DOI: 10.20535/2522-1078.2026.1(19).356053
ROR: 03wfca816
УДК 070:004:316.77(477)

Надходження до редакції: 20.03.2026
Прийняття до друку: 24.04.2026

Осадчук Р. Ю.
аспірант Могилянської школи журналістики та старший викладач кафедри міжнародних відносин Національного університету «Києво-Могилянська академія», м. Київ, Україна
r.osadchuk@ukma.edu.ua
ORCID: 0000-0002-4552-1227

Osadchuk R.
PhD candidate at Mohyla Journalism School and senior lecturer at the department of International Relations of National University of Kyiv-Mohyla Academy, Kyiv, Ukraine
r.osadchuk@ukma.edu.ua
ORCID: 0000-0002-4552-1227

ТЕОРЕТИЧНА РАМКА ДОСЛІДЖЕННЯ СУЧАСНИХ ДЕЗІНФОРМАЦІЙНИХ ОПЕРАЦІЙ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

THEORETICAL FRAMEWORK FOR THE STUDY OF CONTEMPORARY DISINFORMATION OPERATIONS OF THE RUSSIAN FEDERATION

Анотація. Інформаційне середовище стало ключовою ареною геополітичного змагання, де державні актори дедалі активніше використовують цифрові платформи для формування громадської думки та підриву довіри до інституцій всередині та за кордоном. РФ постійно використовує дезінформацію та інформаційні операції для впливу на демократичні країни та інституції, що особливо виявляється у гібридній війні проти України з 2014 року та після широкомасштабного вторгнення у 2022 році. Незважаючи на стрімке зростання уваги до дезінформації як об'єкта дослідження, велика кількість досліджень фокусується на окремих аспектах, роблячи їх ізольованими. Ця стаття пропонує підхід до усунення структурної прогалини в дослідженнях дезінформації, тобто спосіб подолати аналітичну фрагментарність між таксономічними, емпіричними та когнітивними вимірами. Автор пропонує достосувати трирівневу аналітичну рамку для вивчення російських інформаційних операцій проти України. Адаптована з військових доктрин США та НАТО з інформаційних операцій, ця рамка розмежовує технічний, наративний та когнітивний рівні, а також теоретизує функціональні зв'язки між ними. Такий підхід надає можливість всебічного аналізу інформаційних операцій як цілісного продукту, який використовує специфічні способи комунікації, генерує ефективні повідомлення й цілить у точкові вразливості цільової аудиторії задля досягнення впливу, коригуючи та використовуючи всі три рівні одночасно. Рамку апробовано емпірично на прикладі аналізу російської дезінформаційної кампанії про «продаж зброї». Ця кампанія була запущена проросійськими Телеграм-каналами у квітні 2022 року та є актуальною донині. Приклад демонструє, як еволюція наративу, адаптація доставки та когнітивне таргетування діють синхронізовано, взаємно при тому підсилюючись. Результати дослідження сприяють формуванню

більш інтегрованого підходу до вивчення інформаційних операцій і пропонують модель для аналізу майбутніх дезінформаційних кампаній, спрямованих проти України та союзних країн, що може сприяти більш ефективній протидії таким операціям у майбутньому.

Ключові слова: дезінформація, методи дослідження, інформаційні операції, соціальні медіа, журналістика, пропаганда, Україна, РФ

Abstract. The information environment has become a key battleground in geopolitical competition, with state actors increasingly using digital platforms to influence public opinion and undermine institutional trust both within and beyond the country's borders. The Russian Federation has consistently used disinformation and information operations to influence democratic countries and institutions, which is particularly evident in the hybrid war against Ukraine since 2014 and after the full-scale invasion in 2022. Despite the rapid growth of attention to disinformation as an object of study, a large number of studies focus on individual aspects, making them isolated. This article proposes an approach to remove a persistent structural gap in disinformation research, namely, a way to overcome fragmentation across taxonomic, empirical, and cognitive dimensions. The author proposes to use a three-level analytical framework for studying Russian information operations against Ukraine, which is adapted from U.S. and NATO IO military doctrine. The framework distinguishes between the technical, narrative, and cognitive levels. It also theorizes the functional connections among these levels. Such an approach enables a comprehensive analysis of information operations as a holistic product that uses specific communication methods, generates effective messages, and targets the target audience's vulnerabilities to achieve impact by simultaneously adjusting and using all three levels. The framework is empirically validated through an analysis of the Russian "weapons sales" disinformation campaign, launched by pro-Russian Telegram channel, which first surfaced in April 2022 and remains ongoing. The case demonstrates how narrative evolution, delivery adaptation, and cognitive targeting operate in concert, amplifying each other. The findings contribute to a more integrated approach to information operations research. They also provide a model for analyzing future disinformation campaigns targeting Ukraine and allied countries, which could contribute to more effective ways of countering such operations in the future.

Keywords: disinformation, research methods, information operations, social media, journalism, propaganda, Ukraine, Russia

Вступ. Сучасне інформаційне середовище стало одним з головних просторів геополітичного змагання. Державні актори дедалі активніше експлуатують цифрові платформи та медіа для формування громадської думки, підриву довіри до інституцій та послаблення спроможності опонента ухвалювати самостійні рішення, вдаючись до гібридизації підходу

до комунікацій та інформаційних операцій [11; 17]. Україна відчула цей вплив щонайменше з 2014 року від російської гібридної окупації Криму, але повномасштабне вторгнення РФ в Україну у лютому 2022 року надало російській дезінформації додаткову динаміку. Російські гібридні інформаційні операції стали невід'ємною частиною кінетичної війни, оскільки спрямовані одночасно на внутрішню аудиторію РФ для підтримки війни, а також на зовнішні аудиторії, маючи метою виграти кінетичну війну.

Концепції пропаганди та інформаційних операцій у XXI ст. зазнали істотних трансформацій у зв'язку з розвитком технологій. Вивченням пропаганди й інформаційних операцій займалися іноземні та українські науковці, зокрема Г. Ласвел, Ж. Еллюль, Г. Йоветт, В. О'Доннел, І. Пачепа, Дж. Стенлі, К. Джайлз, С. Вулі, Т. Рід, Я. Каленський, Г. Почепцов, Є. Магда та ін., проте більшість дослідників пропаганди й дезінформації стикаються зі стійкою структурною проблемою: дослідження, як правило, концентруються на одному або двох з кількох вимірів, не будучи інтегрованими в єдину аналітичну систему. Кожен з цих методологічних вимірів фіксує реальний аспект функціонування пропаганди, проте ці виміри мало коли й ким застосовуються в комплексі.

Натомість підхід до підготовки інформаційних операцій на трьох рівнях, що використовується військовими США [21], видається більш ефективним для академічного й практичного аналізу таких операцій. Ця стаття, відповідно, покликана усунути названу прогалину й об'єднати різні академічні та військові дослідження задля комплексного аналізу російських інформаційних операцій, спираючись на дослідження пропаганди з різних аспектів, а також апробувати запропонований тут метод емпірично на прикладі дезінформаційної операції.

Мета статті — концептуалізувати трирівневу аналітичну рамку з арсеналу воєнних аналітиків інформаційних операцій США для дослідження російської дезінформації, попередньо апробувавши її на прикладі реальної інформаційної операції після широкомасштабного вторгнення 2022 р., з огляду на її еволюційний розвиток. Запропонована рамка розмежовує технічний рівень (інфраструктура, механізми доставки, експлуатація платформ), наративний рівень (стратегічні наративи, фреймінг, еволюція інформації) і когнітивний рівень (психологічні вразливості, рефлексивне управління, поведінкові ефекти) та визначає функціональні зв'язки між ними, які дозволяють комплексно аналізувати інформаційні операції РФ.

Методи. У статті використано методи критичного інтерпретативного синтезу наукової літератури з трьох взаємопов'язаних предметних областей: теорії пропаганди і дезінформації, методології військових інформаційних операцій та інституційної історії російського інформаційного впливу. Огляд охоплює комбінацію сучасних досліджень обчислювальної пропаганди, військових доктрин інформаційних операцій, актуальних методів виявлення способів поширення та ефектів інформаційних гібридних операцій. На основі цієї рамки методом аналітичної індукції виводиться рамка для дослідження, яка проходить емпіричну апробацію для аналізу інформаційної операції з «продажу зброї».

Результати дослідження. Згідно з визначенням В. Горбуліна та ін. [1, 8], інформаційні операції (ІО) є компонентом інформаційних протистоянь, які спрямовані на «реалізацію спланованих інформаційно-психологічних впливів на аудиторію, впливаючи на її установки та поведінку для досягнення заздалегідь визначених цілей». В сучасному світі ці операції перейшли здебільшого у кіберпростір, де головними інструментами доставки повідомлень стали соціальні мережі, які використовуються для впливу на цільові аудиторії.

Деякі дослідники ІО фокусуються передовсім на повідомленнях і контенті пропаганди та таких операцій, а також на системі цих повідомлень, як у роботі К. Пола і М. Метьюза, які концептуалізували модель «потоку брехні», що стала основоположною для розуміння російських підходів да забруднення інформаційного простору [15]. Інші дослідники цього різновиду комунікацій зосередилися на наративних стратегіях: це, наприклад, метод інформаційного відмивання [19], який дозволяє виявити схеми розповсюдження контенту від периферії до мейнстріму. На наративному рівні у 2017 році сформульовано універсальну типологію інформаційного безладу, запропоновану К. Вордл та Х. Деракшаном [23], яка визначила три ключові типи неправдивої інформації: мізінформацію, дезінформацію та малінформацію, які стали базою для багатьох сучасних досліджень дезінформаційних операцій [11]. Однак, ця таксономія не пояснює механізмів взаємодії названих категорій у реальних інформаційних операціях.

В українському контексті 2023–2024 років спільний звіт Центру стратегічних комунікацій та інформаційної безпеки і Центру демократії та верховенства права [4] задокументував основні наративи російської дезінформаційної реклами. Вони виявили у Фейсбуку 12 базових тем, що послідовно спрямовувалися на підрив обороноздатності України

через рекламні повідомлення. Історичною еволюцією кремлівської пропаганди від радянських часів до початку широкомасштабного вторгнення займалися Р. Горбик та інші [8], порівнюючи радянську модель пропаганди з російською. Л. Смола досліджувала феномен чуток у поширенні неправдивої інформації в епоху постправди, що руйнує суспільний дискурс та підриває основи держави [3].

У сфері когнітивних досліджень впливу на цільові аудиторії останні роботи фокусуються на психологічних умовах ефективності інформаційних операцій. Дж. Зілінскі та ін. показали, що сприйнятливість споживачів до дезінформаційних наративів під фальшивим прапором, які передували вторгненню РФ в Україну 2022 року, корелювала з їхньою попередньою схильністю до конспірологічного мислення і недовірою до інституцій [24]. Г. Пенікук та Д. Ренд вивчали когнітивні вразливості та механізми зміни переконань у споживачів інформації, а саме які фактори впливають на довіру до інформації незалежно від того, чи є вона правдивою [17].

На інфраструктурному рівні масив нових публікацій з проблем ІО стосується технічного виміру операцій, зокрема — виявлення координованої неавтентичної поведінки (СІВ) на соціальних платформах, як-от Фейсбук чи Твіттер/Х. Загальні підходи до ідентифікації мережевих ботів через набір поведінкових патернів були описані у роботі О. Варола та ін. [22], а зараз розширюються до методів, притаманних окремим платформам. Водночас, сама концепція такої поведінки змінюється, бо СІВ в соціальних мережах не завжди є ознакою інформаційної операції [18], а може свідчити й про координацію активістських мереж.

Таким чином, всі три рівні часто презентуються як окремі елементи дослідження різних операцій, проте не конче демонструють комплексності підходу. Для такого огляду нині доцільно використати військову модель інформаційних операцій, яка закріплена у доктрині США [21]. Зокрема, вони виділяють у цій моделі ІО три рівні інформаційного середовища: фізичний, інформаційний та когнітивний. У військових документах фізичний рівень відповідає за матеріальний світ, який включає центри прийняття рішень, людей, а також устаткування для передачі та споживання інформації, як-от антени для передачі інформації, комп'ютери та фізичні медіа. Інформаційний простір включає збір, обробку та поширення інформації. Когнітивний рівень охоплює розум тих, хто отримує та реагує на інформацію, приймає рішення й діє на її основі [21, 12–13]. Водночас доктрина НАТО [12, 1–4, 1–5] описує, на що конкретно

намагаються вплинути такі операції, а саме — на волю, розуміння та можливості акторів, які приймають рішення.

Якщо перекласти цю аналогію на аналіз ворожих інформаційних операцій у науковій та практичній сферах, то перший, технічний рівень включатиме сервери, ботоферми та іншу інфраструктуру; інформаційний описуватиме контент, тобто фото, відео, а також аналіз наративів та їх трансформації. Відповідно, останній, когнітивний рівень включатиме ефект, а саме наявні емоції, цінності, вірування й норми цільової аудиторії і можливі зміни та вплив на ці елементи. Таким чином, дослідники зможуть всеохопно оцінювати можливі ефекти від таких операцій, а не фокусуватися на одному чи двох їх рівнях. Запропонована американськими військовими у сфері ІО архітектура моделі може бути виражена як:

Інформаційна операція = функція від (Технічного рівня, Наративного рівня, Когнітивного рівня та взаємозв'язків між ними),

де ці взаємозв'язки є критичними для аналізу, адже дезінформаційний актор може змінювати свою поведінку у відповідності до зворотного зв'язку будь-якого з рівнів. Так, блокування інфраструктури для доставки контенту у соцмережах може спровокувати пошук нових шляхів для розповсюдження; сприйняття чи несприйняття певних повідомлень аудиторією — до зміни формату доставки тощо.

Для доказу ефективності цього підходу варто застосувати його в аналізі російських інформаційних операцій проти України після широкомасштабного вторгнення 2022 року. Ця стаття є прикладом такого аналізу, оскільки фокусується на поширенні наративу про «продаж зброї»: його росіяни запустили у квітні 2022 року та продовжують використовувати й досі, додаючи в цю ІО все нових аспектів [14].

Так, перші повідомлення про нібито «продаж зброї» корумпованими українськими чиновниками з'явилися в анонімному телеграм-каналі «Легітимний», який пов'язують з російським Генеральним Штабом [2]. Канал анонсував продаж Україною «надлишків» зброї [14] в країни Африки на тлі повідомлень про брак зброї в Україні для відбиття збройної агресії РФ. Повідомлення в «Легітимному» супроводжував підроблений лист від тодішнього міністра оборони О. Резнікова, який містив кілька критичних помилок. Це перше з тематичних повідомлень стало засівом для згаданого наративу в рамках російської ІО. Вже на цьому її

етапі можна виділити технічний рівень — пов'язані з РФ анонімні телеграм-канали та офіційні російські медіа, які синхронно підсилили це повідомлення. На когнітивному рівні — вплив на українську аудиторію зі спробою підриву довіри до державних органів.

Згодом цей наратив отримав додаткове підсилення через ту само інфраструктуру, тобто телеграм-канали, але на цей раз — від імені російських «військових блогерів», які дружно опублікували сфабриковані повідомлення з темної мережі (dark web) [7]. Хоча інформаційна операція й не змінила механізмів фізичного рівня, проте змінився наративний рівень — адже наратив отримав підживлення, додавши нові «докази» й підсиливши та процитувавши оригінальне повідомлення, тобто відбулася й триває досі його еволюція. На когнітивному рівні — ця операція продовжує спробу вплинути на аудиторію України з метою підриву довіри до її інституцій, у цьому випадку Збройних сил України та уряду, а для внутрішньої російської аудиторії ця пролонгована ІО виконує роль виправдання за військове вторгнення й водночас добивається применшення суб'єктності та сталості України як держави.

Наступним кроком цієї операції було підключення зовнішніх акторів задля інтернаціоналізації наративу «продаж зброї» [14]. Росіяни тепер використали повідомлення іноземця, який повірив був у неправдиву інформацію про захоплення росіянами на українському фронті французьких гаубиць «Цезар». Використавши пости його невдоволення у соцмережі, та сама інфраструктура російських медіа й телеграм-каналів підсилила повідомлення, перетворивши фальшиве «захоплення гаубиць» на їх начебто «продаж». Цей факт хутко підхопили в іноземному блозі Bulgarian Military, підсиливши проросійське дезінформаційне повідомлення. У подальших ітераціях цих повідомлень Україна «продавала» зброю то в Європі [13], то ХАМАС [9], мексиканському картелю [10] та іншим акторам, з останнім — за часом до публікації цієї статті — дезінформаційним повідомленням про те, що зброя, яку США передали Україні, була використана Іраном проти США та Ізраїлю [20].

Таким чином, пролонговану в часі інформаційну операцію РФ «продаж зброї», яка розпочалася у 2022 році й триває досі, можна проаналізувати на трьох рівнях. По-перше, **фізичний рівень** її характеризується в основному неперевіреними повідомленнями від анонімних та проросійських телеграм-каналів, російських медіа на периферії та у мейнстрімі, які підсилювали цей дискурс, бо незмінно посилалися один на одного для збільшення правдоподібності повідомлення.

Іноземні користувачі та блогери, які симпатизують РФ, продовжували ротувати це повідомлення далі, використовуючи старі підробки як основу й «доказову базу» для наступних неправдивих повідомлень, впливаючи вже на цільові аудиторії поза межами України та РФ. Підсилення цих повідомлень у соціальних мережах за допомогою ботів та тролів дозволяє цьому наративу раз по раз з'являтися знову й досягати нових аудиторій на соціальних платформах.

Наративний рівень характеризується оновленням наративу від оригінального повідомлення про «продаж надлишків» до продажу необхідного озброєння терористичним групам, як-от мексиканський картель. Стратегічний наратив у цьому випадку — це «Україна продає зброю попри війну». Він підтримує фрейм про продаж допомоги (західної зброї), ігнорування потреб фронту, цинічність державних акторів, а також побічно засвідчує «корупційність» та ненадійність України як партнера та країни, якій не варто довіряти та допомагати. Цей рівень є найчастіше оновлюваним, бо він повсякчас потребує підкріплення, тобто дедалі новішої доказової бази. Подача підсилюється з кожним новим повідомленням, отже й сторонньому споживачу інформації буде важко розплутати набір багатьох взаємно підсилюваних дезінформаційних повідомлень — вони надходять від джерел повідомлень з різним рівнем очевидності й походження, від сліпучо-білого до аспідно-чорного [5]. Варто також відзначити, що навіть медіа з репутацією припускалися «помилки», чим підігравали цьому наративу [15].

Когнітивний рівень у цьому прикладі включатиме провокування недовіри до уряду як підтверджувального упередження [16]. Таким чином, росіяни намагаються посіяти серед українців зневіру у роботі уряду та підважити можливості їх спротиву вторгненню РФ, що цілковито збіжне з цілями пропагандистів РФ, отриманими Департаментом юстиції США [6, 149–150]. Для зовнішніх аудиторій росіяни цією операцією сіють сумнів у доцільності допомоги Україні, як з військового так і гуманітарного її боку, адже ставиться під питання надійність України як державного партнера та розмивається «необхідність» у зброї через буцімто перепродаж чи недбалу втрату цього озброєння. Таким чином, це повідомлення в рамках тривалої ІО росіян опосередковано підсилює соціальну поляризацію населення країн-союзниць шляхом інтеграції у дискурс країн-цілей наративів, що вони підсилюють позицію людей, які виступають проти допомоги Україні. Більше того, це може правити й елементом стратегії рефлексивного управління генерала В. Гєрасімова,

якщо врахувати, що мета РФ є зменшити обсяги допомоги Україні задля отримання переваги у війні. Ця інформаційна операція може впливати на групи прийняття рішень країн-союзниць, формуючи частину інформаційного оточення, і, потенційно, вони можуть зменшувати об'єм допомоги від наших союзників.

Взаємозв'язок трьох названих рівнів очевидно призвів до поступової еволюції наративу «продаж зброї», зважаючи на аудиторію та зворотний зв'язок. Перші посіви дезінформації у Телеграмі не спричинили очікуваного ефекту в Україні, що надалі спонукало росіян змістити фокус на «корисних» розповсюджувачів за кордоном, які, будучи відірваними від реалій війни, підхопили повідомлення й щоразу поширюють дедалі новіші трансформації цього наративу. У зв'язку з цим змінилася й система доставки: від російськомовного Телеграму до англомовних публікацій у вебі та Твіттері/X, тобто на платформах, де цільовий користувач більш вірогідно побачить це повідомлення.

Висновки. Інформаційні операції стали в 2020-х невід'ємною частиною життя як країн у стадії активної війни чи конфлікту, так і країн, які формально не є учасницями таких конфліктів, адже авторитарні країни, на кшталт РФ, постійно використовують їх як арсенал ведення війни іншими способами. Продемонстрована рамка, адаптована в український дослідницький інструментарій з військових доктрин США, є за нинішніх умов корисною для всебічного аналізу інформаційних операцій, адже дозволяє відстежувати їх оновлення синхронізовано на декількох рівнях. Детальне розуміння операцій дозволить виявити слабкі ланки й створити ефективніший захист для протидії інформаційним кампаніям. Майбутні дослідники можуть апробувати запропоновану нами модель до вивчення інших інформаційних операцій, дезінформаційних кампаній, а також поглибити когнітивну частину, яка потребує найбільше ресурсів для доведення через організацію експериментальних досліджень, які б визначали вплив таких інформаційних операцій на аудиторії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Горбулін В., Додонов О., Ланде Д. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. Київ : Інтертехнологія, 2009. 164 с.

2. Служба безпеки України. СБУ викрила агентурну мережу спецслужб РФ, яка дестабілізувала ситуацію в Україні через Telegram-канали. URL: https://ssu.gov.ua/novyny/sbu-vykryla-ahenturnu-merezhu-spetssluzhb-rf-yaka-destabilizuvala-sytuatsiiu-v-ukraini-cherez-telegramkanaly (дата звернення: 23.03.2026).
3. Смола Л. Є. Феномен чуток в епоху постправди. Обрії друкарства. 2024. № 1(15). С. 62–74. URL: https://doi.org/10.20535/2522-1078.2024.1(15).299705 (дата звернення: 09.04.2026).
4. Центр стратегічних комунікацій та інформ. безпеки, Центр демократії та верховенства права. Інформаційні атаки в соціальних мережах: Дослідження впливу російської дезінформації через рекламу в Facebook. 2024. 32 с. URL: https://spravdi.org/wp-content/uploads/2024/04/informaczijni-ataky-v-soczialnyh-merezhah.-doslidzhennya-vplyvu-rosijskoyi-dezinformacziyi-cherez-reklamu-v-facebook.pdf (дата звернення: 24.03.2026).
5. Chan E. Seeding perceptions: modern influence operations in global security. Politics and international relations. 2025. URL: https://doi.org/10.33774/apsa-2025-jxzm3 (date of access: 27.03.2026).
6. Department of Justice. Justice Department disrupts covert Russian government-sponsored foreign malign influence operation targeting audiences in the United States and elsewhere. 2024. URL: https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence (date of access: 26.03.2026).
7. Digital Forensic Research Lab. Russian War Report: Russian governor accuses Ukraine of launching multiple attacks on Kursk. New Atlanticist. URL: https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-russian-mayor-kursk/#telegram (date of access: 26.03.2026).
8. Horbyk R., Prymachenko Y., Orlova D. The transformation of propaganda: The continuities and discontinuities of information operations, from Soviet to Russian active measures. Nordic journal of media studies. 2023. Vol. 5, no. 1. P. 68–94. URL: https://doi.org/10.2478/njms-2023-0005 (date of access: 09.04.2026).
9. Marcelo P. BBC did not report that Ukraine is sending arms to Hamas, a video was fabricated. URL: https://apnews.com/article/fact-check-israel-hamas-ukraine-russia-weapons-265852026856 (date of access: 26.03.2026).
10. McCarthy B. No evidence Mexican cartel obtained US weapons destined for Ukraine. AFP. URL: https://factcheck.afp.com/doc.afp.com.33GZ8H2 (date of access: 26.03.2026).

11. Morse J. C., Pratt T. Information disorder and global politics. International organization. 2025. Vol. 79, S1. P. S26–S43. URL: https://doi.org/10.1017/s0020818325101069 (date of access: 09.04.2026).
12. Nato. NATO allied joint publication 3.10 (AJP-3.10). URL: https://info.publicintelligence.net/NATO-IO.pdf (date of access: 27.03.2026).
13. Osadchuk R. Seven steps to spread a conspiracy: How Russia promoted weapons trade allegations. URL: https://dfrlab.org/2023/03/09/seven-steps-to-spread-a-conspiracy-how-russia-promoted-weapons-trade-allegations/ (date of access: 27.03.2026).
14. Osadchuk R. Y. Multi-step approach for disinformation — analysis of 'ukrainian trades us-donated weapons' narrative. "Scientific notes of V. I. vernadsky taurida national university", series: "philology. journalism". 2025. Vol. 2, no. 3. P. 311–316. URL: https://doi.org/10.32782/2710-4656/2025.3.2/46 (date of access: 09.04.2026).
15. Paul C., Matthews M. The russian "firehose of falsehood" propaganda model: why it might work and options to counter it. RAND Corporation, 2016. URL: https://doi.org/10.7249/pe198 (date of access: 09.04.2026).
16. Paziuk A. et al. Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict. Frontiers in artificial intelligence. 2025. Vol. 8. URL: https://doi.org/10.3389/frai.2025.1566022 (date of access: 09.04.2026).
17. Pennycook G., Rand D. G. The psychology of fake news. Trends in cognitive sciences. 2021. Vol. 25, no. 5. P. 388–402. URL: https://doi.org/10.1016/j.tics.2021.02.007 (date of access: 09.04.2026).
18. Rogers R., Righetti N. Coordinated inauthentic behaviour on Facebook? A typology of manufactured attention. Platforms & society. 2025. Vol. 2. URL: https://doi.org/10.1177/29768624251369784 (date of access: 09.04.2026).
19. Singh K. Information warfare laboratories: comparing russian disinformation operations in romania and potential expansion to moldova and georgia. Connections: the quarterly journal. 2025. Vol. 24, no. 2. P. 35–53. URL: https://doi.org/10.11610/connections.24.2.05 (date of access: 09.04.2026).
20. StopFake. Фейк: іран атакує США та ізраїль ракетами, переданими україні — USA today. StopFake. URL: https://www.stopfake.org/uk/fejk-iran-atakuye-ssha-ta-izrayil-raketami-peredanimi-ukrayini-usa-today/ (дата звернення: 26.03.2026).

21. US Joint Chief of Staff. Joint publication 3-13 information operations. URL: https://irp.fas.org/doddir/dod/jp3_13.pdf (date of access: 28.03.2026).
22. O. Varol et al. Online human-bot interactions: detection, estimation, and characterization (version 2). 2017. (Preprint). URL: https://doi.org/10.48550/ARXIV.1703.03107 (date of access: 28.03.2026).
23. Wardle C., Derakhshan H. Information Disorder: toward an interdisciplinary framework for research and policymaking. Council of Europe. URL: https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77 (date of access: 28.03.2026).
24. J. Zilinsky et al. Justifying an invasion: when is disinformation successful? / Political communication. 2024. P. 1–22. URL: https://doi.org/10.1080/10584609.2024.2352483 (date of access: 09.04.2026).

REFERENCES

1. Horbulin , V., Dodonov, O. & Lande, D. (2009). Informatsiini operatsii ta bezpeka suspilstva: Zahrozy, protydiia, modeliuvannia [Information Operations and Public Security: Threats, Countermeasures, Modeling] Monograph. Intertekhnolohiia [in Ukrainian].
2. The Security Service of Ukraine. (2021, February 1). SBU vykryla ahenturnu merezhu spetssluzhb RF, yaka destabilizuvala sytuatsiiu v Ukraini cherez Telegram-kanaly [The SSU exposed an agent network of the Russian fedaration, which destabilized the situation in Ukraine through Telegram channels]. Retrieved from https://ssu.gov.ua/novyny/sbu-vykryla-ahenturnu-merezhu-spetssluzhb-rf-yaka-destabilizuvala-sytuatsiiu-v-ukraini-cherez-telegramkanaly [in Ukrainian]
3. Smola, L. (2024). The phenomenon of rumors in the era of post-truth. Printing Horizon, (1(15)), 62–74. https://doi.org/10.20535/2522-1078.2024.1(15).299705 [in Ukrainian]
4. Centre for Strategic Communication and Information Security, Centre for Democracy and Rule of Law. (03/24). Informatsiini ataky v sotsialnykh merezhakh: Doslidzhennia vplyvu rosiiskoi dezinformatsii cherez reklamu v Facebook [Information attacks in social networks: a study of impact of Russian disinformation through advertisements in Facebook] Centre for Strategic Communication and Information Security. Retrieved from https://spravdi.org/wp-content/uploads/2024/04/informaczijni-ataky-v-soczialnyh-merezhah.-doslidzhennya-vplyvu-rosijskoyi-dezinformacziyi-cherez-reklamu-v-facebook.pdf [in Ukrainian]

5. Chan, E. (2025). Seeding Perceptions: Modern Influence Operations in Global Security. Politics and International Relations. https://doi.org/10.33774/apsa-2025-jxzm3
6. Department of Justice. (2024, September 4). Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere. United States Department of Justice. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence
7. Digital Forensic Research Lab. (2022, June 17). Russian War Report: Russian governor accuses Ukraine of launching multiple attacks on Kursk. New Atlanticist. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-russian-mayor-kursk/#telegram [in Ukrainian]
8. Horbyk, R., Prymachenko, Y., & Orlova, D. (2023). The transformation of propaganda: The continuities and discontinuities of information operations, from Soviet to Russian active measures. Nordic Journal of M edia Studies, 5(1), 68–94. https://doi.org/10.2478/njms-2023-0005 [in Ukrainian]
9. Marcelo, P. (2023, October 12). BBC did not report that Ukraine is sending arms to Hamas, a video was fabricated. The Associated Press. Retrieved from https://apnews.com/article/fact-check-israel-hamas-ukraine-russia-weapons-265852026856
10. McCarthy, B. (2023, June 6). No evidence Mexican cartel obtained US weapons destined for Ukraine. AFP. Retrieved from https://factcheck.afp.com/doc.afp.com.33GZ8H2
11. Morse, J. C., & Pratt, T. (2025). Information Disorder and Global Politics. International Organization, 79(S1), S26–S43. https://doi.org/10.1017/S0020818325101069
12. NATO. (2009, November). NATO Allied Joint Publication 3.10 (AJP-3.10) [Doctrine]. Retrieved from https://info.publicintelligence.net/NATO-IO.pdf
13. Osadchuk, R. (2023, March 9). Seven steps to spread a conspiracy: How Russia promoted weapons trade allegations. Retrieved from https://dfrlab.org/2023/03/09/seven-steps-to-spread-a-conspiracy-how-russia-promoted-weapons-trade-allegations/ [in Ukrainian]
14. Osadchuk, R. Yu. (2025). Multi-step approach for disinformation — analysis of “Ukrainian trades US-donated weapons” narrative. “Scientific Notes of V. I. Vernadsky Taurida National University”, Series:

"Philology. Journalism," 2(3), 311–316. https://doi.org/10.32782/2710-4656/2025.3.2/46 [in Ukrainian]
15. Paul, C., & Matthews, M. (2016). The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. RAND Corporation. https://doi.org/10.7249/PE198
16. Paziuk, A., Lande, D., Shnurko-Tabakova, E., & Kingston, P. (2025). Decoding manipulative narratives in cognitive warfare: A case study of the Russia-Ukraine conflict. Frontiers in Artificial Intelligence, 8, 1566022. https://doi.org/10.3389/frai.2025.1566022 [in Ukrainian]
17. Pennycook, G., & Rand, D. G. (2021). The Psychology of Fake News. Trends in Cognitive Sciences, 25(5), 388–402. https://doi.org/10.1016/j.tics.2021.02.007
18. Rogers, R., & Righetti, N. (2025). Coordinated inauthentic behaviour on Facebook? A typology of manufactured attention. Platforms & Society, 2, 29768624251369784. https://doi.org/10.1177/29768624251369784
19. Singh, K. (2025). Information Warfare Laboratories: Comparing Russian Disinformation Operations in Romania and Potential Expansion to Moldova and Georgia. Connections: The Quarterly Journal, 24(2), 35–53. https://doi.org/10.11610/connections.24.2.05
20. StopFake. (2026, March 7). Feik: Iran atakuie SShA ta Izrail raketamy, peredanymy Ukraini — USA Today [Fake: Iran attacks US and Israel with missiles transferred to Ukraine — USA Today]. StopFake. Retrieved from https://www.stopfake.org/uk/fejk-iran-atakuye-ssha-ta-izrayil-raketami-peredanimi-ukrayini-usa-today/ [in Ukrainian]
21. US Joint Chief of Staff. (2012). Joint Publication 3-13 Information Operations. US Joint Chief of Staff. Retrieved from https://irp.fas.org/doddir/dod/jp3_13.pdf
22. Varol, O., Ferrara, E., Davis, C. A., Menczer, F., & Flammini, A. (2017). Online Human-Bot Interactions: Detection, Estimation, and Characterization (Version 2). arXiv. https://doi.org/10.48550/ARXIV.1703.03107
23. Wardle, C., & Derakhshan, H. (n.d.). Information Disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe. Retrieved from https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77
24. Zilinsky, J., Theocharis, Y., Pradel, F., Tulin, M., De Vreese, C., Aalberg, T., Cardenal, A. S., Corbu, N., Esser, F., Gehle, L., Halagiera, D., Hameleers, M., Hopmann, D. N., Koc-Michalska, K., Matthes, J., Schemer, C., Štětka, V., Strömbäck, J., Terren, L., ... Zoizner, A. (2024). Justifying an

Invasion: When Is Disinformation Successful? Political Communication, 41(6), 965–986. https://doi.org/10.1080/10584609.2024.2352483

У підготовці цієї статті інструменти штучного інтелекту використовувалися виключно для перевірки граматики та орфографії мови (інструмент — Grammarly), а також задля пошуку релевантних наукових публікацій, дотичних до теми статті (інструмент — Gemini 3 Pro). Всю відповідальність за вміст рукопису та використані джерела несе автор публікації.