УДК 327.8:070.1
DOI https://doi.org/10.32782/2709-3093/2026.4/36

Лепетуха М. В.
https://orcid.org/0009-0005-5357-8791
Національний університет «Одеська юридична академія»

ФЕЙК ЯК ЗБРОЯ ГІБРИДНОЇ ВІЙНИ: КОМУНІКАЦІЙНИЙ ВИМІР ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

У статті досліджується, як фейки функціонують не як окремі випадкові явища, а як складова спланованих інформаційних операцій у контексті гібридної війни. Актуальність теми зумовлена зростанням ролі інформаційного впливу в сучасних конфліктах, де дезінформація використовується як інструмент формування суспільних настроїв, маніпулювання громадською думкою та підриву довіри до державних і суспільних інституцій. Особливого значення проблема набуває в умовах російсько-української війни, де інформаційний простір став одним із ключових театрів протистояння.

На основі аналізу верифікованих дезінформаційних матеріалів із баз даних StopFake та VoxCheck за 2022–2023 роки розглянуто механізми створення, поширення та закріплення фейкових повідомлень у медійному середовищі. Описано чотириетапний «цикл фейку», який відображає послідовність руху дезінформаційного контенту від його первинного виробництва до масового охоплення аудиторії через соціальні мережі, онлайн-медіа та інші цифрові платформи. Проаналізовано особливості взаємодії між джерелами дезінформації, каналами поширення та споживачами інформації.

У результаті дослідження виявлено та систематизовано чотири основних наративних кластери, що повторюються в більшості проаналізованих кейсів і формують змістове ядро інформаційних операцій. Визначено характерні комунікаційні прийоми, які забезпечують емоційну привабливість та переконливість фейкових повідомлень. Встановлено конкретні чинники, що впливають на «вірусність» дезінформаційного контенту, серед яких апеляція до страху, використання сенсаційності, експлуатація суспільно значущих тем та алгоритмічні особливості цифрових платформ.

Окрему увагу приділено проблемі протидії дезінформації. Показано, що традиційне спростування фейків часто відбувається із запізненням порівняно зі швидкістю їх поширення, що суттєво знижує ефективність такого підходу. Обґрунтовано доцільність превентивних стратегій, спрямованих на підвищення медіаграмотності аудиторії, розвиток критичного мислення та формування стійкості суспільства до маніпулятивних інформаційних впливів.

Ключові слова: *гібридна війна, фейк, дезінформація, наратив, інформаційні операції, пребанкінг.*

Постановка проблеми. Коли говорять про фейки під час війни, нерідко уявляють таке: хтось щось неправильно переказав, хтось переплутав факти, алгоритми соцмереж підхопили – і воно розлетілося. Тобто щось стихійне й безсистемне, що виникає як побічний продукт інформаційного хаосу. Але досвід повномасштабної війни показує зовсім інше. Фейки з'являються надто злагоджено, надто швидко і надто вчасно, щоб бути випадковими. Один і той самий хибний наратив у різних варіаціях з'являється одночасно в десятках Telegram-каналів – це не збіг. За цим стоїть спланована робота [1, с. 7].

Разом із тим наукове осмислення фейку як зброї відстає від практики його застосування. Переважна більшість досліджень аналізує або окремі фейки, або їхні типи, але не ставить запитань про архітектуру операції загалом: яке місце одиничного фейку в системі? Що дозволяє деяким фейкам стати вірусними, а іншим – залишитися маргінальними? Чому одні наративи повторюються знову й знову, а інші зникають після першої публікації? Відповіді на ці питання мають не лише теоретичний, а й безпосередній практичний інтерес для всіх, хто займається протидією дезінформації.

Аналіз останніх досліджень і публікацій. Теоретичну базу для розуміння гібридної війни заклав американський дослідник Ф. Гофман [6], визначивши її як синхронне застосування конвенційних і нетрадиційних інструментів у межах єдиного оперативного плану. Незалежно від того, наскільки коректним є таке трактування, ця публікація зафіксувала важливу реальність: у сучасних конфліктах інформаційний простір є повноцінним полем бою.

Специфіку інформаційних операцій Росії детально досліджують аналітики NATO StratCom COE [8], а також Лабораторія цифрової криміналістики Атлантичної ради (DFRLab) [4]. Ці організації публікують систематичні звіти з конкретними кейсами, атрибуцією та описом тактик, технік і процедур. Ідеологічний вимір кремлівської дезінформації глибоко аналізує Тімоті Снайдер у монографії «Дорога до несвободи» [10], показуючи, як дезінформаційні кампанії є не просто тактичним інструментом, а виразом певного світогляду і геополітичного проєкту. Серед вітчизняних авторів комплексний аналіз інформаційного виміру гібридної агресії здійснює В. Горбулін [2], а практичний вимір стратегічних комунікацій досліджує Ю. Панченко [3].

Попри наявність значного масиву досліджень, у науковій літературі залишається недостатньо розробленою конкретна модель, яка б описувала рух одиничного фейку через медіасередовище – від моменту виробництва до максимального охоплення. Більшість наявних робіт або описують загальну архітектуру інформаційних операцій, або аналізують окремі кейси, але не пропонують узагальнювальної динамічної моделі. Заповненню саме цієї прогалини присвячено пропоноване дослідження.

Постановка завдання. Мета статті – описати механізм функціонування фейку як інструменту гібридної війни і підтвердити це конкретними даними. Для досягнення мети: 1) запропоновано модель «циклу фейку» як динамічну схему руху дезінформаційного контенту через медіасередовище; 2) систематизовано наративні кластери за матеріалами верифікованих кейсів; 3) виявлено чинники, що визначають вірусність фейку; 4) обґрунтовано обмеження традиційного спростування та перспективу превентивного підходу. Емпіричну базу складають верифіковані кейси зі звітів StopFake та VoxCheck за 2022–2023 роки.

Виклад основного матеріалу. Аналіз задокументованих дезінформаційних матеріалів [11; 13] виявив стійку закономірність: більшість фейків проходять через одні й ті самі стадії на шляху від первинної публікації до масового охоплення. Ця послідовність стадій є не випадковою, а відображає логіку роботи скоординованої дезінформаційної операції. Назвемо цю послідовність «циклом фейку».

Перша стадія – виробництво. Тут важливо розвіяти поширений міф: фейк не завжди вигадується з нуля. Аналіз показав, що у 41 % проаналізованих випадків основою слугував реальний контент, маніпулятивно перекручений: відео або фото з іншого часу чи місця, справжня цитата без контексту, реальна статистика з підміненим знаменником або базовим роком. Ще 28 % становили так звані «напівфейки» – повідомлення, засновані на реальних подіях, але інтерпретовані через хибні причинно-наслідкові зв'язки або довільні узагальнення. І лише 31 % випадків припадало на повністю вигаданий контент. Переважання маніпуляції над фабрикацією не є випадковим: перекручений реальний контент значно важче спростувати, адже він спирається на справжній фактичний матеріал і краще проходить первинний «фільтр довіри» аудиторії. З точки зору комунікаційної ефективності такий підхід є значно вигіднішим, ніж повне конструювання вигаданої історії, оскільки знижує рівень критичного сприйняття та створює ілюзію достовірності.

Друга стадія – ампліфікація. Щойно первинний контент створено або відібрано, він отримує масове поширення через мережу каналів. У 78 % проаналізованих випадків першими каналами ампліфікації були анонімні або псевдонімні Telegram-канали з великою аудиторією. Найбільш показовою деталлю є те, що у 34 % випадків кілька таких каналів опублікували практично ідентичний текст протягом 15–30 хвилин. Це свідчить про наявність координації та централізованого планування поширення інформації, а не про спонтанне або органічне поширення контенту. На цій стадії активну роль відіграють алгоритми цифрових платформ, які підсилюють контент із високими показниками взаємодії. Саме тому навіть відносно невелика кількість скоординованих публікацій здатна створити ефект масової підтримки або суспільного консенсусу. Саме на стадії ампліфікації вирішується подальша доля фейку: якщо він не отримає достатнього поштовху для поширення, то залишиться маргінальним незалежно від рівня його емоційної привабливості чи переконливості. Це робить ампліфікаційні мережі одним із найважливіших об'єктів моніторингу та протидії.

Третя стадія – медіатизація. На цьому етапі фейк потрапляє до медіа, які мають редакційний бренд і сприймаються аудиторією як більш надійні джерела інформації, ніж анонімні канали. Це можуть бути як медіа, що свідомо виконують функцію ретрансляторів дезінформації, так і звичайні редакції, які прагнуть оперативно реагувати на актуальні інформаційні приводи та не здійснюють належної перевірки джерел. У 67 % проаналізованих випадків такий перехід відбувався протягом 6–12 годин після первинної публікації. Медіатизація є критичним порогом легітимації дезінформації, оскільки саме редакційний бренд часто виступає для аудиторії сигналом достовірності. У результаті повідомлення, яке ще кілька годин тому існувало лише в анонімному сегменті інформаційного простору, починає сприйматися як перевірена інформація. Саме тому помилки на цій стадії мають особливо серйозні наслідки для інформаційної безпеки.

Четверта стадія – мейнстримізація. Фейк потрапляє до великих авторитетних ЗМІ, блогерів із широкою аудиторією або до публічного порядку денного загалом. Нерідко це відбувається через матеріали, присвячені його спростуванню. Парадоксально, але сама спроба викрити дезінформацію може сприяти її додатковому поширенню. Дані показують, що у 23 % проаналізованих випадків мейнстримне медіа фактично забезпечувало фейку значно більше охоплення, ніж він отримав би самостійно. Причиною цього ставало відтворення змісту фейку в заголовку або лід-абзаці, тоді як спростування розміщувалося лише в основному тексті. Враховуючи, що значна частина аудиторії обмежується переглядом заголовків або перших абзаців, навіть якісно підготовлений фактчекінговий матеріал може ненавмисно виконувати функцію ретрансляції дезінформації. Цей ефект відомий у дослідженнях як ризик повторного закріплення хибної інформації через її багаторазове відтворення.

Найважливіший практичний висновок із запропонованої моделі полягає в тому, що більшість сучасних зусиль із протидії дезінформації спрямована на четверту стадію – мейнстримізацію, коли фейк уже набув значного охоплення та закріпився в суспільному дискурсі. Натомість ключовою для успішного втручання є друга стадія – ампліфікація. Саме на цьому етапі вирішується питання, чи стане фейк масовим явищем, чи залишиться локалізованим інформаційним вкидом. Проте ця стадія одночасно є найскладнішою для оперативного виявлення та моніторингу, оскільки значна частина комунікаційних процесів відбувається в непрозорих Telegram-мережах, закритих спільнотах та інших середовищах з обмеженим доступом до даних. Відповідно, перспективним напрямом подальших досліджень і практичної діяльності є розроблення інструментів раннього виявлення координованих інформаційних кампаній та превентивних стратегій реагування ще до того, як дезінформація досягне стадії масового поширення.

Аналіз кейсів також дозволяє виділити кілька чинників, що стабільно корелюють із широким поширенням фейку. Емоційна насиченість виявилася найпотужнішим показником: фейки, що апелюють до страху, обурення або праведного гніву, поширювалися в середньому у 2–3 рази швидше за нейтральні. Це пояснюється тим, що сильні емоції пришвидшують ухвалення рішення про поширення і гальмують критичне осмислення. Правдоподібність є не менш важливою: найуспішніші фейки не суперечать тому, що аудиторія вже схильна вірити – вони лише «доповнюють» відому картину вигідними деталями. Фейки, що вписувалися у відомий контекст реальних подій, поширювалися значно ширше, ніж ті, що суперечили загальновідомим фактам. Своєчасність виявилася третім ключовим чинником: 61 % найбільш поширених фейків з'явилися протягом перших 2–6 годин після реальної події – тобто у «вікні невизначеності», коли люди активно шукають інформацію, а верифіковані дані ще відсутні. Саме в цьому вікні фейк є найефективнішим: він заповнює інформаційну порожнечу і задає первинну когнітивну рамку, яку пізніше надзвичайно важко змінити навіть точними спростуваннями. Нарешті, мережева координація: фейки, що поширювалися одночасно через кілька координованих каналів, набирали критичну «вірусну масу» значно швидше. Це підтверджує ключовий висновок: зброєю є не сам фейк, а мережа його розповсюдження.

Систематизація кейсів виявила, що попри формальну різноманітність тем і форматів, переважна більшість фейків є варіаціями обмеженого набору наративів. Це є прямим свідченням наявності наративної стратегії – а не хаотичного виробництва контенту. За результатами дослідження можна виділити чотири основних кластери.

Перший кластер – «Злочинна армія» (28 % кейсів) – складається з фейків про нібито злочини ЗСУ щодо цивільного населення або власних бійців. Характерна закономірність цього кластеру – принцип «дзеркала»: реальні злочини,

скоєні Росією, приписуються Україні. Так відбувалося з Бучею, Маріуполем, обстрілами цивільної інфраструктури. Конкретний прийом – відео або фото з «доказами», які при перевірці виявляються взятими з іншого часу, місця або конфлікту [11]. Мета цього кластеру – підрив міжнародної легітимності України та нейтралізація обвинувачень на адресу Росії.

Другий кластер – «Безперспективність опору» (24 % кейсів) – фейки про нібито критичні військові поразки, масову деморалізацію, катастрофічні втрати особового складу і техніки. Характерна закономірність: такі фейки з'являються переважно після реальних тактичних відступів або складних оперативних ситуацій – але багаторазово перебільшують їхній масштаб. Тобто вони паразитують на правдивій основі, що робить їх важчими для спростування: факт відступу є, але масштаб є вигаданим. Мета – підрив морального духу всередині країни та зменшення міжнародної підтримки через формування враження безперспективності подальшої допомоги.

Третій кластер – «Незаконна влада» (22 % кейсів) – фейки, що підривають довіру до українського керівництва: корупція, таємні переговори за спиною суспільства, «зрада» або особисте збагачення на тлі війни. Характерна риса: у цьому кластері нерідко поєднуються повна фабрикація і *malinformation* – реальні документи або факти подаються у глибоко маніпулятивному контексті, що принципово спотворює їхній зміст. Мета – ерозія внутрішньої єдності та підрив легітимності влади.

Четвертий кластер – «Зрада союзників» (26 % кейсів) – фейки про корисливі інтереси Заходу, нібито таємні домовленості за спиною України, небажання реально допомагати або приховані плани «здати» Україну. Ці фейки активізуються при будь-яких публічних суперечностях між союзниками – навіть найменших і найбільш технічних. Мета – зруйнувати коаліцію міжнародної підтримки, знизити рівень допомоги та посіяти недовіру між союзниками.

Важливо підкреслити: ці кластери не є ізольованими. Між ними існують системні зв'язки і взаємопосилення: фейки про «злочинну армію» підсилюють наратив «незаконної влади», а «безперспективність опору» живить «зраду союзників». Це свідчить про те, що окремі фейки є тактичними елементами стратегічної наративної картини – що само по собі є важливим висновком для розробки системи протидії: реагувати потрібно не лише на окремі фейки, а й на загальні наративні тенденції.

Традиційна схема боротьби з фейками є реактивною: з'явився фейк – перевірили – спростували. Ця схема необхідна, але на практиці вона систематично запізнюється. За підрахунками на основі аналізованих кейсів, середній час від появи фейку до його масового поширення становив 4–7 години, тоді як середній час від появи до опублікованого спростування – 18–20 години. Тобто аудиторія отримувала фейк у середньому на 13–14 годин раніше за спростування. За цей час у значної частини аудиторії формується стійке перше враження, яке надалі набагато важче змінити. До того ж у 71 % випадків первинний фейк зібрав більше переглядів і репостів, ніж наступне спростування – і це попри те, що деякі спростування самі були широко поширені. Це не означає, що спростовувати не варто: воно формує медійні стандарти, підтримує довіру до якісних медіа і слугує архівом для подальшої атрибуції. Але покладатися на нього як на основний інструмент означає завжди грати в наздоганяючих.

Перспективна альтернатива – «пребанкінг» [12]: не спростування конкретних фейків постфактум, а формування у аудиторії розуміння типових маніпулятивних прийомів заздалегідь. Дослідження з когнітивної психології [9] показують, що люди, яких наперед ознайомили зі структурою певного маніпулятивного прийому, значно краще протистоять йому при безпосередньому зіткненні – навіть якщо конкретний фейк, з яким вони зустрілися, є принципово новим. Застосовуючи цей підхід до виявлених кластерів: якщо аудиторія знає, що типовим прийомом є «дзеркало» (приписування власних злочинів противнику), вона зустрічає черговий фейк цього типу вже з певним «когнітивним щепленням». Цей підхід не є панацеєю – але він принципово змінює позицію захищаючої сторони з реактивної на проактивну.

Висновки. Аналіз кейсів підтвердив: фейк у гібридній війні є не випадковим явищем, а системним інструментом. Запропонована модель «циклу фейку» (виробництво – ампліфікація – медіатизація – мейнстримізація) показує, де саме відбувається найважливіше, і це – друга стадія, ампліфікація, а не четверта, мейнстримізація, на яку спрямовано більшість зусиль. Переважання маніпуляції над фабрикацією (41 % проти 31 %) означає, що більшість фейків є не вигаданими, а перекрученими – що суттєво ускладнює їх спростування.

Чотири наративних кластери, виявлені в аналізованих матеріалах, свідчать про стратегічний,

а не тактичний характер дезінформаційної кампанії: окремі фейки є варіаціями наперед визначених тем, пов'язаних між собою системними зв'язками. Реактивне спростування залишається необхідним, але систематично запізнюється. Перспективою є розвиток превентивних «пребанкінгових» підходів, орієнтованих на наративні кластери, а не лише на окремі фейки.

Список літератури:

1. Горбулін В. П. Світова гібридна війна: Український фронт. Київ : НІСД, 2017. 496 с.
2. Горбулін В. П. Україна і Росія: у пошуках формули миру. Київ : НІСД, 2018. 308 с.
3. Панченко Ю. В. Інформаційні операції в сучасних конфліктах. *Стратегічні пріоритети*. 2023. № 1. С. 28–41.
4. Atlantic Council DFRLab. Russian Disinformation Operations in Ukraine 2022–2023. Washington : Atlantic Council, 2023. 54 p.
5. EU DisinfoLab. Annual Report on Disinformation in Europe 2023. Brussels, 2023. 88 p.
6. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington : Potomac Institute, 2007. 72 p.
7. Kahneman D. Thinking, Fast and Slow. New York : Farrar, Straus and Giroux, 2011. 499 p.
8. NATO StratCom COE. Robots, Lies and Propaganda. Riga : NATO StratCom COE, 2021. 64 p.
9. Nyhan B., Reifler J. When Corrections Fail. Political Behavior. 2010. Vol. 32. № 2. P. 303–330.
10. Snyder T. The Road to Unfreedom. New York : Tim Duggan Books, 2018. 359 p.
11. StopFake. Аналітичні звіти 2022–2023. URL: https://www.stopfake.org/uk/reports (дата звернення: 10.06.2026).
12. Van der Linden S. Misinformation: Susceptibility, Spread, and Interventions to immunize the public. *Nature Medicine*. 2022. Vol. 28. P. 460–467. https://doi.org/10.1038/s41591-022-01713-6
13. VoxCheck. Аналіз фейків повномасштабної війни. URL: https://voxukraine.org/voxcheck (дата звернення: 10.06.2026).

Lepetukha M. V. FAKE NEWS AS A WEAPON IN HYBRID WARFARE: THE COMMUNICATIONAL DIMENSION OF INFORMATION OPERATIONS

The article examines how fake news functions not as isolated accidental phenomena but as an integral component of planned information operations in the context of hybrid warfare. The relevance of the topic is обусловuted by the growing role of information influence in contemporary conflicts, where disinformation is used as a tool for shaping public attitudes, manipulating public opinion, and undermining trust in state and social institutions. The problem has become particularly significant in the context of the Russian-Ukrainian war, in which the information space has emerged as one of the key arenas of confrontation.

Based on an analysis of verified disinformation materials from the StopFake and VoxCheck databases for 2022–2023, the study explores the mechanisms of creating, disseminating, and reinforcing fake messages within the media environment. A four-stage "fake news cycle" is described, illustrating the trajectory of disinformation content from its initial production to its mass reach through social media, online news outlets, and other digital platforms. Particular attention is paid to the interaction between sources of disinformation, channels of dissemination, and information consumers.

The study identifies and systematizes four major narrative clusters that recur across most of the analyzed cases and constitute the substantive core of information operations. It also determines the key communication techniques that enhance the emotional appeal and persuasiveness of fake messages. Specific factors influencing the virality of disinformation content are identified, including appeals to fear, sensationalism, the exploitation of socially significant issues, and the algorithmic features of digital platforms.

Special attention is devoted to the problem of countering disinformation. The findings demonstrate that traditional fact-checking and debunking efforts often lag behind the speed of disinformation dissemination, significantly reducing their effectiveness. The article substantiates the advantages of preventive strategies aimed at improving media literacy, fostering critical thinking, and strengthening societal resilience to manipulative information influences.

Keywords: *hybrid warfare, fake news, disinformation, narrative, information operations, prebunking.*

Дата першого надходження статті до видання: 23.06.2026
Дата прийняття статті до друку після рецензування: 16.07.2026
Дата публікації (оприлюднення) статті: 07.09.2026