24.02.2026).

10. NATO. Allied Joint Doctrine for Strategic Communications (AJP-10.1), Edition A Version 1 with UK Change 1, 2023. URL: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf (accessed: 24.02.2026).
11. NATO Strategic Communications Centre of Excellence. Countering Disinformation: Lessons from Ukraine. Riga: NATO StratCom COE, 2023. 78 p. URL: https://stratcomcoe.org/publications?tid%5B%5D=30 (accessed: 24.02.2026).
12. OECD. Disinformation and Russia's War of Aggression Against Ukraine: Threats and Governance Responses. Paris: OECD Publishing, 2023. 84 p. URL: https://www.oecd.org/en/publications/2022/11/disinformation-and-russia-s-war-of-aggression-against-ukraine_8b596425.html (accessed: 24.02.2026).
13. OECD. Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity, 2024. URL: https://www.oecd.org/en/publications/2024/03/facts-not-fakes-tackling-disinformation-strengthening-information-integrity_ff96d19f.html (accessed: 24.02.2026).
14. Salnikova O., Pavlenko V., Tverdokhlib O. Strategic communications in countering hybrid threats. Information & Security: An International Journal. 2019. Vol. 43, No. 2. P. 153–168. URL: https://www.researchgate.net/publication/350063259_Strategic_communications_as_a_key_factor_in_countering_hybrid_threats (accessed: 24.02.2026).
15. DISARM Framework. Taxonomy of Influence Operations, arXiv:2601.15109v2, February 2026. URL: https://arxiv.org/abs/2601.15109.
16. Informatsiino-psykholohichni operatsii v konteksti informatsiinoi bezpeky Ukrainy. Naukovyi zhurnal, PDF. 2025. URL: http://il.ippi.org.ua/article/view/324704 (accessed: 24.02.2026).
17. Kuzmenkova K. S. Dezinformatsiia yak instrument hibrydnoi viiny: teoretyko-metodolohichnyi analiz. Derzhava ta rehiony. Seriia: Derzhavne upravlinnia. 2025. No. 1. S. 45–55.
18. Mekhanizm protydii nehatyvnomu informatsiino-psykholohichnomu vplyvu na osobovyi sklad ZS Ukrainy. Naukove vydannia, PDF. 2020. URL: https://journal-hnups.com.ua/index.php/nitps/article/view/154 (accessed: 24.02.2026).
19. Institute for the Study of War. URL: https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment_10-11/ (accessed: 24.02.2026).
20. Institute for the Study of War. URL: https://understandingwar.org.
21. Russia's War in Ukraine: Russia's Attempts to Undermine Mobilisation. International Centre for Defence and Security. URL: https://icds.ee/en/russias-attempts-to-undermine-mobilisation.

This is an open access journal and all published articles are licensed under a Creative Commons «Attribution» 4.0.