

ПОЛІТОЛОГІЯ



Стаття та будь-який пов'язаний з нею опублікований матеріал поширюється за ліцензією Creative Commons Attribution License (CC BY 4.0).
The article and any related published material are licensed under the Creative Commons Attribution License (CC BY 4.0).

УДК 327.5:355.01:316.774(477)

DOI: <https://doi.org/10.17721/1728-2217.2026.66.97-103>

Володимир ГУРКОВСЬКИЙ, д-р наук з держ. управл., проф.

ORCID ID: 0000-0003-2021-5204

e-mail: Vladimir.gurkovskyi@gmail.com

Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

Сергій ІЛЬНИЦЬКИЙ, ст. наук. співроб.

ORCID ID: 0009-0009-3000-9034

e-mail: anzhx175wf@icloud.com

Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

Рена МАРУТЯН, д-р наук з держ. управл., доц.

ORCID ID: 0000-0001-9184-1590

e-mail: renata_kiev@i.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

ТРАНСФОРМАЦІЯ СТРАТЕГІЧНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ РФ ПРОТИ УКРАЇНИ (2024–2025): ТЕХНОЛОГІЧНИЙ ВИМІР ТА ПРОАКТИВНА ПРОТИДІЯ

Вступ. Сучасні інформаційно-психологічні операції (ІПСО) Росії остаточно трансформувалися з допоміжного інструменту на системотвірний елемент воєнного мистецтва, інтегрований у стратегічне планування. Дослідження заповнює критичну наукову прогалину щодо недооцінювання технологічного фактора генеративного штучного інтелекту (ШІ) як інструменту "цифрової окупації", що в період 2024–2025 років став основою для переходу Москви до моделі "індустріалізованого виробництва дезінформації". В архітектурі гібридної агресії Кремля інформаційно-комунікативна сфера остаточно легітимізована як повноцінний театр воєнних дій. Стратегічна мета агресора змістилася від кількісних показників охоплення аудиторії до якісних маркерів деструкції – штучного провокування системних уразливостей, паралічу інститутів ухвалення рішень і цілеспрямованого розмивання суспільного консенсусу щодо національної оборони.

Методи. Методологія ґрунтується на системному міждисциплінарному аналізі. Застосовано метод аналізу конкретних кейсів (Case Study) для реконструкції операцій "мапаганда", "майдан-3" і "чорнобильська провокація". Використано аналіз обчислювальної пропаганди (Computational Analysis) через наукову інтерпретацію даних цифрової криміналістики розвідок OpenMinds та DFRLab, що дало змогу верифікувати активність автоматизованих мереж. Аналітичною рамкою дослідження є модель "Unified Kill Chain", яка дала змогу структурувати повний цикл інформаційного нападу – від розгортання інфраструктури до досягнення стратегічного ефекту когнітивного виснаження аудиторії.

Результати. Установлено, що ключовим елементом стратегії РФ стала еволюція операції "майдан-3" у тривалу кампанію з підготовки "кризи легітимності" травня 2025 року. Доведено, що генеративний ШІ використовується динамічно, адаптуючи наративи під актуальні заходи діяльності військово-політичного керівництва України в конкретні періоди. Виявлено феномен "алгоритмічного терору" – синхронізацію ШІ-атак із реальними обстрілами енергосистеми для максимізації паніки. Виокремлено та класифіковано інструменти ірраціонального наративного впливу, що використовуються як когнітивний шум для маскування довгострокових стратегічних операцій дискредитації.

Висновки. Аналіз підтверджує неспроможність чинної реактивної моделі протидії (debunking), оскільки ШІ-атаки забезпечують ворогу "право першого враження". Обґрунтовано необхідність переходу України до проактивної моделі інформаційно-когнітивної безпеки, заснованої на механізмах випереджувального викриття (pre-bunking). Це здійснюється за рахунок ідентифікації технічної інфраструктури ворога на етапі її розгортання та розкриття тактичних патернів (TTPs) до моменту масового викиду дезінформації. Тільки розвиток наступальних інформаційних спроможностей і перенесення когнітивного протистояння на територію ворога дасть змогу нейтралізувати загрозу стратегічній дестабілізації держави.

Ключові слова: ІПСО, мапаганда, гібридна війна, дезінформація, когнітивна стійкість, штучний інтелект, національна безпека, наративна війна, військово-стратегічна перевага, стратегічна дестабілізація, інформаційні кампанії, стратегічні комунікації.

Вступ

Сучасний етап російсько-української війни характеризується остаточною трансформацією ІПСО з допоміжного інструменту на самостійний і визначальний елемент стратегічного впливу, що безпосередньо корегує хід воєнних кампаній (EUvsDisinfo, 2025). У 2024–2025 роках Росія розгорнула безпрецедентну за масштабами кампанію, яка ознаменувала перехід до системної моделі "індустріалізованого виробництва дезінформації". Кампанія була інтегрована в загальну архітектуру гібридної війни (Evans et al., 2025). Цей етап визначається використанням генеративного штучного інтелекту, розгалужених

мереж анонімних телеграм-каналів і маніпуляцією глобальними політичними процесами для стратегічної дестабілізації України. Москва розглядає інформаційний простір як повноцінне поле бою, де успіх операції вимірюється не лише охопленням аудиторії, а реальною деградацією системи державного управління та обороноздатності (EUvsDisinfo, 2025).

Вектор ворожих зусиль у досліджуваний період зосереджувався на проведенні масштабних комплексних операцій впливу, серед яких чільне місце посіли цілеспрямовані кампанії з дискредитації інституційної легітимності вищих органів влади та штучного моделювання

© Гурковський Володимир, Ільницький Сергій, Марутян Рена, 2026

прецедентів ядерного шантажу. Специфіка архітектури цих проєктів полягала в навмисному зміщенні акцентів на імітацію внутрішньоукраїнського суспільно-політичного порядку денного та штучне підбурювання латентних суперечностей. Окремим деструктивним напрямом когнітивного тиску стало таргетування особового складу Збройних Сил України з метою розмивання засад єдиності початковості, дезорієнтації військового управління та штучного створення умов для зниження загальної обороноздатності держави на лінії бойового зіткнення (Kondrat, 2026).

У роботі проаналізовано технологічні спроможності бот-мереж нового покоління, що забезпечують алгоритмічну автоматизацію та промислове масштабування дезінформаційних кампаній за допомогою штучного інтелекту.

Поряд із класичними маніпуляціями, у досліджуваний період зафіксовано масштабне застосування тактики "абсурдної дезінформації". Подібні деструктивні наративи інструменталізовані не для переконання об'єкта у вірогідності штучно створеного факту, а для провокування когнітивного виснаження суспільства та руйнування раціональних фільтрів критичного сприйняття (Paul, & Matthews, 2016; Starbird, 2019). У такий спосіб ірраціональний інформаційний шум виконує функцію операції прикриття, на тлі якої агресор приховано впроваджує довгострокові стратегічні меседжі, спрямовані на дискредитацію військово-політичного керівництва України та підлив інституційної довіри (Rid, 2020; Williams, & McCulloch, 2023).

Досвід протиробства у досліджуваний період засвідчив, що ворожі спецслужби почали ретельніше координувати часові рамки інформаційних атак із глобальним політичним календарем. Кампанії з дискредитації України на міжнародній арені будувалися навколо штучно згенерованих звинувачень у неконтрольованості об'єктів критичної інфраструктури, що спрямовувалося на зрив консолідованих рішень союзників під час ключових самітів (Starbird, 2019). Цей підхід посилювався технологіями візуального маніпулювання, зокрема масштабуванням спеціально скоригованих картографічних матеріалів. Завдяки штучному перебільшенню локальних успіхів окупаційних військ ворог намагався трансформувати незначні тактичні зміни в масштабні інформаційні кризи, розраховані на когнітивне виснаження аудиторії та параліч стратегічного планування партнерів (Paul, & Matthews, 2016; Evans et al., 2025). Таким чином, постає комплексна наукова проблема, що полягає у необхідності осмислення спеціальних інформаційних дій Росії не лише як медійного явища, а як повноцінного компонента ІПсО у стратегії війни та воєнного мистецтва, інтегрованого у стратегічне планування. Критичною науковою прогалиною залишається технологічний фактор, зокрема роль генеративного штучного інтелекту як інструменту "цифрової окупації", який раніше розглядався як допоміжний засіб, а взимку 2024–2025 років перетворився на системотвірний елемент інформаційної агресії. Дослідження цього періоду дає змогу виявити закономірності розвитку операцій, інтегрованих безпосередньо у сферу військового управління, що є критично важливим для формування проактивної стратегії національної безпеки.

Метою статті є концептуальне визначення структури, технологічного інструментарію та архітектури наративів інформаційно-психологічних операцій агресора, спрямованих на тривалу делегітимізацію інститутів державного управління. Відповідно до мети поставлено такі завдання: деконструувати механізми деструктивного впливу на систему військового керівництва та суспільну

стійкість за допомогою координованих мереж генеративного штучного інтелекту, а також обґрунтувати параметри переходу України від реактивної моделі протидії до проактивної стратегії у когнітивній сфері.

Наукова новизна дослідження полягає у класифікації методів, за допомогою яких технології штучного інтелекту адаптуються під конкретні інформаційні тренди, що таргетують уразливі точки державного менеджменту, а також у теоретичному моделюванні механізмів випереджувального викриття (*pre-bunking*) як фундаментальної основи забезпечення стратегічної стійкості держави (Paul, & Matthews, 2016; Starbird, 2019; Williams, & McCulloch, 2023).

Методи

Методологія дослідження ґрунтується на комплексному та міждисциплінарному аналізі, що поєднує інструментарій військової теорії, політичних наук та аналізу цифрових технологій. Для досягнення поставленої мети й отримання верифікованих результатів було застосовано такий апарат наукових методів.

По-перше, метод аналізу конкретних кейсів (*Case Study*) використано для детальної деконструкції та вивчення механізмів реалізації провідних інформаційних операцій РФ узимку 2024–2025 років, зокрема інцидентів ядерного шантажу та кампаній військової "мапаганди". Це дало змогу простежити, як технологічна база та деструктивні наративи попередніх масштабних кампаній Кремля адаптуються ворогом під тривалі стратегічні завдання з підриву інституційної легітимності органів влади.

По-друге, метод аналізу документів та емпіричного узагальнення покладено в основу вивчення аналітичних матеріалів цифрової криміналістики, представлених дослідницькими центрами *OpenMinds* та *Digital Forensic Research Lab (DFRLab)*. Завдяки критичній інтерпретації готових результатів мережевого аналізу зазначених агенцій було верифіковано архітектурні параметри розгортання і топологію роботизованих ШІ-мереж, що застосовувалися у межах досліджуваних операцій впливу (Vosoughi та ін., 2018).

По-третє, використання аналітичних моделей тактичного аналізу онлайн-операцій, розроблених Європейською службою зовнішніх справ (EEAS), а саме рамки "уніфікованого ланцюга ураження" (*Unified Kill Chain*), дало змогу типізувати й покроково структурувати повний цикл інформаційної агресії – від фази проєктування адаптивного контенту великими мовними моделями до моменту настання деструктивних наслідків у вигляді емоційного виснаження цільових аудиторій (Paul, & Matthews, 2016; Starbird, 2019).

По-четверте, структурно-функціональний і порівняльний аналіз залучено для дослідження російських операцій впливу як цілісної архітектури, що підпорядкована законам операційного мистецтва. Зіставлення глобальних воєнно-стратегічних звітів Інституту дослідження війни (*ISW*) із поточним медійним контентом ворога дало змогу виявити кореляцію між подіями на лінії бойового зіткнення та спрямованістю психологічного тиску на особовий склад Збройних Сил України з метою розмивання засад єдиності початковості (Kondrat, 2026).

Нарешті, метод теоретичного узагальнення та логічного синтезу покладено в основу переосмислення чинної реактивної моделі протидії (*debunking*). Це забезпечило підґрунтя для авторської концептуалізації та управлінського обґрунтування параметрів переходу України до проактивної стратегії когнітивної безпеки, що базується на механізмах випереджувального викриття (*pre-bunking*) сценаріїв ворожих маніпуляцій (Rid, 2020; Evans et al., 2025).

Огляд літератури. Дослідження проблематики інформаційно-психологічного протиборства та наративної війни в умовах повномасштабної агресії РФ набули вагомого теоретичного розвитку. Водночас стрімка технологічна еволюція інструментарію Кремля постійно створює розрив між накопиченими емпіричними даними та їхнім концептуальним осмисленням у межах безпекового менеджменту (European External Action Service, 2024).

У західній аналітичній традиції вивчення операцій впливу здійснюється крізь призму інтеграції мілітарних та інформаційних компонентів. Провідні інституції, зокрема Інститут дослідження війни (*Institute for the Study of War – ISW*), фокусуються на макроаналізі воєнно-стратегічного контексту, розглядаючи інформаційні кампанії як підпорядкований елемент загального оперативного задуму командування РФ на театрі воєнних дій (Evans et al., 2025). Технічний вимір деструктивної активності в мережі досліджується Лабораторією цифрових криміналістичних досліджень (*Digital Forensic Research Lab – DFRLab*), яка спеціалізується на верифікації аномальної поведінки бот-мереж і розкритті прихованих кіберінфраструктур (Starbird, 2019). Класифікацію та динаміку еволюції ворожих наративів на загальноєвропейському рівні здійснює спеціалізована платформа *EUvsDisinfo*. Упроваджені нею аналітичні рамки "айсберг" та "галактика дезінформації" дають змогу розмежувати публічні (видимі) прояви когнітивних атак у медіапросторі та латентні процеси алгоритмічного маніпулювання (European External Action Service, 2024).

Фундаментальне значення для розуміння природи сучасних загрозотвірних чинників мають праці П. Померанцева, який обґрунтовує концепт "війни проти реальності" (Pomerantsev, 2019). Автор доводить, що ключовою метою інформаційного тиску є не стільки переконання об'єкта впливу у вірогідності альтернативних фактів, скільки формування тотального когнітивного гігілізу та руйнування раціональних фільтрів сприйняття. Теоретичне підґрунтя для дослідження роботизованих мереж закладено у працях С. Вуллі та Ф. Говарда, які через термін "обчислювальна пропаганда" (*Computational Propaganda*) розкрили механізми автоматизації маніпулятивних потоків (Woolley, & Howard, 2018). У свою чергу, модель "потоків брехні" (*Firehose of Falsehood*), розроблена дослідниками корпорації RAND, детально описує російську тактику швидкого, багатоканального та ірраціонального поширення контенту, орієнтованого на ментальне виснаження аудиторії (Paul, & Matthews, 2016). Окрему наукову вагу мають сучасні розвідки щодо феномена "розпаду істини" (*Truth Decay*), де зміщення акцентів з об'єктивних даних на емоційні тригери розглядається як прямий виклик національній безпеці (Williams, & McCulloch, 2023).

Вітчизняний аналітичний дискурс, представлений дослідженнями Центру протидії дезінформації при РНБО України та Центру стратегічних комунікацій та інформаційної безпеки, безпосередньо враховує практичний досвід протидії сучасним гібридним загрозам. Проте значна частина існуючих публікацій має переважно емпірико-описовий характер, зосереджуючись на фіксації та експрес-спростуванні (*debunking*) поточних фейків. Поза фокусом глибокого теоретичного аналізу часто залишається трансформація інформаційного протиборства у високотехнологічну індустрію, де генеративний штучний інтелект стає базовою платформою для "цифрової окупації" національних сегментів мережі (Rid, 2020).

Наявні моніторингові звіти переважно фіксують кількісні параметри активності ШІ-агентів, зокрема у теле-

грам-просторі (Vosoughi та ін., 2018). При цьому спостерігається очевидний брак наукових праць, присвячених вивченню інтеграції інформаційних ударів безпосередньо у сферу державного та військового управління, де метою є параліч процесу ухвалення рішень і руйнування засад єдиноначальності. З огляду на це, традиційна реактивна парадигма протидії виявляється неспроможною нейтралізувати автоматизовані високошвидкісні загрози. Це зумовлює нагальну потребу розробки нових моделей когнітивної безпеки, заснованих на управлінських принципах проактивності та інституційного пребанкінгу (*pre-bunking*).

Результати

Дослідження інформаційного ландшафту взимку 2024–2025 років дало змогу верифікувати остаточний перехід РФ від моделі ручного керування інформаційними атаками до комплексної стратегії "індустріалізованого виробництва дезінформації", інтегрованої у воєнне планування Кремля (EUvsDisinfo, 2025). Отримані емпіричні дані дають змогу заповнити критичну наукову прогалину щодо оцінки технологічного фактора штучного інтелекту, доводячи, що він перетворюється з допоміжним інструментом на наскрізний елемент "цифрової окупації" національного медіапростору (European External Action Service, 2025).

У межах вивчення стратегічного рівня когнітивної агресії проаналізовано еволюцію операції "майдан-3". Дослідження зафіксувало її трансформацію з тактичної кампанії весни 2024 року, спрямованої на первинне розхитування суспільно-політичної ситуації в Україні, на тривалий інструмент підготовки штучної "кризи легітимності" органів влади (Kondrat, 2026). Ресурсне забезпечення зазначеного проєкту координувалося на вищому рівні керівництва РФ і спрямовувалося на впровадження інтегрованих наративів про "незаконність" українських державних інституцій і провокування внутрішніх конфліктів серед еліт (Kondrat, 2026; Evans et al., 2024). Окремим деструктивним елементом цієї операції в досліджуваній період стали інструментальний аналіз і маніпуляція темою "мирних планів", що використовувалася для дискредитації офіційної дипломатичної позиції Києва на міжнародній арені (EUvsDisinfo, 2024; Бідочко та ін., 2025).

У ході наукової інтерпретації матеріалів технічного моніторингу обчислювальної пропаганди було деталізовано реальні масштаби автоматизації в месенджері Telegram. На основі аналізу верифікованих даних цифрової криміналістики встановлено функціонування скоординованої мережі з 3634 унікальних акаунтів, керованих алгоритмами генеративного штучного інтелекту (Adam, & Rothbardt, 2025). Згідно з відкритими звітами дослідницьких центрів OpenMinds та DFRLab, за аналізований період цією інфраструктурою було згенеровано понад 3 млн коментарів, таргетованих на формування штучного "керованого консенсусу" (Adam, & Rothbardt, 2025). Аналіз цих емпіричних даних дав змогу виявити механізм когнітивного маніпулювання через так званий "LLM-грумінг" (*LLM grooming*), методологічні засади якого в контексті генеративних загроз описані у профільних дослідженнях штучного інтелекту (Danet, 2025). За цією технологією великі мовні моделі попередньо адаптуються для імітації специфічних культурних, ментальних і лінгвістичних патернів української аудиторії, що дає змогу ШІ-агентам мімікрувати під природний голос спільноти. Зазначена технологія дала змогу російським суб'єктам впливу витіснити природні дискусії в локальних чатах і каналах тимчасово окупованих територій, де прокрем-

лівські меседжі штучно позиціонувалися як думка місцевої більшості (Adam, & Rothbardt, 2025).

Дослідження виявило феномен "алгоритмічного терору", який характеризує інтеграцію засобів ІПсО безпосередньо у сферу воєнного управління. Ворог використовував ШІ-платформи для цілодобового семантичного моніторингу українських соціальних мереж і синхронізації інформаційних ударів із реальними ракетно-дроновими обстрілами критичної інфраструктури (European External Action Service, 2025). Точний розрахунок часу викидання панічних повідомлень під час аварійних відключень електроенергії дав змогу агресору максимізувати психологічний тиск на цивільне населення. Синхронно зафіксовано цілеспрямоване таргетування особового складу Збройних Сил України через поширення згенерованого контенту про демографічний колапс, штучні фейки щодо мобілізації жінок і зниження призовного віку, що мало на меті дискредитацію рішень командування та розмивання засад єдиноначальності (Evans et al., 2024).

Важливим результатом дослідження стало розкриття специфіки застосування тактики "абсурдної дезінформації" через концепт "розпаду істини" (*Truth Decay*). Установлено, що масоване тиражування ірраціональних історій (зокрема сфабрикованих за допомогою ШІ-кейсів про купівлю вілли Гітлера або елітного автомобіля Bugatti за кошти західної допомоги) виступало як операція прикриття (Bidochko та ін., 2025; EUvsDisinfo, 2025; Центр протидії дезінформації, 2025). Головна мета таких операцій полягала не в переконанні суб'єкта у вірогідності вигаданого факту, а в інженерній поляризації суспільного простору, максимізації емоційного виснаження та руйнуванні раціональних фільтрів критичного сприйняття (Evans et al., 2024; Williams, & McCulloch, 2023). На тлі створеного емоційного шуму та когнітивного переважання аудиторії Москва приховано впроваджувала довгострокові стратегічні меседжі про "зовнішнє управління" та позбавлення України політичної суб'єктності (EUvsDisinfo, 2025).

У воєнно-географічному вимірі дослідження деконструвало інструмент "мапаганди" як специфічну модель візуальних маніпуляцій. Зіставлення оперативних звітів Інституту дослідження війни (ISW) із пропагандистськими картографічними матеріалами РФ виявило навмисне викривлення просторових даних: незначне просування російських окупаційних військ (близько 0,8 % території за рік) через скориговані графічні схеми подавалося як "масштабний колапс фронту" у районах Покровська та Курахового (Evans et al., 2025). Кульмінаційним етапом координованого тиску на міжнародну спільноту визначено "чорнобильську провокацію", зафіксовану 14 лютого 2025 року. Через автоматизовані ШІ-мережі, які одночасно охопили 1,3 млн користувачів, здійснювалася спроба звинуватити Україну в ядерному тероризмі із чітким розрахунком на зрив міжнародних безпекових переговорів напередодні Мюнхенської конференції (Adam, & Rothbardt, 2025).

Таким чином, верифіковані результати дослідження доводять обмежену ефективність чинної реактивної моделі протидії гібридним загрозам. Виявлена висока швидкість, автономність і масштабованість ШІ-атак Кремля робить інструменти простого спростування фейків (*debunking*) запізнілими, оскільки ворог у когнітивній сфері завойовує "право першого враження" (Kuźnicka-Błaszowska, & Kostyuk, 2025). Це науково обґрунтовує управлінську потребу невідкладного переходу України до проактивної стратегії випереджувального викриття (*pre-bunking*), здатної нейтралізувати деструктивні

сценарії ще на етапі їхнього технологічного проектування (Rehan, 2025).

Дискусія і висновки

Проведене дослідження підтверджує наукову гіпотезу про те, що ІПсО РФ зазнали глибокої якісної трансформації, остаточно перетворившись на наскрізний інструмент досягнення воєнно-стратегічної переваги (European External Action Service, 2025; EUvsDisinfo, 2025). Отримані результати свідчать, що в сучасній практиці гібридного протистояння інформаційний вплив втратив суто допоміжну функцію, еволюціонувавши у самостійний компонент операційного мистецтва, що інтегрований у загальний задум стратегічного планування Кремля. Перехід агресора до "індустріалізованого виробництва дезінформації" означає, що успіх операцій віднедавна оцінюється не лінійними показниками охоплення аудиторії (кількістю переглядів), а деструктивними маркерами деградації обороноздатності та паралічу системи державного управління України (EUvsDisinfo, 2025).

Ключовим чинником деструктивності ворожих операцій у досліджуваній період визначено технологічний прорив у реалізації концепції "цифрової окупації" комунікаційного простору. Наше дослідження довело, що широке впровадження генеративного штучного інтелекту та координованих бот-платформ дало змогу агресору моделювати консенсусні середовища, витісняючи органічний суспільний дискурс (Adam, & Rothbardt, 2025). Алгоритмічна гнучкість сучасних мовних моделей забезпечує ворогу високу швидкість реакції: автоматизовані мережі здійснюють безперервний семантичний моніторинг українського медіаполя, що дає змогу динамічно адаптувати маніпулятивні наративи під конкретні часові проміжки й актуальні кроки військово-політичного керівництва України (Rehan, 2025).

Важливим теоретичним узагальненням статті є деконструкція операційних патернів ІПсО РФ через адаптовану аналітичну рамку "уніфікованого ланцюга ураження" (Unified Kill Chain) (Pols, 2023). Верифікований емпіричний матеріал дає змогу простежити повний цикл інформаційної агресії – від етапу збирання розвідувальних даних та "LLM-грумінгу" до фази масованого "затоплення" (flooding) середовища деструктивним контентом із метою досягнення когнітивного виснаження аудиторії (Danet, 2025; European External Action Service, 2024). Контекстуальний аналіз кампаній зими 2024–2025 років унаочнює високу адаптивність цієї інфраструктури до динаміки подій як на лінії фронту, так і в тилу.

Зафіксований феномен "алгоритмічного терору" демонструє прямий зв'язок між кінетичними ударами по енергетичній інфраструктурі та координованим поширенням панічних наративів у регіональних чатах із метою максимізації психоемоційного тиску на цивільне населення (Center for Countering Disinformation, 2025). Водночас здатність ШІ-мереж до миттєвої зміни оперативних завдань підтвердилася під час подій у російському прикордонні, коли бот-платформи миттєво переорієнтувалися на імітацію "голосу місцевих жителів" для приховування управлінського хаосу в російському прикордонні, реалізуючи на практиці алгоритми прихованого когнітивного впливу та мовної мімікрії (Dadier та ін., 2025). Особливу загрозу становить спрямованість операції "майдан-3" на розмивання інституційної легітимності влади та дискредитацію мобілізаційних процесів через фейки про умови призову, що підтверджує намір агресора спровокувати внутрішній спротив у підрозділах ЗСУ та підірвати засади єдиноначальності (Evans et al., 2024; Kondrat, 2026). Окрім цього, хронологічний збіг

півкових навантажень "чорнобильської провокації" з проведенням Мюнхенської безпекової конференції доводить інструменталізацію штучних техногенних загроз для дискредитації України в очах західних еліт (Adam, & Rothbardt, 2025).

Особливе значення для розвитку теорії безпекового менеджменту має верифікація моделі "поток брехні" (firehose of falsehood) у поєднанні з концептом "розпаду істини" (Truth Decay) (Paul, & Matthews, 2016; Williams, & McCulloch, 2023). Наше дослідження доводить, що навмисне комбінування псевдораціональних аргументів, таких як маніпуляції воєнною статистикою чи "мирними планами" з очевидною "абсурдною дезінформацією" про нібито набуття елітного майна керівництвом держави, виконує функцію когнітивного перевантаження суспільства (EUvsDisinfo, 2024; 2025). Поки ресурси медіаспільноти витрачаються на спростування та верифікацію ірраціональних фейків, агресор приховано впроваджує довгострокові деструктивні смисли щодо "зовнішнього управління" та безальтернативності капітуляції (Бідочко та ін., 2025; EUvsDisinfo, 2025). Кінцевою метою такої "нарративної окупації" є не переконання аудиторії, а формування стійкого когнітивного нігілізму, за якого руйнується сама віра в існування об'єктивної істини, що робить державні інститути вразливими до стратегічної дестабілізації (Pomerantsev, 2019; European External Action Service, 2026).

Підсумовуючи результати проведеного дослідження, можна сформулювати низку обґрунтованих висновків і рекомендацій для сфери державного управління.

Сучасні ІПСО РФ остаточно еволюціонували у високо-технологічну індустрію, де генеративний штучний інтелект стає базовою технологічною платформою. Це дає змогу ворогу здійснювати промислове, контекстуально точне масштабування деструктивних нарративів, які адаптуються під актуальну діяльність військово-політичного керівництва України, з метою руйнування суспільної єдності та підризу морально-психологічного стану особового складу ЗСУ.

Панівна реактивна модель протидії, заснована на класичному спростуванні інформації (debunking), у сучасних реаліях є обмежено ефективною. За умов високої швидкості, автономності та багатоканальності ШІ-атак агресор автоматично здобуває "право першого враження". Коли сфабрикований контент охоплює мільйонну аудиторію до оприлюднення офіційної позиції органів влади, подальші роз'яснення не здатні повноцінно нівелювати завдану когнітивну шкоду, що свідчить про кризу чинних інструментів інформаційного захисту.

Забезпечення стратегічної стійкості держави потребує невідкладного концептуального переходу системи державного управління до проактивної моделі когнітивної безпеки, інтегрованої у загальну архітектуру національної оборони. Практична реалізація цього підходу має базуватися на механізмах випереджувального викриття (pre-bunking). Ця стратегія передбачає ідентифікацію технологічних патернів (TTPs) і розгортання інфраструктури ворога ще на етапі проектування операцій, що дає змогу заздалегідь інформувати суспільство про потенційні сценарії маніпуляцій і формувати стійкий інституційний імунітет.

З метою підвищення ефективності державного менеджменту в когнітивній сфері рекомендовано змістити акценти оборонної політики з пасивної інфо-оборони на стратегію активного стримування. Це передбачає розробку та впровадження наступальних спроможностей в інформаційному просторі, спрямованих на перенесення

когнітивного протистояння на територію агресора. Синхронізація заходів стратегічних комунікацій із превентивними діями у кіберпросторі дасть змогу руйнувати мобілізаційний потенціал ворога, підривати внутрішню стійкість його системи управління та максимізувати для керівництва Кремля ціну продовження гібридної агресії.

Внесок авторів: Володимир Гурковський – концептуалізація (спільна розробка поняття "цифрова окупація"), методологія (системний аналіз інформаційних впливів Кремля як багаторівневої структури), написання (перегляд і редагування – теоретичне обґрунтування проактивної моделі інформаційної безпеки); Сергій Ільницький – формальний аналіз (ідентифікація типових операційних патернів ворога на основі мережевого моніторингу активності ботів у Telegram), валідація даних (детальна реконструкція хронології операцій "майдан-3", "мапаганда" та "чорнобильська провокація"), написання (оригінальна чернетка – систематизація стратегічних нарративів і цілей агресора); Рена Марутян – експертиза з питань когнітивної безпеки та державної стратегії, синтез отриманих даних для обґрунтування неефективності реактивних методів захисту та розроблення пропозицій щодо переходу до проактивної моделі протидії російським ІПСО, стратегічна візія, що передбачає розвиток наступальних інформаційних спроможностей України.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

- Бідочко, Л., Задирака, К., & Пилипенко, А. (2025, Листопад 27). "Зрада інтересів росії": як пропаганда використовує "план Трампа" для продовження війни. MediaSapiens. <https://ms.detector.media/informatsiini-kanali/post/38670/2025-11-27-zrada-interesiv-rosii-yak-propaganda-vykorystovuiye-plan-trampa-dlya-prodovzhennya-viyny/>
- Центр протидії дезінформації. (2025, February). Фейк про купівлю президентом України Володимиром Зеленським будинку Гітлера. <https://cpd.gov.ua/international-direction/yevropa/fejki-pro-kupivlyu-prezidentom-ukrayiny-volodymyrom-zelenskym-budynku-gitlera/>
- EUvsDisinfo. (2025, December 16). 5 5 підступних дезінформаційних нарративів, які поширює Кремль. <https://euvsdisinfo.eu/ua/5-5-pidstupnih-dezininformatsiynih-narativ/>
- EUvsDisinfo. (2025, December 29). Огляд 2025 року: битва за нарратив. <https://euvsdisinfo.eu/ua/oglyad-2025-roku-bitva-za-narativ/>
- Adam, I., & Rothbardt, S. (2025, April). Narrative and provocation: What Telegram had to say about the February attack on Chornobyl nuclear plant. DFRLab. <https://dfrlab.org/2025/04/25/narrative-and-provocation-what-telegram-had-to-say-about-the-february-attack-against-chornobyl-npp/>
- Danet, D. (2025). LLM Grooming: A New Cognitive Threat to Generative AI. HAL Science. <https://hal.science/hal-05241525v1/document>
- European External Action Service. (2024, January). 2nd EEAS report on foreign information manipulation and interference threats: Exposing the architecture of FIMI operations. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en
- European External Action Service. (2025, March). 3rd EEAS report on foreign information manipulation and interference threats: Exposing the architecture of FIMI operations. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en
- European External Action Service. (2026, March 12). 4th EEAS annual report on foreign information manipulation and interference threats. https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en
- EUvsDisinfo. (2024, December 21). 1,000 and 4,000 days of deception: Russia's evolving information manipulation. <https://euvsdisinfo.eu/1-000-and-4-000-days-of-deception-russias-evolving-information-manipulation/>
- EUvsDisinfo. (2024, December 26). 1,000 and 4,000 days of Russia weaponising information in its war against Ukraine. <https://euvsdisinfo.eu/1000-and-4000-days-of-russia-weaponising-information-in-its-war-against-ukraine/>
- Evans, A., Wolkov, N., Gasparyan, D., Gibson, O., Hird, K., & Kagan, F. W. (2025, February 12). Russian offensive campaign assessment. Institute for the Study of War. <https://www.understandingwar.org/wp-content/uploads/2025/04/Russian20Offensive20Campaign20Assessment2C20February20122C2020252028229.pdf>
- Evans, A., Wolkov, N., Gasparyan, D., Gibson, O., Mappes, G., Trotter, N., Runkel, W., & Stepanenko, K. (2024, December 4). Russian offensive campaign assessment. Institute for the Study of War. <https://www.understandingwar.org/wp-content/uploads/2025/04/Russian20Offensive20Campaign20Assessment2C20December20242C20202420PDF-compressed.pdf>

Kondrat, A. (2026). *Special operation Maidan-3: New details of the disinformation campaign*. Svidomi. <https://svidomi.in.ua/en/page/special-operation-maidan-3-new-details-of-the-disinformation-campaign>

Kuźnicka-Błaszowska, D., & Kostyuk, N. (2025). Emerging need to regulate deepfakes in international law: The Russo-Ukrainian war as an example. *Journal of Cybersecurity*, 11(1), tyaf008. <https://doi.org/10.1093/cybsec/tyaf008>

Paul, C., & Matthews, M. (2016). The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it. RAND Corporation. <https://www.rand.org/pubs/perspectives/PE198.html>

Pols, G. (2023). *The Unified Kill Chain*. Cyber Security Academy. <https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf>

Pomerantsev, P. (2019). *This is not propaganda: Adventures in the war against reality*. PublicAffairs.

Rehan, T. (2025, February 10). AI-driven disinformation campaigns on Twitter (X) in the Russia-Ukraine war. *Small Wars Journal*. <https://smallwarsjournal.com/2025/10/02/ai-driven-disinformation/>

Starbird K. (2019). *Disinformation's spread: bots, trolls and all of us*. Nature. <https://www.nature.com/articles/d41586-019-02235-x>

Williams, H. J., & McCulloch, C. (2023). *Truth decay and national security: Intersections, outcomes, and potential solutions*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/perspectives/PEA100/PEA112-2/RAND_PEA112-2.pdf

References

Adam, I., & Rothbardt, S. (2025, April). *Narrative and provocation: What Telegram had to say about the February attack on Chernobyl nuclear plant*. DFRLab. <https://dfrlab.org/2025/04/25/narrative-and-provocation-what-telegram-had-to-say-about-the-february-attack-against-chernobyl-npp/>

Bidochko, L., Zadyraka, K., & Pylypenko, A. (2025, November 27). *"Betrayal of Russia's Interests": How Propaganda Uses "Trump's Plan" to Continue the War*. MediaSapiens [in Ukrainian]. <https://ms.detector.media/informatsiini-kanali/post/38670/2025-11-27-zrada-interesiv-rosii-yak-propaganda-vykorystovuie-plan-trampa-dlya-prodovzheniya-viyny/>

Center for Counteracting Disinformation. (2025, February). *Fake about the purchase of Hitler's house by Ukrainian President Volodymyr Zelensky* [in Ukrainian]. <https://cpd.gov.ua/international-direction/yevropa/fej-k-pro-kupivlyu-prezydentom-ukrayiny-volodymyrom-zelenskym-budynku-gitlera/>

Danet, D. (2025). *LLM Grooming: A New Cognitive Threat to Generative AI*. HAL Science. <https://hal.science/hal-05241525v1/document>

European External Action Service. (2024, January). *2nd EEAS report on foreign information manipulation and interference threats: Exposing the architecture of FIMI operations*. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

European External Action Service. (2025, March). *3rd EEAS report on foreign information manipulation and interference threats: Exposing the architecture of FIMI operations*. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

European External Action Service. (2026, March 12). *4th EEAS annual report on foreign information manipulation and interference threats*. https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en

Volodymyr HURKOVSKYI, DSc (Public Administration), Prof.

ORCID ID: 0000-0003-2021-5204

e-mail: Vladimir.gurkovskiy@gmail.com

Central Scientific Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine

Serhii ILNYTSKYI, Senior Researcher

ORCID ID: 0009-0009-3000-9034

e-mail: anzhx175wf@icloud.com

Central Scientific Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine

Rena MARUTIAN, DSc (Public Administration), Assoc. Prof.

ORCID ID: 0000-0001-9184-1590

e-mail: renata_kiev@i.ua

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

TRANSFORMATION OF RUSSIA'S STRATEGIC INFORMATION OPERATIONS AGAINST UKRAINE (2024–2025): THE TECHNOLOGICAL DIMENSION AND PROACTIVE RESPONSE MECHANISMS

Background. Modern information and psychological operations (PSYOP) of Russia have finally transformed from an auxiliary tool into a system-forming element of the art of war integrated into strategic planning. The study fills a critical scientific gap regarding the underestimation of the technological factor of generative artificial intelligence (AI) as a tool of "digital occupation", which during 2024–2025 became the basis for Moscow's transition to the model of "industrialized disinformation production". Within the architecture of the Kremlin's hybrid aggression, the information and communication sphere has finally been legitimized as a full-fledged theatre of military operations. The strategic goal of the aggressor has shifted from quantitative indicators of audience coverage to qualitative markers of destruction, namely the artificial provocation of systemic vulnerabilities, paralysis of decision-making institutions, and the purposeful erosion of public consensus on national defence.

Methods. The methodology is based on a systemic interdisciplinary analysis. The case study method was applied to reconstruct the operations "Mapaganda", "Maidan-3" and "Chernobyl provocation". Computational propaganda analysis was employed through the scientific interpretation of digital forensics data from OpenMinds and DFRLab, which made it possible to verify the activity of automated networks. The analytical framework of the study is the "Unified Kill Chain" model, which enabled the structuring of the full cycle of an information attack – from infrastructure deployment to achieving the strategic effect of audience cognitive exhaustion.

Results. It was established that the key element of the Russian strategy was the evolution of the "Maidan-3" operation into a long-term campaign aimed at preparing the "crisis of legitimacy" in May 2025. It was proven that generative AI is used dynamically, adapting narratives to

EUvsDisinfo. (2024, December 21). *1,000 and 4,000 days of deception: Russia's evolving information manipulation*. <https://euvsdisinfo.eu/1-000-and-4-000-days-of-deception-russias-evolving-information-manipulation/>

EUvsDisinfo. (2024, December 26). *1,000 and 4,000 days of Russia weaponising information in its war against Ukraine*. <https://euvsdisinfo.eu/1000-and-4000-days-of-russia-weaponising-information-in-its-war-against-ukraine/>

EUvsDisinfo. (2025, December 16). *5 insidious disinformation narratives spread by the Kremlin*. <https://euvsdisinfo.eu/ua/5-підступних-дезінформаційних-наратив/> [in Ukrainian]

EUvsDisinfo. (2025, December 29). *2025 review: battle for the narrative* [in Ukrainian]. <https://euvsdisinfo.eu/ua/огляд-2025-року-битва-за-наратив/>

Evans, A., Wolkov, N., Gasparyan, D., Gibson, O., Hird, K., & Kagan, F. W. (2025, February 12). *Russian offensive campaign assessment*. Institute for the Study of War. <https://www.understandingwar.org/wp-content/uploads/2025/04/Russian20Offensive20Campaign20Assessment2C20February20122C2020252028229.pdf>

Evans, A., Wolkov, N., Gasparyan, D., Gibson, O., Mappes, G., Trotter, N., Runkel, W., & Stepanenko, K. (2024, December 4). *Russian offensive campaign assessment*. Institute for the Study of War. <https://www.understandingwar.org/wp-content/uploads/2025/04/Russian20Offensive20Campaign20Assessment2C20December2042C20202420PDF-compressed.pdf>

Kondrat, A. (2026). *Special operation Maidan-3: New details of the disinformation campaign*. Svidomi. <https://svidomi.in.ua/en/page/special-operation-maidan-3-new-details-of-the-disinformation-campaign>

Kuźnicka-Błaszowska, D., & Kostyuk, N. (2025). Emerging need to regulate deepfakes in international law: The Russo-Ukrainian war as an example. *Journal of Cybersecurity*, 11(1), tyaf008. <https://doi.org/10.1093/cybsec/tyaf008>

Paul, C., & Matthews, M. (2016). The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it. RAND Corporation. <https://www.rand.org/pubs/perspectives/PE198.html>

Pols, G. (2023). *The Unified Kill Chain*. Cyber Security Academy. <https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf>

Pomerantsev, P. (2019). *This is not propaganda: Adventures in the war against reality*. PublicAffairs.

Rehan, T. (2025, February 10). AI-driven disinformation campaigns on Twitter (X) in the Russia-Ukraine war. *Small Wars Journal*. <https://smallwarsjournal.com/2025/10/02/ai-driven-disinformation/>

Starbird K. (2019). *Disinformation's spread: bots, trolls and all of us*. Nature. <https://www.nature.com/articles/d41586-019-02235-x>

Williams, H. J., & McCulloch, C. (2023). *Truth decay and national security: Intersections, outcomes, and potential solutions*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/perspectives/PEA100/PEA112-2/RAND_PEA112-2.pdf

Отримано редакцією журналу / Received: 30.04.26

Прорецензовано / Revised: 11.05.26

Схвалено до друку / Accepted: 21.05.26

Опубліковано / Published: 30.06.26

current activities of Ukraine's military-political leadership during specific periods. The phenomenon of "algorithmic terror" was identified, referring to the synchronization of AI attacks with real attacks on the power system to maximize panic. The irrational narrative influence tools used as cognitive noise to mask long-term strategic discredit operations were identified and classified.

C o n c l u s i o n s . The analysis confirms the failure of the current reactive countermeasure model (debunking), since AI attacks provide the enemy with the "right of first impression". The necessity of Ukraine's transition to a proactive model of information and cognitive security based on pre-bunking mechanisms was substantiated. This is achieved by identifying the enemy's technical infrastructure at the stage of its deployment and revealing tactical patterns (TTPs) before the mass injection of disinformation. Only the development of offensive information capabilities and the transfer of cognitive confrontation onto the enemy's territory will make it possible to neutralize the threat of the state's strategic destabilization.

K e y w o r d s : Information and Psychological operations (PSYOP), propaganda, hybrid warfare, disinformation, cognitive resilience, artificial intelligence, national security, narrative warfare, military-strategic advantage, strategic destabilization, information campaigns, strategic communications.

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.