НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова

праця на правах рукопису

ОСАДЧУК РОМАН ЮРІЙОВИЧ

УДК 070:316.472.4

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНІ ОПЕРАЦІЇ РФ ПІД ЧАС ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ В УКРАЇНУ: СТРАТЕГІЯ ТА ПРИКЛАДИ ЇЇ РЕАЛІЗАЦІЇ

06 «Журналістика»
061 «Журналістика»

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Р. Ю. Осадчук

Науковий керівник **Яковлєв Максим Володимирович**, доцент, кандидат політичних наук

Київ – 2026

АНОТАЦІЯ

Осадчук Р. Ю. Інформаційні операції РФ під час повномасштабного вторгнення в Україну: стратегія та приклади її реалізації — Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 061 «Журналістика» (06 — Журналістика). — Національний університет «Києво-Могилянська академія», Київ, 2026.

Дисертацію присвячено комплексному дослідженню російських інформаційних операцій проти України, що здійснюються в період після початку повномасштабного вторгнення Російської Федерації (2022–2026 рр.). Актуальність роботи зумовлена принциповою зміною масштабу, інтенсивності й технологічної складності російських операцій впливу після лютого 2022 року, а також безпрецедентною доступністю первинних документальних джерел — витоків внутрішньої документації державно-афілійованих суб'єктів впливу (передусім Social Design Agency та Structura), — що вперше дають можливість зіставити стратегічний задум операцій із задокументованими прикладами його реалізації.

Об'єктом дослідження є інформаційні операції Російської Федерації проти України, що здійснюються в період повномасштабного вторгнення (2022–2026 рр.). *Предметом дослідження* є стратегія цих операцій, реконструйована за матеріалами внутрішньої документації російських суб'єктів впливу, у її співвідношенні з прикладами реалізації у різних цифрових середовищах. *Мета дослідження* — з'ясувати на конкретних прикладах, як реалізується стратегія інформаційних операцій РФ під час повномасштабного вторгнення.

Методологія дослідження поєднує якісний аналіз стратегічних документів РФ у сфері інформаційної безпеки, метод кейс-стаді та обчислювальні методи виявлення скоординованої неавтентичної поведінки. Центральним методологічним інструментом є розроблена автором *трирівнева аналітична рамка*, що розрізняє технічний (інфраструктура, механізми доставки контенту), наративний (стратегічні наративи,

фреймінг, інформаційне відмивання) та когнітивний (психологічні вразливості, рефлексивний контроль, поведінкові ефекти) рівні інформаційних операцій. Емпіричну базу дослідження становлять три контрастні кейси інформаційних операцій. По-перше, операція «Двійник» (Doppelgänger) (система клонованих сайтів ЗМІ, які розповсюджувалися через рекламу); скоординована поведінка у коментарях соціальних платформ Telegram, X та Facebook; масштабна TikTok-операція з дискредитації представників українського військово-політичного керівництва.

Наукова новизна одержаних результатів полягає в тому, що *вперше* здійснено системний аналіз стратегічного рівня російських інформаційних операцій проти України на основі витоків внутрішньої документації SDA та Structura із зіставленням реконструйованої стратегії з емпірично задокументованими прикладами її реалізації. *Вперше* застосовано трирівневу аналітичну рамку (технічний, наративний, когнітивний виміри) як інтегрований інструмент аналізу трьох контрастних кейсів російських інформаційних операцій. *Вперше* показано, як єдиний стратегічний задум зазнає принципово різної тактичної реалізації залежно від типу цифрової платформи, на якій реалізується операція. Уведено у науковий обіг корпус із 649 скріншотів операції «Двійник» в Україні. Здійснено багатоканальну атрибуцію трьох емпірично різних російських інформаційних операцій. *Удосконалено* понятійно-категоріальний апарат вітчизняних студій інформаційних операцій через інтеграцію міжнародних аналітичних стандартів (DISARM, ABC) із теоріями комунікацій та доктринальною спадщиною РФ з часів «активних заходів», а також методологію дослідження державних інформаційних операцій. *Дістали подальший розвиток* концепція кросплатформної дифузії дезінформаційних повідомлень у логіці моделі «потоку брехні», теза про спадковість російських інформаційних операцій та осмислення інформаційних операцій РФ як компонента гібридної війни проти України.

Основним науковим внеском дисертації є емпірично обґрунтоване положення про адаптацію тактик за умови збереження стратегічної стабільності як визначальної характеристики російських інформаційних операцій проти України в період

повномасштабного вторгнення. Це положення випливає зі концептуалізації стратегічного рівня інформаційних операцій на основі практичної реалізації трьох різних операцій. Ці операції спростовують поширене уявлення про російські операції впливу як про хаотичну сукупність різних тактичних підходів й підтверджують існування зрілої формалізованої стратегічної доктрини, що зберігає внутрішню логіку незалежно від платформного середовища її втілення.

Практичне значення одержаних результатів полягає у можливості їхнього застосування для діяльності суб'єктів протидії російським інформаційним операціям, у застосуванні матеріалів для курсів з медіаграмотності, безпекових студій, комунікацій та аналізу російських інформаційних операцій. Результати можуть бути корисними у професійній діяльності журналістів і фактчекерів.

Дисертація складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 274 сторінки, з яких 215 сторінок основного тексту. Список використаних джерел налічує 273 позиції.

Ключові слова: інформаційні операції, інформаційна війна, дезінформація, соціальні медіа, російсько-українська війна, стратегія, Росія, штучний інтелект, медіапростір, пропаганда, гібридна війна, інформаційна безпека, операції впливу, Україна, стратегічні комунікації

ABSTRACT

Osadchuk R. Yu. Information operations of the Russian Federation during the full-scale invasion of Ukraine: strategy and examples of its implementation — Qualification scientific work submitted as a manuscript.

PhD thesis to obtain the degree of Doctor of Philosophy in the Program Subject Area 061 «Journalism» (06 – Journalism). – National University of Kyiv-Mohyla Academy, Kyiv, 2026.

The dissertation is devoted to a comprehensive study of Russian information operations against Ukraine carried out during the period of the full-scale invasion by the Russian Federation (2022–2026). The relevance of this study is driven by a fundamental shift in the scale, intensity, and technological complexity of Russian influence operations after February 2022. At the same time, there is the unprecedented availability of primary documentary sources—namely, leaks of internal documentation from state-affiliated influence actors (primarily the Social Design Agency and Structura). These sources enable a comparative analysis between the strategic intent of operations and documented examples of their execution.

The **object of the study** is the information operations of the Russian Federation against Ukraine conducted during the full-scale invasion (2022–2026). The **subject of the study** is the strategy of these operations, reconstructed from the internal documentation of Russian influence actors, in its correlation with examples of implementation across various digital environments. The **aim of the study** is to elucidate, through specific examples, how the strategy of the Russian Federation's information operations is implemented during the full-scale invasion.

The **methodology of the study** combines a qualitative analysis of the Russian Federation's strategic documents in the field of information security, the case study method, and computational methods for detecting coordinated inauthentic behavior (CIB). The central methodological tool is a three-tiered analytical framework developed by the author, which distinguishes between the technical level (Infrastructure, content delivery mechanisms), narrative level (strategic narratives, framing, information laundering), and cognitive level (psychological vulnerabilities, reflexive control, behavioral effects).

The empirical baseline of the study comprises three contrasting cases of information operations. 1) Operation "Doppelgänger" (a system of cloned media websites distributed via advertising); 2) The coordinated behavior in the comment sections on the social platforms Telegram, X, and Facebook. 3) A large-scale TikTok operation aimed at discrediting representatives of the Ukrainian military and political leadership.

The **scientific novelty** of the findings lies in the fact that, for the first time, a systemic analysis of the strategic level of Russian information operations against Ukraine has been conducted based on leaked internal documentation from the SDA and Structura, cross-referencing the reconstructed strategy with empirically documented examples of its execution. For the first time, a three-tiered analytical framework (technical, narrative, and cognitive dimensions) has been applied as an integrated tool to analyze three contrasting cases of Russian information operations.

Furthermore, it is demonstrated for the first time how a single strategic intent undergoes fundamentally different tactical implementations depending on the type of digital platform hosting the operation. A corpus of 649 screenshots of Operation "Doppelgänger" in Ukraine has been introduced into scholarly circulation. Multi-channel attribution of three empirically distinct Russian information operations has been performed.

The conceptual and categorical apparatus of domestic information operations studies has been enhanced by integrating international analytical standards (DISARM, ABC) with communication theories and the doctrinal legacy of the Russian Federation dating back to the era of "active measures," alongside the refinement of methodologies for researching state-sponsored information operations. The study further develops the concept of cross-platform diffusion of disinformation messages within the logic of the "firehose of falsehood" model, the thesis regarding the continuity of Russian information operations, and the conceptualization of Russian information operations as a component of the hybrid warfare waged against Ukraine.

The **primary scientific contribution** of the dissertation is the empirically substantiated proposition that the *tactics adapt under conditions of strategic stability* serves as the defining characteristic of Russian information operations against Ukraine during the full-scale invasion.

This proposition emerges from the conceptualization of the strategic level of information operations, grounded in the practical execution of three distinct operations. These operations refute the common perception of Russian influence operations as a chaotic agglomeration of disparate tactical approaches. At the same time, it confirms the existence of a mature, formalized strategic doctrine that maintains its internal logic regardless of the platform environment in which it is deployed.

The **practical significance** of the results lies in their applicability to the activities of entities countering Russian information operations, as well as the integration of these materials into courses on media literacy, security studies, communications, and the analysis of Russian information operations. The findings may also prove beneficial to the professional activities of journalists and fact-checkers.

The dissertation consists of an introduction, four chapters, general conclusions, a list of references, and appendices. The total volume of the work is 274 pages, of which 215 pages constitute the main body text. The list of references includes 273 entries.

Keywords: information operations, information warfare, disinformation, social media, Russo-Ukrainian War, strategy, Russia, artificial intelligence, media space, propaganda, hybrid war, information security, influence operations, Ukraine, strategic communications

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. 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
2. Осадчук, Р. (2025). Російські дезінформаційні операції проти України під час широкомасштабного вторгнення: кейс-стаді. *Синопсис: текст, контекст, медіа*, 215. https://doi.org/10.28925/2311-259x.2025.3.10
3. Осадчук, Р. (2026). Теоретична рамка дослідження сучасних російських дезінформаційних операцій. *Обрії Друкарства*, (2026: Online first). https://doi.org/10.20535/2522-1078.2026.1(19).356053

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Osadchuk, R. (2024) The model of Russian disinformation after the large-scale invasion of Ukraine: The case of 'Ukraine sells Western arms' narrative. *ECREA 2024, 10th European Communication Conference Book of Abstracts*, p. 99-100. https://flore.unifi.it/bitstream/2158/1392253/1/ECREA-2024-Abstract-Book.pdf
2. Осадчук Р.Ю. (2025) Модель розповсюдження російської дезінформації. *Російська війна проти України: трансформації соціальних інституцій та практик: збірник тез науково-практичної конференції*, с. 28-32 https://ekmair.ukma.edu.ua/handle/123456789/36638
3. Осадчук, Р. Ю. (2023). Багатоступеневий підхід РФ у побудові і розповсюдженні дезінформації: приклад "продажу зброї". *Протидія дезінформації в умовах російської агресії проти України: виклики й перспективи: тези доповіді*, с. 277-281. https://doi.org/10.32782/PPSS.2023.1.72

Публікації, які додатково відображають наукові результати дисертації

1. Kalenský, J., & Osadchuk, R. (2024). *How Ukraine fights Russian disinformation: Beehive vs mammoth* (p. 48) [Hybrid CoE Research Report 11]. Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Російські інформаційні операції проти України та демократичних країн Заходу є досить нагальною та концептуально складною проблемою сучасних комунікаційних досліджень. Повномасштабне вторгнення Російської Федерації (РФ) в Україну 24 лютого 2022 року остаточно трансформувало інформаційний вимір російсько-української війни з допоміжного інструменту в невід'ємну її частину. В умовах такого «гібридного» протистояння інформаційні операції є нерозривною складовою кінетичних дій.

Актуальність обраної теми зумовлена щонайменше чотирма взаємопов'язаними факторами. По-перше, після вторгнення російські інформаційні операції мусили трансформуватися. На початку вторгнення традиційні пропагандистські джерела РФ були заблоковані у багатьох країнах, що зумовило масштабний перехід в онлайн. Таким чином,епізодичні кампанії в мережі Інтернет отримали більше уваги з боку РФ та почали свій шлях до побудови індустріалізованої архітектури. В умовах російсько-української війни імплементація стратегії інформаційних операцій перейшла від RT та інших державних установ до приватних підрядників, пов'язаних із Кремлем. Зокрема, цими організаціями є «Агенція соціального проєктування» (АСП) та Група компаній «Структура» (Структура), які мають зв'язки з Кремлем й детально проаналізовані у цій роботі. Зв'язки підрядників з Адміністрацією Президента РФ були підтверджені документально через наявні внутрішні документи організацій, які були опубліковані в матеріалах афідевіту Міністерства юстиції США та в декількох журналістських і аналітичних розслідуваннях (Department of Justice, 2024a; Belton et al., 2024; Morozova and Laine, 2024; Pamment and Tsurtsumia, 2025). Ця зміна організаційної моделі інформаційних операцій вимагає оновлення дослідницького інструментарію, який досі переважно орієнтувався на ідентифікацію окремих кампаній. Натомість потрібен комплексний підхід, сфокусований на аналізі екосистеми російської дезінформації.

По-друге, сучасний стан досліджень інформаційних операцій можна характеризувати як методологічно фрагментований, оскільки в дослідженнях відсутня інтегрована аналітична рамка. Наприклад, дослідження зі сфери комп'ютерних наук концентруються на технічній інфраструктурі інформаційних операцій. Тобто, на автоматизованому створенні акаунтів, координованій неавтентичній поведінці та мережевих структурах поширення контенту (Badawy et al., 2018; Varol et al., 2017; Woolley and Howard, 2018). У той час як дослідження у сфері медіа та комунікацій переважно зосереджуються на наративних стратегіях дезінформації. Ці дослідження аналізують дезінформаційний дискурс (Taranenko, 2023) та формування й використання наративних технік, як-от «стратегічних наративів» (Miskimmon et al., 2013). Окремим аспектом цих досліджень є вивчення фреймування подій державними акторами, а також використання концепції «потоку брехні» (Paul and Matthews, 2016). Дослідники психологічного рівня інформаційних операцій зазвичай аналізують когнітивні упередження, евристики та механізми поширення дезінформації серед звичайних споживачів та цільових аудиторій (Lewandowsky et al., 2012; Pennycook and Rand, 2021; Ecker et al., 2022). Кожен напрям випрацьовує цінні результати в межах власного аналітичного виміру, проте ігнорує взаємозв'язки з іншими. Проте, інтегрований характер сучасних російських інформаційних операцій формується зв'язками між технічними можливостями, наративними стратегіями та когнітивними наслідками.

По-третє, цифрове середовище, в якому розгортаються ці операції, демонструє безпрецедентну нестабільність. По-перше, дезінформація вільно мігрує між платформами (Telegram, TikTok, X, Facebook, тощо), ігноруючи кордони платформ та держав. По-друге, актори інформаційних операцій почали інтегрувати великі мовні моделі (ВММ) у виробництво синтетичного контенту (OpenAI, 2024). Оператори почали використовувати техніки ухилення від модерації, як «клоакінг» та сортування за географією (gofencing – англ.) (Châtelet and Osadchuk, 2024; Qurium Media Foundation, 2022). Насамкінець, недовговічність значної частини матеріалів, насамперед рекламних оголошень та відеоматеріалів, ускладнює будь-який аналіз. Повідомлення в будь-який

момент можуть бути видалені з платформи, не залишаючи слідів свого існування, попри те, що сотні й тисячі реальних користувачів могли їх побачити. Такий стан речей вимагає одночасно нових методологічних рішень для документування та моніторингу тимчасового (ефемерного) контенту, а також теоретичних підходів, здатних охопити кросплатформну архітектуру сучасних російських дезінформаційних операцій.

По-четверте, для України проблема дезінформації вже давно вийшла за рамки академічного й практичного значення, адже наразі має статус частини стратегічної безпекової доктрини. Внутрішня документація підрядників інформаційних операцій підтверджує спрямованість російських операцій у соціальних медіа на українську аудиторію. Основними завданнями цих операцій є «дискредитація військово-політичного керівництва», «розкол еліт», «деморалізація ЗСУ» та «дезорганізація населення» (Department of Justice, 2024a). Розуміння й знання цих цілей обумовлює потребу у зміні підходу до аналізу операцій й призводить до необхідності у виробленні емпірично обґрунтованих рекомендацій. Такі рекомендації можуть бути корисними державним інституціям, неурядовим організаціям та технологічним платформам, які працюють над побудовою стійкої протидії подібним кампаніям.

Сукупність зазначених факторів зумовлює актуальність розробки інтегрованого трирівневого аналітичного підходу, який включає технічний, наративний і когнітивний рівні. Цей підхід здатний одночасно концептуалізувати взаємозв’язки між інфраструктурою доставки контенту, його смисловою архітектурою та психологічними механізмами впливу. В цій роботі забезпечено також емпіричну верифікацію цього підходу на матеріалі сучасних російських інформаційних операцій..

Мета дисертаційного дослідження: з’ясувати на конкретних прикладах як реалізується стратегія інформаційних операцій РФ під час повномасштабного вторгнення (2022-2026).

Досягнення поставленої мети передбачає розв’язання таких **дослідницьких завдань**:

1) систематизувати категоріально-понятійний апарат дослідження інформаційних операцій та технік, які вони використовують (пропаганди, дезінформації, наративів, фреймів та координованої неавтентичної поведінки) в умовах цифрового медіасередовища та визначити місце дослідження в сучасному науковому полі;
2) обґрунтувати потребу в трирівневій аналітичній рамці, яка охоплює технічний, наративний та когнітивний рівні на основі огляду наявного методологічного інструментарію дослідження російських інформаційних впливів;
3) обґрунтувати методологію дослідження, що поєднує якісний аналіз стратегічних документів та кейс-стаді документально зафіксованих операцій як їхнього емпіричного прояву, застосувавши трирівневу аналітичну рамку (технічний, наративний, когнітивний рівні) для аналізу інформаційних операцій;
4) провести історичну реконструкцію інституційних і доктринальних витоків сучасних російських інформаційних операцій від інфраструктури «активних заходів» епохи Холодної війни до сучасних гібридних форм;
5) виокремити еволюцію державної та недержавної протидії інформаційним операціям для виявлення переваг і недоліків поточної системи відповіді на загрозу та виявити зміни логіки й державної архітектури інформаційних операцій у доктринальних документах інформаційної безпеки РФ;
6) реконструювати стратегічний рівень російських інформаційних операцій проти України після 2022 року на основі внутрішньої документації підрядників (АСП та Структури), виокремивши ключові стратегічні установки та внутрішню логіку;
7) з’ясувати як унікальний авторський корпус повідомлень операції «Двійник» демонструє реалізацію стратегії російського інформаційного впливу;

8) з’ясувати основні характеристики масштабної TikTok-операції проти представників української влади як прикладу реалізації стратегії інформаційних операцій, встановивши специфіку операції на трьох рівнях та розглянувши дифузію контенту на інших платформах;
9) провести комп’ютеризоване тематичне моделювання коментарів у Telegram, X та Facebook з метою індуктивного виявлення наративних кластерів, що просуваються через скоординовану неавтентичну поведінку;
10) зіставити виявлені емпіричні закономірності операцій з оприлюдненими внутрішніми документами російських дезінформаційних підрядників (АСП, Структура) задля встановлення механізмів реалізації стратегії інформаційних операцій РФ проти України, координаційних зв’язків між трьома кейсами та російськими підрядниками інформаційних операцій;
11) сформулювати практичні рекомендації для державних інституцій, неурядових організацій, навчальних закладів, дослідницьких центрів і технологічних платформ щодо протидії російським інформаційним операціям на технічному, наративному та когнітивному рівнях на основі академічних висновків з трьох кейсів.

Гіпотези дослідження

Емпірична частина роботи спрямована на верифікацію чотирьох дослідницьких гіпотез, які операціоналізують імплементацію стратегії інформаційних операцій РФ на матеріалі трьох кейсів сучасних операцій.

Гіпотеза щодо операції «Двійник» (Doppelganger) у Facebook:

- **Гіпотеза 1.** Російські інформаційні операції в українському сегменті соціальних медіа спрямовані на деморалізацію населення України шляхом систематичного підривання довіри до державних інституцій та міжнародних союзників через встановлення негативного порядку денного засобами рекламних повідомлень і меметичних конструкцій.

Гіпотеза щодо TikTok-операції зі звинуваченнями у корупції:

- **Гіпотеза 2.** Виявлені TikTok-відео є частиною скоординованої мережі неавтентичних акаунтів і відповідної операції впливу, а не ізольованим випадком дискредитації посадової особи.

Гіпотеза щодо координованої активності у коментарях в Telegram, X і Facebook:

- **Гіпотеза 3.** Скоординована діяльність у коментарях у досліджуваному корпусі переважно реалізує стратегію перенесення відповідальності за війну з Російської Федерації на Україну та країни Заходу й дискредитацію військово-політичного керівництва України

Загальна гіпотеза щодо координації між кейсами:

- **Гіпотеза 4.** Повідомлення, виявлені у трьох проаналізованих кейсах, корелюють із цілями, зафіксованими у внутрішніх документах російських дезінформаційних підрядників (АСП, Структура), що підтверджує їхню належність до спільної інституційної архітектури впливу.

Об’єкт дослідження — інформаційні операції Російської Федерації проти України, що здійснюються в період після початку повномасштабного вторгнення (2022-2026 рр.).

Предметом дослідження є стратегія інформаційних операцій, реконструйована за матеріалами внутрішньої документації російських суб'єктів інформаційних операцій у її співвідношенні з прикладами реалізації у різних цифрових середовищах.

Методи дослідження. Для досягнення поставленої мети та розв’язання дослідницьких завдань у роботі застосовано комплекс взаємодоповнювальних методів, обраних відповідно до специфіки предмета та логіки трирівневої аналітичної рамки.

Загальнонаукові методи. Застосовано *історико-генетичний* метод для реконструкції доктринальних витоків російських інформаційних операцій від «активних заходів» до сучасних форм російської дезінформації. Цей метод дозволив обґрунтувати тезу про спадковість стратегічної логіки з радянських часів. *Системно-структурний* підхід використано для концептуалізації трирівневої рамки як інтегрованої системи для

аналізу інформаційних операцій. *Порівняльний метод* застосовано як для зіставлення трьох емпіричних кейсів між собою для пошуку зв'язків через контент та цілі. також цей метод було використано для співвіднесення практичної реалізації стратегії з доктринальними документами, що описують стратегію інформаційного впливу РФ.

Якісні методи дослідження медіа. Застосовано *метод покрокового огляду стрічки*, який був концептуалізований та апробований Light, Burgess та Duguay (2016) та розширений Duguay та Gold-Apel (2023). Цей метод використано для аналізу інтерфейсу соціальних платформ Facebook і TikTok задля збору релевантного контенту інформаційних операцій впливу. Використано *аналіз цифрових артефактів* (Krafft and Donovan, 2020) для систематизації авторського корпусу 649 скриншотів повідомлень операції «Двійник». *Контент-аналіз* (Krippendorff, 2019) застосовано для систематичної категоризації наративного матеріалу у повідомленнях та публікаціях. *Критичний дискурс-аналіз* (Fairclough, 2013; van Dijk, 2008) використано для виявлення стратегій делегітимізації в російських інформаційних повідомленнях на різних платформах.

Методи розвідки відкритих джерел і верифікації. Для дослідження кейсів було застосовано *мультимодальний метод детекції місінформації* (Barve et al., 2023), *методологію верифікації мультимедійних документів* (Khan et al., 2025) та *аналіз патернів неавтентичної поведінки*. Ці методи дозволили виявити та верифікувати дезінформаційні публікації. Документування ефемерного контенту було проведено *методом збереження скриншотів* (Hayden et al., 2024; Inwood and Zappavigna, 2024). Це дозволило зберегти рекламні повідомлення та відеоматеріали, які згодом були видалені платформами.

Змішані та комп'ютеризовані методи. Загальна архітектура емпіричного дослідження TikTok-операції відповідає *розвідувально-послідовному змішаному дизайну* (Creswell, 2014). Він передбачав пошук окремих прикладів інформаційної операції для визначення патернів, які уможливили подальший аналіз і систематизацію схожих повідомлень. Тематичне моделювання корпусу з 32561 коментаря трьох соціальних мереж (Telegram, Facebook, X) було виконано методом комплексного *тематичного*

моделювання BERTopic (Grootendorst, 2022; Turton et al., 2021). Підхід складався з чотирьох послідовних обчислювальних етапів. По-перше, було використано семантичне векторне представлення коментарів засобами багатомовної моделі трансформера paraphrase-multilingual-mpnet-base-v2 (Hugging Face, 2019). Далі було знижено вимірність методом UMAP (McInnes et al., 2018). На наступному кроці було використано кластеризацію на основі щільності методом HDBSCAN (Campello et al., 2013). Насамкінець, теми було репрезентовано через c-TF-IDF (Grootendorst, 2022) з використанням методу максимальної граничної релевантності (Maximal Marginal Relevance – англ.) (Goldstein and Carbonell, 1996). Ця комбінація методів обрана з огляду на потребу одночасно охопити двомовний (український та російський) корпус коментарів і виявити теми, які обговорювалися в масиві даних. Далі ці теми було індуктивно сформовано у наративні кластери без апріорної таксономії й усталеної кількості кластерів.

Метод тріангуляції. Для того, щоб встановити зв'язки між трьома прикладами інформаційних операцій та їхнім зв'язком із російськими інституціями, було застосовано розвідку відкритих даних і тріангуляцію джерел. Тобто було зіставлено емпіричні патерни проаналізованих операцій з оприлюдненими внутрішніми документами АСП і Структури задля реконструювання практичної реалізації стратегії РФ (Department of Justice, 2024a; Belton et al., 2024).

Обґрунтованість обраного методологічного комплексу полягає в тому, що жоден окремий метод не здатний самостійно охопити весь спектр навіть кількох сучасних російських інформаційних операцій. Це пов'язано з їхньою гібридною, кросплатформною та технологічно мінливою природою, яку важко охопити. Тому інтеграція якісних, комп'ютеризованих та OSINT-методів є критичною для аналізу комплексних операцій. Ця комбінація дає змогу одночасно аналізувати інфраструктуру операцій, наративну архітектуру та оцінювати когнітивний потенціал впливу.

Наукова новизна отриманих результатів. Наукова новизна дисертаційного дослідження полягає у тому, що:

Вперше:

- здійснено системний аналіз стратегічного рівня російських інформаційних операцій проти України на основі витоків внутрішньої документації АСП та Структури із зіставленням реконструйованої стратегії з емпірично задокументованими прикладами її реалізації, що дозволило простежити реалізацію стратегічного задуму;
- розроблено та емпірично застосовано трирівневу аналітичну рамку (технічний, наративний, когнітивний виміри) як інтегрований інструмент аналізу трьох контрастних кейсів російських інформаційних операцій, що уможливило зчитування реалізації стратегії одночасно в інфраструктурному, змістовному та психологічному вимірах як взаємопов'язаної системи, на відміну від наявних підходів, що зазвичай розглядають один із цих аспектів ізольовано;
- уведено в науковий обіг унікальний авторський корпус із 649 скриншотів повідомлень російської операції «Двійник» в Україні. Повідомлення були зібрані протягом січня–липня 2024 року методом покрокового огляду стрічки. Абсолютна більшість повідомлень були видалені з платформи Facebook, є недоступними зараз та раніше не були предметом наукового аналізу;
- продемонстровано як єдиний стратегічний задум зазнає принципово різної тактичної реалізації залежно від типу цифрової платформи, на якій реалізується операція, що визначено як характеристику російських інформаційних операцій після 2022 року;
- здійснено багатоканальну атрибуцію трьох емпірично різних російських операцій, а саме «Двійник» у Facebook, операції з відео у TikTok та координованих коментарських мереж, до спільної інституційної архітектури

АСП і Структури через зіставлення з афідевітом Міністерства юстиції США та внутрішніх документів цих організацій та виявлення спільної бази меметичного контенту, що використовувалася в різних операціях.

Удосконалено:

- понятійно-категоріальний апарат інформаційних операцій шляхом інтеграції міжнародних аналітичних стандартів (DISARM, ABC) із теоріями комунікацій та доктринальною спадщиною РФ з часів «активних заходів»;
- методологію дослідження державних інформаційних операцій через поєднання якісного аналізу стратегічних документів та кейс-стаді реалізації цієї поведінки.

Набули подальшого розвитку:

- концепція кросплатформної дифузії дезінформаційних повідомлень у логіці моделі «потоку брехні». Вона була доповнена доказами міграції контенту операцій між TikTok, Telegram і X у формі вторинних адаптацій з перекладами на інші мови;
- теза про спадковість російських інформаційних операцій як стратегічної традиції, яка відтворює базові принципи радянських «активних заходів» в умовах нової технологічної інфраструктури;
- осмислення інформаційних операцій РФ як структурного компонента гібридної війни проти України, зокрема в частині співвідношення між стратегією й тактичною реалізацією.

Особистий внесок здобувача. Усі основні наукові результати, винесені на захист, отримані здобувачем особисто. Авторові належать:

- аналіз доктринальних документів РФ та внутрішніх документів АСП та Структури задля виявлення стратегії сучасних інформаційних операцій РФ;
- розробка інтегрованої трирівневої аналітичної рамки на основі військових доктрин США та НАТО;

– збір і систематизація унікального корпусу 649 скриншотів рекламних повідомлень операції «Двійник» в Україні методом покрокового огляду стрічки протягом січня–липня 2024 року;
– проєктування та реалізація обчислювального наративного аналізу 32561 коментаря на основі BERTopic, а також інтерпретація отриманих 125 тем та їх об'єднання у сім наративних кластерів;
– застосування методів OSINT-верифікації, мультимодальної детекції та аналізу дифузії у кейсі TikTok-операції;
– зіставлення виявлених емпіричних патернів операцій з оприлюдненими внутрішніми документами російських дезінформаційних підрядників;
– формулювання рекомендацій щодо протидії російським інформаційним операціям на технічному, наративному та когнітивному рівнях.

У публікаціях, виконаних у співавторстві, особистий внесок здобувача полягає в такому:

– Châtelet and Osadchuk (2024): концептуалізація методології аналізу клоакінг-технік, ідентифікація патернів географічного фільтрування контенту в українському сегменті операції «Двійник», збір емпіричного матеріалу;
– Kalenský and Osadchuk (2024): систематизація рекомендацій щодо інституційної протидії російській дезінформації для демократичних країн, аналіз українського кейсу та порівняльний аналіз механізмів протидії;
– Osadchuk et al. (2024): розробка методологічної рамки виявлення координованої неавтентичної поведінки в коментарях соціальних мереж, обробка та аналіз масиву понад 580000 коментарів, аналіз одиничних коментарів, концептуалізація кросплатформного дизайну дослідження;

Gigitashvili and Osadchuk (2022): аналіз російського наративу про так звані «біолабораторії» та інші повідомлення як *casus belli*, а також документування використання історичних дезінформаційних шаблонів у передвоєнний період.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано на кафедрі «Могилянська школа журналістики» факультету соціальних наук та соціальних технологій Національного університету «Києво-Могилянська академія» в межах науково-дослідної теми «Соціальні комунікації в умовах цифрових трансформацій: інформаційні впливи, дезінформація та виклики для професійних практик і стандартів журналістики» (державний реєстраційний номер: 0125U003879).

Практичне значення отриманих результатів. Практичне значення дисертації визначається тим, що отримані результати створюють емпіричну та концептуальну основу для діяльності низки суб'єктів протидії російським інформаційним операціям.

По-перше, трирівнева аналітична рамка та методологічний інструментарій можуть бути використані державними, дослідницькими та аналітичними центрами, неурядовими організаціями, а також підрозділами стратегічних комунікацій для систематизованого для розробки методичних рекомендацій із моніторингу, ідентифікації, атрибуції та оцінки російських інформаційних операцій. Запропонований підхід до аналізу реалізації стратегії одночасно на технічному, наративному та когнітивному рівнях дозволяє відмовитися від реагування на окремі тактики на користь системної протидії, орієнтованої на стратегічний задум супротивника.

По-друге, систематизовані та доповнені рекомендації щодо протидії інформаційним операціям на трьох рівнях на основі проаналізованих кейсів. Ці напрацювання можуть бути використані державними, приватними та неурядовими організаціями.

По-третє, комп'ютеризований підхід наративного аналізу (BERTopic-архітектура з багатомовним творенням векторів, UMAP-зниженням розмірності та HDBSCAN-кластеризацією) є відтворюваним і може застосовуватися для оперативного аналізу нових масивів коментарів у двомовному (українсько-російському) інформаційному просторі.

По-четверте, авторський архів 649 скриншотів операції «Двійник» в Україні та аналіз операції у ТікТок мають документальну цінність. Цей емпіричний матеріал є

унікальним, адже він представляє сліди російських інформаційних операцій, які вже видалені платформами. Тому цей масив даних може бути використаний у подальших порівняльних дослідженнях та освітніх програмах.

По-п’яте, результати дослідження мають освітнє застосування в межах університетських та практичних курсів з медіаграмотності, безпекових студій, комунікацій та аналізу російських інформаційних операцій, а також у програмах підвищення кваліфікації фахівців з комунікацій державного й недержавного секторів.

Апробація результатів дисертації. Основні положення та результати дисертаційного дослідження доповідалися та обговорювалися на 8 міжнародних, всеукраїнських та регіональних конференціях протягом 2022-2026 років. Зокрема, в рамках:

- Десятої міжнародної конференції Європейської асоціації досліджень комунікацій та освіти (ECREA) у м. Любляна, Словенія, 25 вересня 2024 р., де була представлена доповідь англійською мовою на тему: «The model of Russian disinformation after the large-scale invasion of Ukraine: The case of ‘Ukraine sells Western arms’ narrative»;
- Воркшопу Спільного дослідницького центру Європейської Комісії (European Commission’s Joint Research Center) «DISINFO Workshop», м. Брюссель, Бельгія, 25 вересня 2025 р., де була представлена доповідь англійською мовою на тему: «AI as a tool of disinfo weaponization»;
- Міжнародної конференції «The Russo-Ukrainian War: Russia’s information warfare strategies in comparative perspective» (https://ruwconference.ca/) у м. Оттава, Канада, 21-22 лютого 2025 року, де була представлена доповідь англійською мовою на тему: «Russian disinformation campaigns against Ukraine during the full-scale invasion»;
- Наукової конференції «Революція Гідності: на шляху до історії» в Національному музеї Революції Гідності, м. Київ, Україна, 21 листопада

2023 р., де відбулась презентація на тему: «Еволюція російської дезінформації та асиметрична відповідь України»;

- Наукового семінару Харківського національного університету Повітряних Сил імені Івана Кожедуба (ХНУПС) «Інформаційне протиборство в умовах російсько-української війни», 30 листопада 2023р., м. Харків (онлайн), Україна, де була представлена доповідь на тему: «Багатоступеневий підхід російської дезінформації»;
- Панельної дискусії під назвою: «Russia's hybrid war through different channels, tools, and continents» в рамках конференції «Unveil the truth: Eastern Partnership fact-checking conference» у м. Тбілісі, Грузія, 12 вересня 2024р.;
- Двох панельних дискусій «Tip of the Spear: A report from the frontlines of the war on disinformation» та «Red Flags: Russia's & China's influence operations around the world» під час міжнародної конференції «#Connexions 24. Extreme in the Mainstream: Information Disorder, (Dis)engagement, & Digital (R)evolution», Університету Техасу (University of Texas), м. Остін, Штат Техас, США, 18-20 березня 2024;
- Глобальної інформаційної конференції Департаменту оборони США (Department of Defense Global Information Conference) під назвою: «Forging The Future: from strategy to action» у м. Вашингтон, Округ Колумбія, США, 12-14 березня 2024 р., де був виступ з темою: «Massive Russian influence operation targeted former Ukrainian defense minister on TikTok».

Публікації. Основні результати дисертаційного дослідження висвітлено у 6 наукових публікаціях здобувача, а саме: 3 статтях у фахових наукових виданнях України категорії «Б», 3 матеріалах доповідей наукових конференцій. До того ж, результати дослідження були опубліковані у 3 аналітичних звітах міжнародних дослідницьких інституцій та 5 брифінгах аналітичного центру DFRLab (США). Фахові публікації та доповіді на наукових конференціях здійснені автором самостійно. Інші публікації частково висвітлювали окремі результати цього дослідження.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів (з підрозділами), висновків та списку використаних джерел. Також у роботі містяться додатки.

Перший розділ «Теорії інформаційних впливів та концепції дезінформаційних практик» містить два підрозділи: синтезування теорій інформаційних впливів та концепцій дезінформаційних практик; систематизацію базових понять та допоміжних категорій апарату інформаційних операцій та пропаганди. Цей розділ представляє проблематику дослідження, поточні теоретичні рамки досліджуваної тематики та категорії, які використовуються в інформаційних операціях.

Другий розділ «Методологічні засади дослідження інформаційних впливів Росії у медійній сфері» містить три підрозділи: критичний огляд актуальних методів дослідження російського інформаційного впливу; аналіз ключових категорій медіа та напрямків дослідження; обґрунтування методології авторського емпіричного дослідження російських інформаційних операцій. Цей розділ представляє проблематику дослідження, вводить рамку для аналізу інформаційних операцій, а також описує методи дослідження частин інформаційних операцій РФ.

Третій розділ «Стратегія російських інформаційних операцій» реконструює стратегічну спадковість російської інформаційної традиції від апарату «активних заходів» до сучасних гібридних форм. Цей розділ поглиблює визначення проблематики та спадковості сучасних інформаційних операцій впливу, які продовжують традиції та підходи, опрацьовані Росією десятиліттями в рамках «активних заходів», та адаптують їх до сучасності. Другий підрозділ описує еволюцію й становлення протидії російським інформаційним операціям. Наступний підрозділ детально демонструє зміни у стратегічних документах РФ, які регулювали сферу інформаційного протиборства та інформаційних операцій. Цей підрозділ демонструє, як РФ формувала концепцію «контр-заходів» для протидії іншим країнам. Фінальний підрозділ аналізує внутрішню документацію підрядників російських інформаційних операцій АСП та Структури задля визначення стратегічного задуму та можливої реалізації доктринальних документів.

Четвертий розділ дослідження під назвою «Аналіз сучасних російських операцій в Україні та країнах Заходу» містить емпіричний аналіз трьох кейсів: рекламної операції «Двійник» (Doppelganger) у Facebook, кросплатформної TikTok-кампанії зі звинуваченнями посадових осіб України у корупції та координованої активності у коментарях в Telegram, X і Facebook. Цей розділ встановлює зв'язки між кампаніями та, на основі даних, формулює рекомендації щодо протидії таким операціям для різних стейкхолдерів.

Загальний обсяг дисертації становить 274 сторінки, з яких 215 сторінок основного тексту. Список використаних джерел налічує 273 позиції. Також є 4 додатки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ РАМКИ ТА КОНЦЕПТУАЛЬНИЙ ВИМІР ІНФОРМАЦІЙНИХ ВПЛИВІВ

1.1 Теорії інформаційних впливів та концепції дезінформаційних практик

Перед дослідженням сучасних інформаційних впливів варто почати зі стану розробки цієї теми у науковому середовищі. Сучасний інформаційний простір дає змогу використовувати різні підходи, теорії та способи розуміння того, як відбувається вплив через інформацію. Поточні напрацювання у сфері комунікацій, безпекових студій, психології та пропаганди є досить фрагментарними й описують лише окремі складові феномену інформаційних операцій. З огляду на міждисциплінарність поняття інформаційних операцій та сфер його застосування, доцільним є поєднання теорій медіаефектів, теорії сучасного медійного середовища, а також теорій сприйняття й обробки інформації, що співіснують і доповнюють одна одну. До того ж, для розуміння інформаційних операцій потрібно виходити за межі теорій і використовувати наявні практичні типології, моделі функціонування дезінформаційних систем та визначення політик платформ і держав для позначення характерних аспектів інформаційних операцій.

У рамках вивчення інформаційних впливів існує кілька рівнів теорій, що описують це явище. Серед них як класичні теорії (встановлення порядку денного, фреймінг), так і спроби описати сучасне медійне середовище (інформаційний безлад, «потік брехні») або ж аналітичні концепції для опису такого впливу (координована неавтентична поведінка, іноземна маніпуляція інформацією та втручання). Тому в цьому розділі буде реконструйовано всі ці рівні теорії, щоб виявити прогалини в поточних напрацюваннях.

Фундаментальною теоретичною концепцією є «теорія порядку денного» (agenda-setting), яку оригінально запропонували дослідники McCombs та Shaw (1972). У своєму початковому формулюванні дослідники продемонстрували, що значущість тем у новинному висвітленні переноситься на значущість цих тем у свідомості аудиторії.

Таким чином, медіа безпосередньо не вказують людям, що думати, але підштовхують до того, про що думати (McCombs and Shaw, 1972). Пізніше дослідники розширили цю концепцію подальшими дослідженнями порядку денного другого рівня (McCombs et al., 1997). На цьому рівні медіа передають значущість конкретних характеристик та оцінки подій. Тобто, вони не тільки говорять «про що думати», а й додають фрейм цим темам, впливаючи на те, «як про це думати». До того ж, у цьому контексті важливою є теорія культивації, згідно з якою медіа формують розуміння світу у цільової аудиторії (Gerbner et al., 1978).

Важливим є визнання того, що сучасні інформаційні операції відбуваються в умовах гібридної медійної системи (Chadwick, 2013). Чедвік описує сучасне інформаційне середовище як сукупність традиційних та нових медіа. Тобто, в цій системі соціальні мережі є такими ж важливими, як і традиційні медіа, й можуть впливати на порядок денний користувачів та читачів. Ця гібридизація дозволяє акторам здійснювати свій вплив через мережу розгалужених повідомлень, які не завжди можна прив’язати до конкретного актора, як у прикладі з коментарями в соціальних мережах. У той же час інформаційні операції експлуатують асиметричну структуру медійних систем країн-цілей (Benkler et al., 2018). Шкідливі актори адаптують свої стратегії до різних кластерів, які можуть бути ізольованими, мати внутрішні упередження, не мати запобіжників перевірки інформації та сприймати її за ідеологічним співпадінням. Всередині таких кластерів медійної системи дезінформація може швидко масштабуватися.

До того ж оновлення моделі порядку денного запропонувала Гуо (Guo, 2014), а саме мережевий порядок-денний, що є третім рівнем. Згідно з ним, медіа (у широкому розумінні) передають не лише лінійні факти, а й складніші зв’язки та відношення між атрибутами події чи персони. Таким чином, джерела інформації об'єднують об'єкти та атрибути в асоціативні кластери, які формують мислення аудиторії. У подальших дослідженнях мережевого порядку денного (Liu et al., 2022) було встановлено, що позасистемні інфлюенсери іноді були навіть більш значущими для формування

розуміння подій. На формування цих асоціативних зв'язків між реальними явищами та людьми й працюють інформаційні операції, адже вони не завжди намагаються переписати, про що саме думати, а використовують вже наявні популярні теми й роблять певні аспекти явищ більш значимими через повторення.

Додатковим розширенням цієї концепції є злиття порядків денних (agenda-melding), згідно з яким індивіди активно поєднують різноманітні порядки денні з різних джерел (McCombs et al., 2014). Цими джерелами можуть бути традиційні медіа, соціальні мережі або локальні спільноти. Таким чином, кожна людина конструює цілісну картину світу, яка задовольняє її потребу в належності до різних груп. Злиття порядків денних пояснює, чому аудиторія в різних закритих чи периферійних спільнотах фактично допомагає створювати образи того, що відбувається навколо. Для організаторів інформаційних операцій злиття порядків денних означає, що успішне впровадження контенту потребує його сумісності з уже наявним у цільової аудиторії баченням світу. Цей підхід найчастіше використовується для впливу через коментарі у соціальних мережах, що продемонстровано в останньому кейс-стаді.

Однією з інтегральних частин порядку денного є використання наративів. Наратив — це структурована інтерпретаційна рамка, що впорядковує події, дійових осіб та набір цінностей у цілісні історії, які мають сенс. Тобто, мова йде не про окремі повідомлення, а радше про системну рамку, крізь призму якої можна пояснити ту чи іншу подію (Halverson et al., 2011). В аналізі медіа та пропаганди, наративи функціонують як системи сенсів, що пропонують та дозволяють аудиторії сформувати чи навіть нав'язати причинно-наслідкові пояснення та моральні оцінки щодо певних подій. Для інформаційних операцій та державного впливу ключовим є концепція «стратегічного наративу», описана Miskimmon et al. (2013). Під стратегічним наративом розуміється стратегічний наратив як «*репрезентацію послідовностей подій та ідентичностей, що пропонують аудиторії рамку для надання сенсів подіям*» (Miskimmon et al., 2013, с.5), зокрема стосовно міжнародних акторів та їхніх намірів. Наративи посідають центральне місце в операціях впливу, оскільки вони фактично узгоджують численні повідомлення

на різних платформах й створюють певну рамку сприйняття. Таким чином, замість того, щоб переконувати за допомогою окремих одиничних тверджень, пропагандистська машина діє шляхом подання інформації крізь повторювані наративи (наприклад, про «зовнішню загрозу» чи «моральний занепад»). Концептуально, наративи перебувають на вищому рівні абстракції, ніж окремі повідомлення, та є «містком» та історією, яка категоризує акторів як «злодіїв», «жертв», або «героїв».

Важливим елементом інформаційних впливів є «фреймінг». Фрейми (або рамки) — це специфічні способи подання інформації, які акцентують увагу на одних аспектах реальності, одночасно приховуючи або применшуючи значення інших, щоб сприяти конкретному визначенню проблеми або її інтерпретації (Entman, 1993; Chong and Druckman, 2007). Простіше кажучи, якщо наратив — це історія, яка пояснює певні події, то фрейм — це збільшувальне скло чи лінза, яке надає більшої ваги певним аспектам цієї історії. У той час як наративи пропонують всеосяжні сюжетні лінії, фрейми спрямовують інтерпретацію точкових подій. Один і той самий наратив може підтримуватися кількома фреймами. Наприклад, подія (широкомасштабне вторгнення РФ в Україну) може бути пояснена (фреймована) як «загроза національній безпеці РФ», «крах дипломатії та Заходу», «агресія Заходу», але пояснена через наратив «фортеці, яка оточена ворогами й мусить захищатись». У дослідженнях інформаційних операцій фреймінг є особливо важливим для розуміння того, як аудиторію підштовхують до певних висновків, інтерпретацій та упереджень, не обов’язково з використанням неправдивої інформації.

Наявність специфічних наративів та фреймів може сприяти ілюзії консенсусу в соціальних мережах у користувачів і впливати на їхню комунікацію та бажання висловлювати думку. Цю динаміку описує теорія спіралі мовчання (Noelle-Neumann, 1993), згідно з якою індивіди безперервно сприймають клімат думок. Люди це роблять через страх соціальної ізоляції і таким чином стримують погляди, які, на їхню думку, є побічними та непопулярними. У контексті гібридної системи (Chadwick, 2013) така оцінка спирається, зокрема, на очевидні індикатори, як-от кількість коментарів, реакцій і репостів. Саме цю вразливість експлуатують оператори інформаційних операцій через

координовану неавтентичну поведінку. Мережі ботів та бригади тролів впливають на кількісні індикатори, на основі яких користувачі роблять висновки про думку більшості, запускають реальні спіралі мовчання серед автентичних користувачів, які спираються на цю думку перед поширенням. (Hampton et al., 2014). Ба більше, у деяких випадках користувачі можуть поширювати інформацію, з якою не згодні (Haug et al., 2025) через страх ізоляції, який намагаються нав'язати шкідливі актори. У той же час, за умов анонімності ця теорія може не підтверджуватися у певних контекстах (Porten-Cheé and Eilders, 2015).

В рамках формування цих індикаторів важливо згадати про концепцію *координованої неавтентичної поведінки* (coordinated inauthentic behavior, CIB – англ.), яка була офіційно прийнята компанією Meta як політика з 2018 року (Meta, 2018). Згідно з політиками Мета це поведінка, яка є одночасно 1) координованою (залучає не одного, а кількох акторів, що діють узгоджено), тобто, це має бути не одна сторінка, а набір акаунтів чи сторінок у соціальних мережах; 2) неавтентичною (викривлює походження або популярність контенту); та такою, що 3) порушує правила платформи (суперечить умовам надання послуг) та (4) є фактично поведінкою. Тобто, цей концепт не є теорією в широкому розумінні, але є дороговказом для платформ та дослідників інформаційних операцій у вивченні й виявленні аспектів таких операцій на платформах соціальних мереж. Це визначення було сформовано під впливом дослідження російського втручання у вибори у США 2016 року. Проте це технічне визначення вписується в ширшу дослідницьку традицію аналізу того, що Starbird et al. (2019) називають «інформаційними операціями», тобто структурованими спробами маніпулювати інформаційним середовищем через стратегічне розгортання сфабрикованих або викривлених сигналів. Для такого викривлення, зокрема, використовуються бот-мережі та тролі.

Окрім такої поведінки, існує також проблема визначення неправдивого контенту, яка стала досить актуальною після 2016 року. У сучасному науковому та політичному дискурсі загальноприйнятною є система, яку запропонували й систематизували Клер

Вордл (Claire Wardle) та Хоссейн Дерахшан (Hossein Derakhshan) у 2017 році у звіті для Ради Європи (Wardle & Derakhshan, 2017). Вони запропонували концепцію «*інформаційного безладу*» (information disorder), яка включає різні типи неправдивого контенту, а також ввели в обіг таку класифікацію: «місінформація» (misinformation), «дезінформація» (disinformation) та «малінформація» (malinformation), які є ключовими для розуміння динаміки сучасного хаотичного інформаційного середовища.

Місінформація це хибна або неточна інформація, що поширюється без безпосереднього наміру завдати шкоди (Tandoc et al., 2018). Основним критерієм для цього визначення є саме відсутність умислу нанести шкоду іншим, що включає багато різноманітних ситуацій. Наприклад, особи, які поширюють місінформацію, можуть вважати вміст правдивим й таким, що вартує поширення, проте, в той же час, неправильно тлумачити контекст повідомлення або ж несвідомо посилюючи зманіпульовані наративи, пропаганду чи дезінформацію з щирою вірою в таку інформацію. Місінформацію доцільно розуміти як нестратегічний компонент інформаційного безладу, який працює на користь шкідливим акторам в інформаційних операціях. Місінформація виникає в інформаційних системах як побічний продукт уявлень та когнітивних упереджень індивідів, низького рівня медіа- та цифрової грамотності, а також підбору інформації алгоритмами й високій швидкості та інтенсивності потоку інформації, який люди споживають щоденно. Втім, місінформація все одно може нанести шкоду як вектор для розповсюдження пропаганди та дезінформації, бо може слугувати як вдале джерело ефективного розповсюдження інформації, яку запускають шкідливі актори.

Дезінформація це хибна інформація, яка свідомо створюється та поширюється з наміром ввести в оману або завдати шкоди (Wardle & Derakshan, 2017; Chadwick and Stanyer, 2022). Саме намір нанести шкоду є головним елементом цього типу інформаційного безладу. Ця концепція походить від радянського терміна «дезінформація», який позначав таємну державну діяльність, спрямовану на вплив на громадську думку або політичні системи інших країн (Rid, 2020). У сучасній науковій

літературі дезінформація включає в себе діяльність як державних, так і недержавних організацій, включаючи кампанії впливу на вибори та інші демократичні процеси та інституції, а також інформаційні операції, спрямовані на дискредитацію окремих осіб, організацій або країн. Дезінформація відрізняється від місінформації не лише наявністю наміру, але й своїм стратегічним характером. Вона часто розробляється з метою досягнення конкретних політичних чи економічних цілей й часто вбудовується у ширші й стратегічні операції впливу. Таким чином, дезінформація є ключовою категорією інформаційного впливу, функціонуючи як один із основних інструментів, за допомогою яких суб'єкти маніпулюють суспільним сприйняттям й впливають на інформаційне середовище, а з ним й на прийняття рішень. При цьому, мотивація використання дезінформації є різною від ідеологічних мотивів та дестабілізації опонентів до фінансової вигоди (Hameleers, 2023).

Малінформація — це достовірна інформація, яка поширюється з наміром завдати шкоди. На відміну від попередніх двох типів інформації, які обов'язково є хибними або містять елементи неправди, малінформація не передбачає брехні, проте натомість завдає шкоди внаслідок вибірковості контексту чи оприлюднення лише частини інформації. Відповідно до звіту (Wardle & Derakshan, 2017), ця категорія охоплює такі практики, як оприлюднення (витоки) приватних комунікацій, спрямованих на шкоду репутації організації чи особи, використання автентичних матеріалів разом з перебільшенням, або ж витік персональних даних (доксінг) з метою, наприклад, залякування. Малінформація ускладнює традиційне визначення пропаганди, оскільки ігнорує критерій правдивості попри свою шкідливість. Зазвичай вважається, що пропаганда передбачає викривлення інформації, однак малінформація є маніпулятивним способом використання саме правдивої інформації. Таким чином, малінформація є частиною гібридних загроз та операцій впливу, адже може використовуватись для підриву довіри до інституцій, залякування осіб чи впливу на політичні процеси.

Важливим доповненням до цих категорій інформаційного безладу є поняття політики Європейського Союзу — «іноземне маніпулювання інформацією та

втручання» (Foreign Information Manipulation & Interference, або FIMI – англ.). Згідно з визначенням Служби зовнішньої діяльності Європейського Союзу, FIMI описує здебільшого «легальну модель поведінки, яка загрожує або має потенціал негативно впливати на цінності, процедури та політичні процеси» (EEAS, 2023, с.4). Така діяльність має «маніпулятивний характер, проводиться навмисно та координовано державними або недержавними акторами, включно з їхніми проксі-силами як усередині, так і за межами власної території» (EEAS, 2026, с.4). Отже, FIMI фактично пояснює як розповсюдження дезінформації та місінформації може впливати на внутрішні процеси іноземних держав й намагається визначити такий вплив, щоб віднайти шляхи ефективної протидії.

Одним із головних акторів, який проводить FIMI в Україні та країнах Європи, є РФ, що стало особливо помітно після незаконної анексії Криму. Узагальнено підхід РФ до дезінформаційних операцій з 2014 року найкраще описано в моделі «потоку брехні» (firehose of falsehood), запропонованій Paul та Matthews (2016). Модель якісно відрізняється від класичного західного розуміння комунікацій й активних заходів радянських часів. Пропаганда та «активні заходи» прагнули переконати аудиторію у важливості та правдивості конкретних тверджень через удавану аргументацію. У свою чергу, модель «потоку брехні» надає пріоритет обсягу, швидкості та різноманіттю повідомлень, ігноруючи достовірність і якість цих повідомлень. Цей підхід підриває саму здатність цільової аудиторії до розуміння процесів та подій (Hutchings, 2024, с.157–158). Таким чином, він підважує суспільний консенсус щодо того, що взагалі може бути правдивим. Згідно з моделлю потоку, росіяни перенасичують інформаційне середовище суперечливими твердженнями та конспірологічними поясненнями задля дезорієнтації аудиторії.

Paul & Matthews (2016) визначили чотири ключові характеристики цієї моделі. Перша — це великий обсяг і багатоканальне розгортання: повідомлення поширюються через якомога більшу кількість каналів задля повторної появи перед очима аудиторії, що збільшує довіру (Pennycook & Rand, 2021). Це якісний перехід від традиції «активних

заходів», бо окрім керованого списку фронт-організацій та журналістів насичення простору відбувається контентом без вибірковості на багатьох платформах одночасно. Друга — це оперативна, безперервна й повторювана доставка контенту в реальному часі. Для якісних підробок у цій моделі часу немає, а будь-які фактичні неточності чи помилки приймаються як ціна оперативного темпу. Швидкість для повідомлень є визначальною, оскільки людям властиві «якірні» упередження та упередження «першості» (інформацію, яку людина отримала «першою», важко викорінити). Третя характеристика — фактична відсутність прив'язки до об'єктивної реальності: контент не обов'язково підтверджується фактами, як, наприклад, у випадку «дівчини Лізи» (Meister, 2016), яка нібито зазнала насильства у Німеччині. Ця історія спровокувала протести й суспільний резонанс, особливо серед російськомовного населення, але була вигадкою. Четверта й фінальна характеристика — відсутність прагнення до несуперечливості й послідовності. У цій системі суперечливі наративи розгортаються паралельно, оскільки метою є дезорієнтація. Еталонним прикладом є збиття літака MH17, у виправдання якого за 4 роки EUvsDisinfo назбирав 120 прикладів дезінформації (EUvsDisinfo, 2019), включно з теоріями про «мертвих» пасажирів на борту до вибуху та конспірологією, що це був інший літак. У той же час, дослідження Vosoughi et al. (2018) у Science емпірично продемонструвало, що неправдива інформація поширюється набагато швидше за достовірну: ігноруючи істину й цілісність, ставлячи на швидкість, модель «потоку» отримує структурну перевагу у сучасних медійних системах. До того ж, когнітивне перевантаження, що виникає внаслідок надвеликого обсягу інформації, знижує здатність аудиторії до критичного опрацювання та змушує спиратися на евристики, як-от упередження підтвердження, соціальний доказ, авторитетність джерела тощо (Kahneman, 2013).

Теорією, яка б пояснювала сприйняття індивідами інформації, є модель ймовірності свідомої обробки інформації (*Elaboration Likelihood Model*, ELM), яку описали Petty та Cacioppo (1986). Теорія ELM передбачає обробку інформації індивідом за допомогою одного з двох шляхів — швидкого (периферійного) або повільного

(аналітичного) (O'Keefe, 2012). У разі використання швидкого — індивід витрачає менше енергії, але спирається на евристики (Kahneman, 2013), в тому числі повторюваність інформації, чим і можуть користуватися шкідливі актори для проведення інформаційних операцій. Вони експлуатують цю когнітивну архітектуру, навмисно насичуючи інформаційний простір емоційно насиченим контентом, що запам'ятовується та обходить повільний шлях обробки інформації, що демонструють проаналізовані операції у розділі 4.

Загалом, розглянуті теорії та моделі намагаються концептуалізувати різні медійні впливи, описуючи те, як цей вплив може здійснюватися, розповсюджуватися мережами або мати наслідки. Проте інформаційні операції використовують широкий набір інструментів для досягнення своєї мети, й група теорій не завжди дозволяє чітко розмежувати рівні конкретної операції. Саме тому в наступному підрозділі розглянуто основні категорії інформаційних операцій, а в наступному розділі систематизовано рівні вивчення інформаційних операцій і дезінформації та запропоновано трирівневий підхід до аналізу інформаційних операцій як цілісного явища.

1.2 Базові поняття та допоміжні категорії інформаційних операцій та пропаганди

Необхідність впливати на інших, використовуючи комунікацію в історії з'явилась разом з необхідністю мати можливість для спілкування між кількома людьми чи спільнотами людей. Зі збільшенням цих груп така необхідність зростала експоненційно. Соціальна комунікація в цьому випадку виконувала допоміжну роль у державному управлінні, легітимації влади в очах громадян та задля формування спільного бачення спільноти та майбутнього. У військовому сенсі така комунікація зазвичай має назву «інформаційні операції».

Концепція інформаційних операцій (ІО) у Сполучених Штатах, згідно з Об'єднаною публікацією 3-13 (Joint Publication 3-13), визначається як «*інтегроване застосування, під час військових операцій, можливостей, пов'язаних з інформацією, узгоджених з іншими напрямками операцій, для впливу, зриву, спотворення або узурпації*

процесу прийняття рішень противників і потенційних противників, одночасно захищаючи наші власні» (US Joint Chief of Staff, 2012).” Американська модель розглядає ІО як додаткову сферу, яка слугує для досягнення кінетичних цілей, але не є самостійною сферою протиборства.

Важливо зазначити, що інформаційні операції в західній літературі зазвичай часто асоціюються з атаками на інфраструктуру комунікацій, тобто мережі та електронні системи, а операції впливу позначають активності зі впливу на опонентів, де головним фокусом є когнітивний ефект. Проте у доктринах РФ ці два рівні є невіддільними елементами стратегії, тому у цій роботі обидва терміни використовуються як взаємозамінні синоніми. Під *інформаційним впливом* у цій роботі мається на увазі ефект використання інструментів ІО.

Російська військова думка не використовує визначення інформаційних операцій напряму, а вбудовує інформаційні операції впливу у ширшу концепцію інформаційного протиборства. Згідно з російськими джерелами та теоретиками, інформаційне протиборство визначається як «*боротьба між державами в інформаційному просторі з метою завдати шкоди інформаційним системам, процесам та ресурсам, критичним структурам, [та] підриву політичних і соціальних систем*» задля «*дестабілізації суспільства та держави-противника в цілому*» (Grisé et al., 2022, с.9). Тобто, це поняття означає, що РФ має протяжну конфронтацію з опонентами, яка фактично не має кінця.

Окремим поняттям в російському словнику є інформаційна війна. В російській академічній літературі це поняття означає пролонговану інформаційну конфронтацію задля «*отримання «інформаційної переваги*» (Родионов, 1998, с.67-70). У той же час, Міністерство оборони РФ визначає інформаційну війну як західний концепт на позначення «*протиборство між двома або групою держав в інформаційному просторі з метою заподіяння шкоди державним інформаційним системам, процесам та ресурсам, критично важливим та іншим об'єктам*» (Большая российская энциклопедия, 2023; Grisé et al., 2022, с.106). Тобто, якщо протиборство має більш точну мету «дестабілізації опонента» в цілому й не мати чіткого початку, то інформаційна

війна є загостреною фазою протиборства, яка може супроводжуватись кінетичною війною й починатись разом з нею. Разом з тим, Марк Галеотті в 2013 році назвав сучасний підхід РФ до війни проти України «доктриною Герасимова», яка визначала «*гібридну війну*», тобто гібрид «*кінетичної та інформаційної війни*», хоч пізніше й відмовився від цього терміну (Galeotti, 2018). Згідно з цим підходом, невійськові засоби, зокрема інформаційні операції, домінуватимуть у майбутніх конфліктах. Цю концепцію підхопили вітчизняні та західні дослідники, хоча сама РФ у своїх документах не використовує цей термін, адже для РФ інформаційне протиборство є невід'ємною частиною мирного та військового протистояння, що суперечить необхідності додаткового визначення. Проте в цій роботі, яка спирається на західні й українські традиції дослідження інформаційних загроз (операцій), гібридна війна є іншим позначенням терміна інформаційного протиборства.

Важливим елементом цих процесів є рівень інформаційних операцій (ІО), які напряму не кодифіковані в російській літературі. Проте ми можемо дедукувати визначення ІО з доктрин РФ як дискретних активностей в інформаційному просторі *«з метою завдати шкоди для дестабілізації суспільства та держави-противника»*. Тобто операція є дискретною, має чіткий початок, цілі та її результативність може бути оцінена кількісно та якісно. У той час як протиборство та інформаційна війна мають як кінцеву точку поразку, так і перемогу над супротивником. Операції, як частина інформаційно-психологічного рівня протиборства, працюють на маніпуляцію свідомістю опонента задля досягнення конкретних дій. Що важливо, інформаційне протиборство є постійним процесом, який не припиняється у мирний час. До того ж, інформаційний вплив інтегрується в єдиний комплекс дій разом із дипломатичними, економічними та військовими заходами, що робить їх нерозривними елементами державної політики РФ. Детальніше логіку інформаційних операцій РФ визначено на основі доктринальних документів РФ у розділі 3.3.

Критичним елементом інформаційного протиборства та фактично ціллю операцій впливу є *рефлексивне управління*, що є теорією інформаційної війни радянської епохи,

яка була чітко інтегрована в сучасну російську військову доктрину (Thomas, 2004; Giles, 2016a). Теорія, розроблена радянським військовим психологом Володимиром Лефевром, стверджує, що можна маніпулювати процесом прийняття рішень супротивника, контролюючи інформаційне середовище, в якому ці рішення приймаються (Thomas, 2004). На відміну від прямого впливу на опонентів, рефлексивне управління змінює ситуацію, в якій приймається рішення, стратегічно надаючи вивірену інформацію, яка включає як правду, так і дезінформацію. Такий вплив змінює середовище прийняття рішень, що змушує об'єкти впливу добровільно обирати варіанти, які будуть вигідні ініціатору.

Отже, якщо американське бачення розглядає інформаційні операції (ІО) як підтримку операцій в рамках сфокусованої військової структури, то російська доктрина інформаційного протиборства передбачає тотальну й безперервну інформаційну боротьбу, що охоплює мир і війну, правду і брехню, публічний дискурс і кіберпростір. Зокрема, частиною постійного російського інформаційного протиборства та інформаційних операцій є такі інструменти як пропаганда та дезінформація, які використовувались для цілей ІО у 20 ст., але отримали нове дихання у 21 ст.

Пропаганда, у широкому сенсі, має значення «*розповсюдження ідей*» (Etymonline, 2025), тобто досить нейтральну конотацію, якщо не заглиблюватися у контекст, що саме розповсюджувалося або «*насаджувалося*». Оскільки розповсюдження інформації є основою комунікації, то може видатися, що пропаганда отримала свою негативну асоціацію несправедливо. Проте перед тим, як заглибитись у дефініцію, варто зупинитись на історії цього поняття.

Вперше слово «пропаганда» було використано Папою Римським Григорієм XV, який започаткував у 1622 р. організацію з промотування католицької віри «*sacra congregatio de propaganda fide*» або ж Конгрегацію пропаганди віри (Vatican, 2025). Ця організація мала на меті промотування християнської віри й місіонерство. У цьому контексті, воно мало значення розповсюдження ідей, без негативної конотації. З часом це слово отримало більш негативне забарвлення, й у 18–19 ст. почало наповнюватись

більше ідеологічними та політичними сенсами. Незважаючи на поважний вік слова «пропаганда», люди тлумачать це поняття по-різному. Зокрема, воно може мати значення від «*інформації, яка не подобається*» до «*спеціального впливу для промивки мізків*». Проте найбільші зміни принесла Перша світова війна.

Хоча перші згадки щодо дезінформування у війні згадуються у книзі «Мистецтво війни» (Сунь-цзи, 2024, с.25), перші описані приклади відносять до часів Римської імперії під час битви Октавіана та Марка Антонія (Ferguson, 2024), однак саме Перша світова війна стала переломним моментом у систематичному використанні пропаганди як інструменту ведення війни державними акторами. Вперше такі технології масової комунікації, як газети, кіно, плакати та радіо, були використані в глобальному масштабі, аби мобілізувати суспільство, сформувати громадську думку щодо ворога та необхідність продовження війни, демонізувати ворога та забезпечити міжнародну підтримку. Тобто була використана пропаганда агітації згідно з класифікацією Еллюля (Ellul, 1973, с.71). Пропаганда у цій війні стала центральною зброєю, яка охопила усе суспільство (Welch, 2014, с.12).

Тобто, приклад Першої світової війни вніс пропаганду як інтегральну частину інформаційної боротьби й ведення війни між державами, з метою впливу на тил, своїх військових та ворогів. Ба більше, країни почали створювати організації, які відповідали за пропаганду.

Перша світова війна також продемонструвала силу пропаганди для впливу на масову психологію та суспільну думку. Уряди експлуатували емоції, формуючи уявлення про війну для масштабної мобілізації своїх громадян. Поширення інформації про звірства іншої сторони, частина з яких була неправдивою, продемонструвало, що правду від вигадки в умовах війни було важко відрізнити (Ponsonby, 1940, сс.128-134). Пропаганда виявилася ефективним інструментом для підтримки морального духу країн і створення бачення війни як справедливої, зокрема, в німецькому суспільстві.

Після Першої світової війни термін пропаганда остаточно затвердився у своєму більш сучасному форматі зі стійкими негативними конотаціями та асоціаціями щодо

маніпулятивної та оманливої комунікації зі сторони держав, що може відповідати сучасному розумінню ІО. Проте, серед наукових визначень слід відзначити кілька дефініцій, які намагаються охопити спектр можливих проявів цього поняття.

Першим таким визначенням є дефініція Гарольда Лассвела, яке він надав у своїй статті 1927 року «The theory of political propaganda» (Теорія політичної пропаганди - укр.), а саме: «*Пропаганда – це управління колективними ставленнями крізь маніпуляцію важливих символів*» (Lasswell, 1927, с.627). У своєму визначенні Лассвел вказує на те, що це процес стратегічного менеджменту маніпуляцією. Символами у цьому випадку виступають інструменти соціальної комунікації, а саме: чутки, плакати, заклики, тощо. Тобто, будь-які інструменти, які промотують певну поведінку або норму, та які є важливими для впливу на цільову групу. Це схоже на теорію рефлексивного управління, адже йдеться про вплив на сприйняття.

Джовет та О'Доннел надають своє визначення пропаганди як «*навмисної систематичної спроби сформувати сприйняття, маніпулювати пізнанням та спрямовувати поведінку на досягнення відповіді, яка просуває бажану інтенцію пропагандиста*» (Jowett & O'Donnel, 2019, с.6). Ця дефініція також вказує на навмисність таких дій. Проте, по-перше, Йоветт і О'Доннел натякають на те, що цей процес не завжди успішний («*спроба*»), через те, що люди складніші істоти й можуть надавати різні відповіді на стимули. По-друге, важливим елементом є «*систематичність*», що свідчить про те, що пропаганда - це радше процес (ніж одна кампанія чи операція), який поступово призводить (чи не призводить) до зміни сприйняття. До того ж, автори зазначають вплив на пізнання, тобто не тільки на точку зору щодо певних подій, а також на процес вивчення та розкриття світу, спонукаючи до «*заломлення*» реальності під кутом зору, який вигідний пропагандистові. Таке дещо ширше визначення більше відповідає тому, як працюють сучасні ІО РФ, адже вони не стільки спонукає до переконання щодо деяких фактів, а радше працює з довгостроковим формування «*магічного*» мислення та цинізму у сприйнятті подій, символів та рішень, що призводять до поступового розчарування, відчуття розпачу, безсилля та, іноді, злоби.

Сам Еллюль визначав пропаганду як «*набір методів, який використовує організована група, що хоче викликати активну чи пасивну участь у своїх діях маси індивідів, психологічно об'єднаних через психологічну маніпуляцію та включених у організацію*» (Ellul, 1965, с.61). Схоже визначення надають Аронсон та Пратканіс: «*Масове спонукання чи вплив крізь маніпуляцію символами та психологією індивіда*» (Pratkanis and Aronson, 1992, с.13), фокусуючись на психологічній маніпуляції. Таким чином, визначення переходить у набір інструментів для впливу на психологічну складову реципієнтів шляхом маніпуляції недосконалістю психологічних процесів людей.

Більш сучасним типом пропаганди можна вважати комп'ютерну пропаганду (computational propaganda — англ.), яка є феноменом сучасної політичної комунікації. Згідно визначення Вулі та Говарда, пропаганда означає «*використання алгоритмів, автоматизації та людського включення для цілеспрямованого поширення оманливої інформації через мережі соціальних медіа»* (Woolley & Howard, 2019, с.4). Комп'ютерна пропаганда функціонує в онлайн середовищах, де ключовими рушійними силами впливу є автоматизація, персоналізація та віральність, на відміну від традиційної пропаганди, яка значною мірою залежала від централізованого розповсюдження через традиційні засоби масової інформації. Саме цей тип пропаганди є основним у сучасних ІО.

Комп'ютерна пропаганда залежить від стратегічного використання новітніх цифрових інструментів, наприклад ботів у соціальних мережах, тролів, методів мікро таргетування та алгоритмічного посилення, задля маніпуляції інформацією й, таким чином, суспільною думкою (Bradshaw and Howard, 2018, с. 26). Тобто ця комунікаційна практика використовує нові методи для досягнення схожих цілей. Цей тип пропаганди включає створення наративів, історій та матеріалів, а також активне використання різноманітного іншого контенту онлайн з опорою на технологічний розвиток комунікаційних систем. Цей розвиток призвів до небачених досі масштабів та швидкості розповсюдження, а також він дозволив краще таргетування на більш вузькі аудиторії, збільшуючи можливий вплив такої пропаганди.

Важливо коротко окреслити різницю між «ботами» та «тролями». Під ботами зазвичай розуміють акаунти у соціальних мережах, які використовують автоматизацію, тобто програмне забезпечення, яке дозволяє виконувати деякі функції, наприклад, ставити вподобайки, писати запрограмовані коментарі або поширювати певні публікації. Тролі ж, традиційно, — це реальні користувачі, які публікують образливі чи емоційні коментарі, що зривають дискусію та провокують інших користувачів. Російські інформаційні операції використовують обидва підходи, а саме ботів для збільшення метрик (реакцій, коментарів, поширень) та тролів для зриву дискусій й запуску наративів (Mazza et al., 2022).

Проте важливими й дещо незмінними залишаються цілі та мета пропаганди як інструменту інформаційних операцій. Основною метою є переконання й зміна перцепції людьми подій, політик чи людей для впливу однієї з груп на іншу з метою спонукати її до дій, вигідних першій. Вплив частіше за все відбувається на ставлення (attitudes), цінності (values) та вірування (beliefs) цільової аудиторії або лідерів групи, які, в свою чергу, впливатимуть на інших її членів. До того ж Еллюль наголошує, що пропаганда здатна формувати цілу систему переконань, яка створює схильність до певних дій. Тріада «*ставлення-цінності-вірування*» впливають на поведінку й є важливим елементом для впливу на цільову групу. У цьому контексті, зокрема, ставлення визначається як «*готовність відповісти на ідею, об'єкт або курс дій*» (Jowett & O'Donnel, 2019, с.34).

Іншою метою пропаганди є мобілізація підтримки та конкретних дій. Зокрема, Еллюль (Ellul, 1973, с.71) наголошував, що пропаганда агітації є одним з найголовніших видів пропаганди та спонукає до зміни режиму, протестів чи інших реактивних дій, як мобілізація під час воєнних дій чи під час п'ятирічки у Радянському Союзі.

Наступною метою пропаганди є легітимація влади, режиму чи певної політики. Пропаганда в цьому випадку є інструментом нормалізації та визнання політичних систем та влади, як наприклад, образ ворога допоміг Британії пояснити «*військові цілі … та підсилити бойовий дух*» (Welch, 2014, с.6). Цим часто користуються авторитарні

режими для виправдання свого існування як «*охоронця порядку й стабільності*», як це робить РФ. Бернайс (1928), в свою чергу, зазначав, що пропаганда дозволяє пов'язати політику з інтересами громадськості.

Ще однією метою пропаганди можна вважати соціальну інтеграцію, що походить з типології Еллюля, й вбачає нормалізацію певних ідей через норми й цінності суспільства та культуру. Таким чином відбувається включення людей до певного соціального порядку. Отже, включення певних ідей, як наприклад, придушення опозиції чи промоція жертовності в РФ, створює нормалізацію цього явища та певну мовчазну згоду, або ж «спіраль тиші» (Noelle-Neumann, 1993).

Іншою метою пропаганди, та основною для цієї роботи, є дестабілізація «ворожих» країн. Сучасна пропаганда часто підриває довіру до інституцій та органів влади, підсилює розбіжності між людьми, збільшуючи поляризацію та дестабілізуючи суспільство умовного ворога. Сучасна пропаганда РФ працює в цій парадигмі, намагаючись не переконати опонентів, а радше деморалізувати, дезорієнтувати та паралізувати процес прийняття рішень (Paul & Matthews, 2016). Ця функція включає публікацію у різних джерелах інформації, від соціальних мереж до традиційних медіа, великої кількості інформації, яка може й часто є суперечливою.

Отже, пропаганда у своїй сутності є методом комунікації, який об'єднує різні інструменти й підходи, використовуючи як правдиву інформацію (промоція здорового образу життя), так і неправдиву інформацію (штучне походження вірусу ВІЛ (Department of State, 1987)). Пропаганда має негативну конотацію й досить широке визначення, що робить її не зовсім коректним терміном для використання у сучасних реаліях. Навіть незважаючи на оновлення терміну, він не охоплює всі важливі аспекти інформаційних операцій, складності інформаційного ландшафту та можливостей негативних акторів. Більше того, пропаганда є лише частиною інформаційного інструментарію авторитарних режимів для впливу на опонентів, але в суспільному дискурсі найбільшої уваги набуває поширення саме неправдивої інформації.

У 2010-х роках у побут увійшов термін «*фейкові новини*», який став словом року (Collins, 2017) та стрімко увійшов у публічний та політичний дискурс, особливо після виборів Президента США у 2016 році, ставши популярним неологізмом для опису дезінформації в мережі (Egelhofer & Lecheler, 2019). Однак незважаючи на широке розповсюдження, вжиток цього терміну в академічних та професійних дослідженнях є некоректним й оминається дослідниками (Lazer et al., 2018). Нечіткість цього визначення, його високе політичне навантаження призвели до здатності розмивати сутнісні відмінності між різними формами неправдивої інформації (Wardle & Derakshan, 2017). Оскільки цей термін може означати одразу й сфабрикований контент (як діпфейки), представлений як реальний, сатиру, клікбейт й пропаганду, його використання не є бажаним, а натомість варто використовувати типологію інформаційного безладу, описану у підрозділі 1.1. Найважливішим терміном є саме дезінформація, що є певною реінкарнацією радянських часів і словника. Наприклад, у радянські часи дезінформаційні кампанії таргетували як окремих осіб, наприклад, посадовців ФРН (Rid, 2020) або Папу Римського (Pacepa & Rychlak, 2013), так і цілі країни чи їхні органи. Одним із таких прикладів є «Операція Денвер» (Rid, 2020), яка розглянута у підрозділі 3.1.

Окрім базових понять дезінформації, місінформації та малінформації, сучасні дослідження пропаганди спираються на низку допоміжних категорій, що описують механізми та стратегії впливу. Поняття, як-от «наратив» та «фрейм», що визначені у підрозділі 1.1, та «мем» не замінюють основні категорії, а радше операціоналізують їх та пояснюють, як саме шкідлива інформація конструюється, поширюється та інтерналізується в медіасередовищі. У цій роботі наративи будуть використовуватись для демонстрації інтерпретативних рамок, які нав’язує російська дезінформація та пропаганда закордонним аудиторіям для того, щоб уникнути відповідальності та нав’язати свою точку зору щодо бачення подій в реальному світі, як тих до яких РФ причетна напряму та тих, що відбуваються всередині демократичних країн.

У цифрову епоху для ефективної трансляції фреймів часто використовують меми. Хоча вони традиційно асоціюються з інтернет-гумором, у комунікаційному контексті мем — це культурний «пакет» інформації, що поширюється від людини до людини через імітацію (Shifman, 2013a; Shifman, 2013b). Це може бути картинка, звук, анімація, відео тощо. Меми є «живими» організмами-компонентами операцій впливу й, у випадку соціального резонансу, можуть існувати поза безпосереднього кола розповсюдження операторів впливу. Оскільки меми надзвичайно стислі та емоційні (сарказм, іронія), вони діють в обхід критичного мислення, що робить їх ідеальними інструментами для надшвидкого («вірусного») розповсюдження широкими верствами, ствердження всередині ізольованої групи як символу приналежності до цієї групи, а також для підривної діяльності. Отже, вони можуть не напряму атакувати інституції, представників влади, політичних рухів тощо, у гумористичній манері, трансформуючи висміювання та критику у «гумор».

Ще однією важливою допоміжною категорією є теорії змови. В класичному розумінні такі теорії є «поясненням історичних подій, яке визначає головним чинником їхнього виникнення … змовників, котрі діють таємно у власних інтересах і на шкоду суспільному благу» (Uscinski, 2017, с.3). Теорії змови мають чітку структуру й потенціал віральності, особливо на тлі падіння довіри до традиційних медіа та державних інституцій. Такі теорії мають замкнуту й цілісну внутрішню структуру, яка дозволяє цьому інструменту розвиватися всередині маргінальних груп та широкого загалу (Яковлєв, 2023). До того ж вони зазвичай приписують зловмисний намір актору (зазвичай уряду) й використовують спростування як додаткові докази правоти. Російські актори використовують теорії змови як свідомий інструмент для розмиття розуміння істини про події, уникнення відповідальності, легітімимізації дій РФ та делегітимізації країн Заходу (Yablokov, 2015).

Зрештою, синергія різних елементів (пропаганди, фреймів, мемів та теорій змов) створює ізольовану замкнуту екосистему, де цільова аудиторія стає мимовільним

учасником маніпуляції та інтерпретації світу, який тиражує та посилює наративи та фрейми, що покликані дестабілізувати когнітивну автономію системи.

У сукупності ці концепти можна охарактеризувати як такі, де операції впливу діють на стратегічному рівні, тобто найбільш абстрактному, й використовують пропаганду, дезінформацію та наративи у своїй роботі задля дестабілізації опонента. Наративи та теорії змов ІО забезпечують структурування змісту на макрорівні для різних аудиторій, в той час як фрейми спрямовують інтерпретацію на мікрорівні. Меми ж виступають носіями наративів та фреймів, що уможливлюють швидке поширення через мережі неавтентичної поведінки та традиційних джерел білої пропаганди. Ця ієрархія підкреслює, що пропаганда та дезінформація — це структурована ієрархічна система виробництва сенсів та контролю над групами та громадянами. Розуміння й об'єднання цих споріднених концепцій дозволяють створити більш точну аналітичну базу, яка здатна охопити всю складність сучасних маніпуляцій у медіапросторі.

РОЗДІЛ 2
МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ РОСІЇ У МЕДІЙНІЙ СФЕРІ

2.1 Актуальні методи досліджень інформаційних впливів Росії в світі

Дослідження російського інформаційного впливу має методологічну складність через гібридну природу впливу, стратегічну неоднозначність та постійну мінливість інформаційного простору, також постійну адаптацію акторів до технологічних і геополітичних умов. Російський інформаційний вплив охоплює різні медіасистеми, мови, платформи та регіони, поєднуючи такі інструменти, як: відкриті заяви політичних осіб та дипломатів, висвітлення подій у підконтрольних медіа з прихованими маніпуляціями, розповсюдження державних наративів через проксі-акторів (посередників) за кордоном тощо.

Традиційні дослідження інформаційних операцій часто надають перевагу одному аналітичному аспекту перед іншими. Наприклад, фахівці з комп'ютерних наук фокусуються на технічних механізмах доставки повідомлень (Badawy et al., 2018), дослідники комунікацій вивчають наративні стратегії (Gouliev, 2025), а психологи досліджують когнітивні упередження, що сприяють поширенню (Rand and Pennycook, 2021). Такий фокус накладає свої обмеження, адже приховує зв'язки між технічними можливостями, наративними стратегіями та психологічними наслідками інформаційних повідомлень, що характерні для сучасних кампаній впливу (Осадчук, 2026). Саме тому варто об'єднувати кілька рівні задля комплексного охоплення проблеми, що й було зроблено в цій роботі, зокрема шляхом аналізу інформаційних операцій на трьох рівнях.

Перший, технічний рівень має охоплювати цифрову інфраструктуру, платформи та механізми, за допомогою яких операції впливу доносяться до цільових аудиторій. Цей аспект ґрунтується на тому, що контент, незалежно від його переконливості, потребує технологічних засобів виробництва, посилення та розповсюдження (Woolley & Howard,

2018). Аналіз цього рівня розкриває можливості, ресурси та тактичну адаптацію суб'єктів впливу. Для дослідження цього аспекту можливо використовувати частини аналізу мереж, вразливостей соціальних платформ, які використовуються для доставки контенту, а також різних підходів цифрової гуманітаристики, включно з методами розвідки відкритих джерел.

У дослідженнях російських операцій впливу детально задокументовано використання автоматизованих акаунтів (ботів) та координованої неавтентичної поведінки для штучного посилення повідомлень і створення враження масової підтримки, якої насправді немає (Broniatowski et al., 2018). Методологічно дослідники застосовують мережевий аналіз, вивчення метаданих акаунтів та розпізнавання інформаційних аномалій, а також певних поведінкових патернів для ідентифікації бот-мереж, що вказують на використання програмного забезпечення чи автоматизації для відправлення повідомлень. Наприклад, Варол та інші (Varol et al., 2017) розробили алгоритм машинного навчання, який здатний виявляти автоматизовані акаунти, шляхом аналізу часових графіків публікацій, лінгвістичних особливостей та структур мережевих зв'язків.

Інформаційні операції впливу часто застосовують техніки та тактики, щоб сховатися від дослідників, заплутати потенційні цілі інформаційних операцій або ж приховати реальне джерело інформації. Так, наприклад, зловмисні актори можуть підроблювати сайти, які на зовнішній вигляд будуть ідентичними реальним медіа, але насправді міститимуть інформацію, яку реальний сайт ніколи не публікував (Châtelet and Osadchuk, 2024). Або ж, сайти можуть використовувати «геофенсинг» (англ. — geofencing) (відсортовування по локаціях), використовуючи програмне забезпечення для того, щоб зловмисний контент, як, наприклад, операція «Двійник», потрапляв саме до цілей інформаційного впливу у певних країнах (Qurium Media Foundation, 2022). Деякі підходи аналізу відкритих джерел, як мережевий пошук, аналіз реєстраційних записів (Whois), а також аналіз вихідного коду вебсайтів є корисними для розслідування таких кампаній. До того ж, дослідження на технічному рівні використовують обчислювальні

методи, зокрема аналіз мереж, аналіз великих даних для класифікації за допомогою машинного навчання. Основними джерелами слугують дані платформ (наприклад, розділ «Прозорість сторінки» у Facebook), веб-архіви, DNS-записи та метадані.

Наступним рівнем є рівень контенту, тобто вмісту того, що публікують пропагандисти та шкідливі актори. Якщо технічний рівень відповідає за доставку, тобто відповідає на питання «як?», то цей рівень фокусується на питанні «що?». У цьому підході важливий аналіз суті повідомлень та фреймінгу цієї інформації, що поширюється через операції впливу. Цей вимір визнає, що кампанії впливу використовують певні наративні стратегії, розроблені для досягнення цілком специфічних політичних, соціальних або військових цілей, як наприклад, описано у внутрішніх документах російських організацій «Агенція соціального проєктування (АСП) та «Група компаній структура» (Структура), які опублікували в афідевіті Міністерства юстиції США (Department of Justice, 2024a), де чітко визначені цілі інформаційного впливу РФ на Україну. Аналіз контенту може допомогти з тим, щоб привідкрити завісу задуму пропагандиста, ідентифікувати потенційну цільову аудиторію та, за можливості, виявити координацію між різними платформами й каналами, якщо вони використовують схожі текстові прийоми, зокрема наративи, однакові тексти тощо.

Доцільним для такого методу є аналіз повторюваних наративів та аналіз того, як вони змінюються в часі, якщо ця зміна є. Російські операції впливу часто розгортають наративи, які просувають вигідні РФ цілі, як-от уникнення відповідальності за злочини. Ці наративи часто акцентують увагу на занепаді Заходу, історії про агресивні та русофобські країни навколо тощо. Досить часто російські медіа та державні представники конструюють «альтернативну реальність», яка не обов’язково змушує аудиторію вірити в конкретні твердження, а радше спонукає однаково сумніватися в усіх джерелах інформації. Прикладами цього можуть бути велика кількість наративів про збиття літака MH17 (EUvsDisinfo, 2024) та отруєння Скрипалів (Warrick and Troianovski, 2018). Деякі з цих наративів повторюються роками й використовуються як фундамент для майбутніх кінетичних та інформаційних операцій. Так, наприклад, у звіті

«Наративна війна» (Narrative Warfare) (DFRLab, 2023a) проаналізовано російські наративи за 8 років, які розвінчувала неурядова організація StopFake. У звіті можна побачити, що російські наративи з різною інтенсивністю повторювалися й запускалися в інформаційний простір РФ та України з метою делегітимізувати уряд України. До того ж, деякі з тих наративів, а саме про «біолабораторії» чи «агресивну» Україну, росіяни намагалися використати як *casus belli* (Gigitashvili & Osadchuk, 2022) для повномасштабного вторгнення у 2022 році.

Під час аналізу наративів варто звертати увагу не тільки на офіційні («білі») джерела російської пропаганди, такі як RT або РІА, а й на видання, які розповсюджують «сіру» та «чорну» пропаганду (Ellul, 1973). На відміну від «білої» інформації, що є відкритим впливом з очевидним та неприхованим джерелом, «чорна» пропаганда є повністю сфабрикованою інформацією з прихованим або підробленим джерелом. Поєднання ж двох видів формує «сіру» пропаганду, яка поєднує факти з вигадками або ж вирвані з контексту дані з можливим приховуванням оригінального джерела (хоча не у всіх випадках). Підхід, коли частина правдивої інформації огортається у шар неправди, є особливо ефективним, оскільки він робить повідомлення більш правдоподібним та таким, що заплутує читачів. Прикладом такої дезінформації й пропаганди можуть слугувати теорії змови так званого «зеленого екрану», коли колишні журналісти Кремлівських видань почали розповсюджувати повідомлення, що Президент Зеленський у 2022 році записував свої звернення до українців не в Києві, а закордоном на зеленому екрані за допомогою комп'ютерної графіки. Вся історія базувалась на реальному фото Зеленського на тлі зеленого екрану, який використовували для запису промови на технологічну подію (Osadchuk, 2022). Для дослідження таких повідомлень особливо ефективними є методи перевірки фактів (фактчекінг), верифікації джерел та аналіз джерел, які цю інформацію поширюють, включно з аналізом того, чи вибірково подається інформація в них.

Також на рівні контенту важливим є мапування різноманіття повідомлень, які є частиною тактики Російської Федерації під назвою «*потік брехні*», що отримала назву

через однойменний звіт Rand Corporation (Paul and Matthews, 2016). У цій роботі дослідники визначили характерну модель інформаційного впливу РФ, що виражений надмірним обсягом та багатоканальним поширенням повідомлень з ігноруванням послідовності чи відповідності фактам. Ця модель базується на принципі, що часте повторення інформації підвищує впізнаваність і сприйняту достовірність, незалежно від правдивості (Pennycook and Rand, 2021), тоді як величезний обсяг суперечливих повідомлень може пригнічувати здатність аудиторії до критичної оцінки (Ramsay and Robertshaw, 2019).

Іншим підходом до дослідження інформаційних впливів є когнітивний. Цей рівень досліджує психологічні механізми, евристики та упередження, за допомогою яких операції впливу впливають на індивідуальне та колективне розуміння, відношення та поведінку. Цей вимір визнає, що контент та способи його доставки для цільових аудиторій, зрештою, спрямований на досягнення вимірюваних змін у поведінці чи сприйнятті конкретних груп людей. Так, результатом цього впливу може бути вплив на те, як цільові групи сприймають реальність (Lasswell, 1927), опрацьовують інформацію та приймають рішення (Benkler et al., 2018, с.33). Когнітивний рівень пов'язує операції впливу з усталеними психологічними дослідженнями переконання та ефектів дезінформації.

Дослідники використовують експериментальні моделі для вимірювання того, як вплив контенту маніпуляцій позначається на ставленні, цінностях та віруваннях і реальних діях, як наприклад, поширенні неправдивих повідомлень (Guess et al., 2019). Опитування, експерименти та спостереження використовуються для вивчення політичної поляризації, довіри до інституцій, віри у власну спроможність впливати на процеси (efficacy beliefs) та електоральну поведінку. Наприклад, Allcott and Gentzkow (2017) продемонстрували, що міс та дезінформаційні новини становили хоч і невелику, але потенційно вирішальну частку в загальному споживанні новин під час виборів 2016 року. У той же час Grinberg et al. (2019) виявили, що вплив дезінформації був зосереджений серед вузького сегмента вкрай заангажованих користувачів, що навряд

змінило хід виборів. Проте важливою знахідкою стало те, що дезінформація може бути спрямована на специфічні верстви населення задля їхньої додаткової поляризації чи зміни уявлень про світ, та у свою чергу - поведінки.

В рамках когнітивного рівня також вивчають стратегічні концепції РФ, наприклад, «рефлексивне управління». У цьому підході важливим є вивчення когнітивних вразливостей, які використовують державні актори. Їхні операції впливу систематично експлуатують добре вивчені когнітивні упередження та евристики, а саме підтверджувальне упередження, вмотивоване мислення, евристику доступності та емоційне мислення (Kahneman, 2013). Російські операції таргетують контент на аудиторії, формуючи повідомлення таким чином, щоб вони підходили аудиторії. Часто повідомлення обходять критичну оцінку споживачів інформації через використання емоцій або ж ідеологічно вмотивоване мислення, тобто співпадіння з наявними політичними вподобаннями. Так, Kahan (2013) демонструє як ідеологічно вмотивоване мислення може використовувати логіку для виправдання політичної позиції, ігноруючи емоційний вплив. Таким чином, дезінформатори можуть надати певну інформацію з боку підтримки певної ідеології, щоб отримати підтримку групи, яка поділяє цю ідеологію. До того ж, дослідження таких понять й алгоритмічних пасток розповсюдження інформації, як «ехо-камери» та «фільтри-бульбашки» демонструють, як структура сучасних соціальних платформ створює середовище, де контент може бути підсилений для певної ізольованої групи (Pariser, 2012).

Комбінований підхід цих трьох рівнів підсилюється дослідженням їхніх взаємозв'язків (Осадчук, 2026). Технічна інфраструктура уможливлює стратегії контенту, а саме підсилення за допомогою мереж ботів, що робить «потік брехні» (firehose of falsehood) досяжним у великих масштабах (Woolley & Howard, 2018). Рефлексивне управління визначає контент та способи доставки, адже створення інформаційного простору й шуму, що призведе до перевантаження, потребує як технічної інфраструктури для розповсюдження великих обсягів інформації, так і

планування щодо повідомлень, які мають бути доставлені, зважаючи на психологію їхнього сприйняття.

Запропонована трирівнева аналітична рамка (технічний, наративний, когнітивний рівні) розробляється в контексті низки існуючих аналітичних підходів та інструментів дослідження інформаційних операцій. Найпоширенішим методом у міжнародній дослідницькій практиці є рамка «актор-поведінка-контент» (англ. Actors–Behavior–Content, ABC), концептуалізована Каміллою Франсуа (François, 2019), її подальші розширення з додаванням вимірів дистрибуції та ефекту, тобто ABCDE (Pamment, 2020), а також рамка DISARM, яка мапує тактики, техніки та процедури (англ. - Tactics, Techniques and Procedures) (Terp and Breuer, 2022). Аналіз співвідношення між цими підходами та запропонованою рамкою є необхідним для демонстрації позиціонування аналітичного внеску цієї роботи та для підкреслення концептуального зв'язку запропонованої рамки з наявною аналітичною традицією, а також її диференціації.

Камілла Франсуа запропонувала рамку ABC у межах роботи Трансатлантичної робочої групи для слухань в комітеті Палати представників (House Committee Hearing, 2019). Ця рамка розрізняє три виміри інформаційної операції, а саме: 1) маніпулятивних акторів (A), які стоять за операцією; 2) поведінку (B), що охоплює техніки поширення повідомлень; 3) вміст (C), тобто власне тексти, аудіовізуальні матеріали та інші форми повідомлень. Аналітична простота цієї схеми зумовила її широке прийняття провідними дослідницькими аналітичними центрами, безпековими інституціями та підрозділами соціальних платформ, які займаються розвідкою загроз та безпекою.

Пандемія COVID-19 та пов'язана з нею «інфодемія» у 2020-2021 роках призвели до аналітичного розширення рамки. Найпоширенішим оновленням є фреймворк ABCDE, у якому до перших трьох вимірів додано також виміри поширення (D, distribution) та ефекту (E, effect). Вимір D описує канали та механізми поширення повідомлень, а вимір E, в свою чергу, орієнтований на оцінку реального впливу операції на цільові аудиторії. Це розширення створює умови для більш повного аналізу циклу інформаційних операцій.

Рамка DISARM, яка побіжно проаналізована у підрозділі 3.4, фокусується на документації та диференціації тактик, технік і процедур (tactics, techniques, and procedures, або TTP - англ.) дезінформаційних операцій. Вона була адаптована на основі модельної рамки зі сфери кібербезпеки — MITRE ATT&CK (Terp and Breuer, 2022). Враховуючи цей вимір, DISARM створювався як спосіб документування інцидентів та обміну даними між дослідницькими, факт-чекінговими організаціями та платформами соціальних мереж. Отже, це радше інструмент стандартизованого кодування конкретних операцій, аніж рамка для теоретичного осмислення дезінформаційних операцій.

Запропонована у цьому дисертаційному дослідженні трирівнева рамка частково перетинається з цими підходами та доповнює їх, проте не конкурує чи витісняє їх. Серед елементів перетину є змістова відповідність технічного рівня запропонованої рамки сумі вимірів B та D у рамці ABCDE. По-друге, наративний рівень частково відповідає виміру C. Такий перетин є не випадковим, адже він свідчить, що запропонована рамка не суперечить попередній аналітичній традиції, а імпортує її напрацювання та дозволяє перенесення емпіричних висновків між парадигмами без фундаментальних концептуальних втрат.

Водночас запропонована рамка має ряд відмінних рис, які виправдовують її окреме формулювання як аналітичного інструмента дослідження сучасних російських інформаційних операцій.

Перша відмінна риса — це автономний когнітивний рівень. Запропонована рамка інтегрує когнітивний рівень як автономний предмет аналізу, на якому поєднуються три теоретичні традиції: система когнітивних упереджень та евристик (Kahneman, 2013); теорія рефлексивного управління, що походить з радянсько-російської військової традиції та була ретельно реконструйована західними аналітиками (Thomas, 2004; Giles, 2016a); та психологічна література щодо механізмів сприйняття та поширення правдивої інформації та дезінформації (Lewandowsky et al., 2012; Pennycook and Rand, 2021; Ecker et al., 2022). У базовій рамці ABC цей вимір відсутній взагалі, адже акцент зроблено на акторах та інструментах, а не на психологічних механізмах сприйняття інформації. У

розширенні ABCDE цей вимір присутній як E (effect), проте сформульований переважно через категорії вимірюваного ефекту конкретної операції. Тоді як у запропонованій рамці когнітивний вимір охоплює також задумувальний рівень, тобто реконструкцію інтенцій оператора пропаганди й що саме намагались передати актори своїми операціями. Частково це можна проаналізувати у внутрішніх документах акторів (Department of Justice, 2024a; Pamment and Tsurtsumia, 2025) або ж через аналітичну реконструкцію. Розуміння когнітивного рівня як поєднання задуму та ефекту дозволяє реконструювати інтенції російських акторів. Ця модель базується на традиціях радянських «активних заходів» та підтверджується доступними внутрішніми документами виконавців.

Друга відмінна риса — це інтерактивність компонентів. Запропонована рамка не є модульною, а робить акцент на взаємодії компонентів. Рамки ABC, ABCDE та DISARM у своїй базовій реалізації розділяють аналітичний процес на паралельні категорії. Згідно з цими рамками, дослідники окремо описують акторів, окремо поведінку, окремо контент, після чого результати збираються у підсумковий звіт. Запропонована трирівнева рамка натомість акцентує увагу на тому, що взаємозв'язки між рівнями є важливими (Осадчук, 2026). Тобто, технічна інфраструктура фактично уможливлює наративні стратегії, як наприклад, реалізацію моделі «потоку брехні» (Paul and Matthews, 2016), яка є малоефективною без автоматизованої інфраструктури підсилення та поширення. Наративний матеріал підбирається з урахуванням когнітивних вразливостей цільової аудиторії, тобто відбір тем, наративів, тропів, мемних шаблонів й фреймів пов'язаний з цільовою аудиторією. Зворотні зв'язки між рівнями є також важливими. Наприклад, посилення певних наративів алгоритмами платформ через підвищені емоційні реакції може надати сигнал дезінформаторам щодо резонансності теми й призвести до збільшення контенту в її рамках, що, у свою чергу, може змінити ефект всієї операції. Таким чином, аналітичний фокус переноситься з характеристики окремих компонентів на інтегрований процес та спробу реконструкції логіки операції.

Третя відмінна риса — адаптація до специфічного актора операцій. Запропонована рамка свідомо інтегрує концепти, що виникли саме в межах радянсько-російської військової й інформаційної традиції, а саме рефлексивне управління (Thomas, 2004), підхід «потоку брехні» у його російській емпіричній реалізації (Paul and Matthews, 2016), а також логіку «активних заходів» з її акцентом на тривалі стратегічні наративи (Rid, 2020). Універсальні рамки на кшталт ABCDE є аналітично «нейтральними» та можуть бути застосовані до будь-яких операцій будь-яких країн. Проте вони фактично позбавлені специфіки, що потрібна для аналізу російських операцій, враховуючи спадковість стратегічної традиції, яка реконструйована в другому розділі цієї роботи.

Запропонована рамка не претендує на статус принципово нового аналітичного інструмента, що повністю замінює існуючі. Радше вона дозволяє виконати інтеграційне переформулювання з чіткою специфікацією трьох рис, а саме: (а) автономного когнітивного рівня з реконструкцією як інтенцій акторів, так і ефектів на аудиторії; (б) фокусу на зв’язках та взаємодії між рівнями замість їх паралельного членування; (в) адаптації до російської військово-інформаційної традиції з відповідним включенням концептів рефлексивного управління та «потоку брехні».

Запропонована рамка є комплементарною щодо рамки DISARM, адже її трирівнева структура може слугувати концептуальним каркасом, в який можуть бути включені конкретні TTP, які кодифіковані за таксономією DISARM. Це є важливою операційною характеристикою запропонованого підходу, адже він не потребує та не пропонує заміщення наявних підходів та документації TTP, а забезпечує для них рамку інтерпретації вищого рівня. Ця рамка сполучає рівень інструментів з рівнями стратегічного задуму, а також когнітивними наслідками цих операцій. Запропонована у цій роботі рамка виступає аналітичним містком між існуючими традиціями дослідження інформаційних операцій з акцентом на російську специфіку як основного емпіричного поля цієї дисертації.

2.2 Ключові категорії медіа та напрямки дослідження російських медіа

Для концептуалізації дослідження потрібно визначити медіа, а саме видання та платформи. Ці канали комунікації дозволяють РФ активно вести інформаційні операції та поширювати дезінформацію та пропаганду. Після розпаду СРСР концепція державного міжнародного мовлення зазнала радикальної трансформації. Загалом міжнародне мовлення задумувалося як інструмент публічної дипломатії країн та засіб роз'яснення культури та політики конкретної держави іноземній громадськості (Nye, 2004). Проте в контексті Російської Федерації воно було перепрофільоване на критичний елемент інформаційної війни. Ці медіа впроваджують дезінформацію через пряму фальсифікацію та за допомогою стратегічного підходу до встановлення порядку денного у мовних середовищах, де вони представлені. Вони досягають цього за допомогою локалізації російських наративів та інтеграції у так звані «антисистемні» чи опозиційні групи. RT (Russia Today) та Sputnik впливають на іноземні аудиторії та пропагують точку зору РФ. Йдеться не про традиційне завоювання «сердець і розумів», а радше про підрив та дестабілізацію інформаційного простору супротивника (Griffin, 1984).

Головним елементом RT є її адаптивність до інформаційного простору та анти-системних груп у країнах-цілях. Ці «медіа» використовують студійні декорації високої якості, ведучих-носіїв мови, а також професійний монтаж. Цією «професійністю» вони створюють звичний для глядача образ медіа, проте такого, що кидає виклик центральним ЗМІ країни-цілі. Часто RT перебирає на себе претензії «маргінальних» груп у країнах Заходу (наприклад, скептиків щодо НАТО). Це створює ситуативний альянс між інтересами російської держави та внутрішнім інакомисленням у цих країнах, а також альтернативним порядком деним, який підважує встановлений демократичний суспільний порядок. Більше того, позиціонуючи себе як медіа, що закликає «дізнатися більше» (Question More - слоган RT), RT експлуатує демократичну цінність скептицизму, перетворюючи її на зброю проти довіри до інституцій.

Цей скептицизм може бути організований наративно в інтерпретаційні структури з причинно-наслідковими зв'язками як-от «стратегічні наративи». RT та Sputnik мають

велику кількість мовних редакцій, і порівняльне вивчення цих видань може надати розуміння стратегічного впливу РФ на іноземні країни. Відтак російське іноземне мовлення (іномовлення) реалізує кілька взаємопов'язаних рівнів такого стратегічного наративу. На системному рівні «головний наратив» ставить під сумнів легітимність ліберального світового порядку після розпаду Радянського Союзу. Згідно з цією перспективою, наявний світовий порядок позиціонується як американський проєкт, а не логічний розвиток історії людства. На нижчому рівні Росія подається як протиставлення західному світу, тобто незалежний суб'єкт (іноді цивілізаційний проєкт), що захищає багатополярність від експансії країн Заходу. Цей фрейм є досить популярним в аудиторіях так званого Глобального Півдня з історичних причин, які не можуть бути відкинуті як чиста маніпуляція. Окремі події, злочини чи дії, як, наприклад, збиття рейсу MH17, отруєння Скрипалів, повномасштабне вторгнення в Україну, описуються у цих медіа через сталі структури й фрейми «західної провокації», підозр у операціях «під чужим прапором» та заперечення вини РФ. Тривале споживання таких медіа формує викривлене розуміння реальності (Gerbner et al., 1978).

Окрім цього, російське міжнародне мовлення інвестує в розбудову інституційної ідентичності, яка імітує професійну й незалежну журналістику для того, щоб посісти позицію авторитету серед споживачів, які не сприймають та не споживають мейнстрімні медіа. Модель впливу RT та Sputnik відкидає ідею промоції російських інтересів і позиціонує ці медіа як альтернативу нібито гомогенності західних медіа. RT часто використовує високий рівень виробництва контенту задля створення іміджу респектабельного видання. Вони розповсюджують теорії змов (Yablokov, 2015) надають майданчик альтернативним місцевим голосам та також співпрацюють з журналістами (Menn, 2024), які знаходяться на полярних сторонах політичного дискурсу.

Важливими в цьому аспекті є структурні умови медійної системи країни розповсюдження, де цей контент може посилитися, трансформуватися або нейтралізуватися. Фокус дослідження виключно на контенті RT як ізольованому векторі впливу недооцінює те, яким чином ефекти цього контенту підсилюються внутрішніми

акторами у соціальних мережах та вразливістю, спричиненою світовим падінням довіри до традиційних інституцій. Також іноземні державні медіа РФ рідко є першоджерелом дезінформації у внутрішніх інформаційних середовищах інших країн. Їхня значно важливіша функція полягає у ролі ресурсу легітимізації, тобто авторитетного джерела для підтвердження маргінальних повідомлень та теорій змов, які виникають у внутрішніх дезінформаційних мережах і потребують ширшого розповсюдження. Ці мережі можуть підсилювати стратегічний наратив РФ за допомогою так званого «зв'язкового стратегічного наративу» (Zakharchenko, 2025), в якому стратегічний наратив формується не тільки державними медіа країни-цілі, а й альтернативними повідомлення (RT) та комунікаціями у соціальних мережах. У цій моделі RT та Sputnik можуть функціонувати як передавачі пропаганди, так і як джерела для «відмивання» наративу та «спіну» реальних подій чи думок всередині країни (Квіт, 2008, с.123-125). До того ж, іноді безпосередньо російські актори можуть створювати ці повідомлення (Osadchuk, 2023b).

Важливо відзначити, що після того, як проти російських державних медіа були введені санкції (European Council, 2022), а також ускладнилася робота в інших країнах (Johnson, 2022), вони потребували нові способи впливу на іноземні аудиторії. Частина методів стосувалася фінансування поляризованих журналістів (Justice Department, 2024b) та розповсюджувачів контенту для створення ідеологічних матеріалів, які б розколювали суспільства. Інша ж частина полягає у використанні пов'язаних з виданням журналістів та розповсюдженні інформації через соціальні медіа. Тому в цій роботі буде розглянуто не лише основні медіа джерела РФ за кордоном, а й проаналізовано розповсюдження повідомлень через соціальні мережі.

Російські дезінформаційні кампанії демонструють характерну кросплатформову архітектуру, тобто міграцію повідомлень між вебсайтами та багатьма соціальними платформами, яку дослідники називають моделлю «потоку брехні» (Paul and Matthews, 2016). Ця модель характеризується великим обсягом наративів, їх багатоканальним розповсюдженням й навмисною суперечливістю. Benkler, Faris та Roberts (2018)

дослідили сталу схему поширення наративів під час виборів США у 2016 році, яка складалась з кількох етапів. По-перше, це введення наративу у дискурс, тобто поява наративів у пов'язаних із державою російських ресурсах (RT та Sputnik), які звідти переходять на маргінальні внутрішні платформи США (зокрема, автори вказують на Breitbart та InfoWars). По-друге, цей контент починає активно бути підсиленим через скоординовану поведінку у соціальних мережах, який звідти потрапляє у мейнстримний дискурс через висвітлення провідними медіа самого факту дискусії або скандалу, спровокованого цими публікаціями.

Операційна логіка кросплатформного розповсюдження підпорядковується підходу «посіву та посилення» (seeding and amplification). Тобто, публікації контенту на платформі або вебсайті з низьким рівнем модерації (Telegram-канали або спеціально створені сайти), з поступовим систематичним просуванням цього контенту на більш помітних платформах через координоване поширення, підсилення метрик (переглядів, реакцій, коментарів) та перехоплення хештегів. Наприклад, з початком повномасштабного вторгнення в Україну в лютому 2022 року Telegram перетворився на центральний вузол російської дезінформаційної інфраструктури. Він одночасно функціонує як середовище для створення контенту, канал розповсюдження та система архівації, яка є досить стійкою до модерації.

Додатково, російські джерела як RT використовують підхід «відмивання новин», коли новини, написані в RT, перекладаються іншими мовами та розповсюджуються як оригінальні великою кількістю блогів та «альтернативних» майданчиків, щоб уникнути модерування та заборон. Так, Koronska et al. (2024) прослідкували, як новини з RT та Sputnik були перекладені та розповсюджені у Польщі. Цей спосіб дозволяє уникати прямого цитування та сприяє дифузії проросійських наративів попри заборони та блокування. Схожі методи розповсюдження новин використовуються в багатьох інших країнах, хоча такі публікації є лише частиною розповсюдження російських новин за кордоном.

Діяльність пов’язаних із Росією бот-мереж була детально задокументована завдяки звітам самих платформ, аналізу академічних наборів даних та журналістських розслідувань. Наприклад, архів Twitter Elections Integrity, оприлюднений у 2018 році, містив базу даних про 3,841 акаунт, які пов’язані з Пригожинським «Агентством інтернет-досліджень» (internet research agency, IRA — англ.), які сукупно згенерували понад дев’ять мільйонів твітів (Linvill and Warren, 2020). Аналіз Linvill та Warren виявив, що деякі акаунти не функціонували переважно як очевидні ретранслятори пропаганди, а імітували складнішу поведінку, агрегуючи новини або ж дискутуючи про ігри. Значна частина їхнього контенту складалася з неполітичних матеріалів, поширених для побудови ззовні автентичних відносин із підписниками, що є важливим інструментом, перш ніж починати розповсюдження політично заангажованого контенту.

CIB є частиною альтернативної або периферійної інформаційної екосистеми. Така поведінка охоплює широку сукупність акторів та платформ: альтернативні новинні ресурси, що діють поза межами мейнстримних журналістських норм; ідеологічно орієнтовані блоги та подкасти; платформи та спільноти конспірологів; маргінальні соціальні мережі, включно з форумами на кшталт 4chan, reddit та їхніх наступників; анонімні Telegram-канали; а також закриті онлайн-спільноти, організовані довкола спільних ідентичностей, від релігійних та націоналістичних до антиглобалістських. Ці середовища зазвичай мають кілька спільних структурних рис, що роблять їх особливо цінними для операцій іноземного інформаційного впливу. По-перше, такі операції мають низькі витрати на обхід модерації контенту, адже на таких платформах зазвичай відсутні суворі обмеження для вільного поширення будь-яких наративів. По-друге, висока довіра аудиторії до неінституційних джерел у «немейнстрімних» середовищах. Тобто, на таких платформах користувачі апріорі схильні вірити «альтернативним» та «конспірологічним» (Яковлєв, 2023) повідомленням більше, ніж офіційним медіа.

Відносини між пов’язаними з російською державою медіа та периферійними екосистемами в інших країнах не є просто однобічною експлуатацією - йдеться про ідеологічне узгодження та взаємне посилення. Такі відносини розмивають просту межу

між «державним» та «недержавним» впливом й вимагають більш прискіпливого аналізу та методологій.

Тому однією з найбільш значущих динамік у сучасних дослідженнях дезінформації є процес, за якого наративи, що виникають у периферійних або маргінальних інформаційних середовищах, мігрують в основний дискурс. Цей процес, який відбувається через послідовність певних етапів, можна назвати «відмиванням наративу» або ж «наративною ін'єкцією». Прикладами такого процесу є підроблені матеріалами про «яхту Зеленського» чи «карт'є Олени Зеленської» (The Economist, 2024; Linvill and Warren, 2023). Цей процес зазвичай складається з кількох етапів: посів, нашарування та інтеграція (Meleshevich and Schafer, 2018). Посів (placement) - це процес розміщення неправдивого контенту в соціальних мережах або на вебсайті, зазвичай маловідомому. Для таких публікацій часто використовуються новостворені порожні облікові записи у соціальних мережах, які були створені для того, щоб запустити кейс дезінформації таким чином, щоб залишитись анонімними. Іноді, на таких акаунтах з'являється нова інформація від «інсайдера», як наприклад, під час кейсу про «карт'є». Публікація через такий акаунт дозволяє іншим користувачам підхопити відео чи фото як доказ та поширити далі, не зважаючи на джерело чи його автентичність.

Наступним етапом є нашарування (layering), яке призводить до каскаду різних цитувань першоджерела. Це процес повторення та підсилення дезінформації багатократно задля того, щоб ускладнити пошук першоджерела, збільшити дистанцію до оригіналу публікації та ймовірність того, що ширше коло користувачів побачить цю інформацію. На цьому етапі можуть залучатись додаткові вебсайти, які можуть розміщувати на своїй платформі зовнішні матеріали, безкоштовно або ж як рекламні матеріали за гроші. Ці «посередники» діють як додатковий фільтр для відмивання першоджерела та допомагають ампліфікації наративу, щоб збільшити довіру до дезінформації.

Фінальним етапом цієї схеми є інтеграція (integration) - момент, коли дезінформація розповсюджується новинними виданнями з репутацією або отримує

широке розповсюдження реальними користувачами соціальних мереж. Таким чином, ця інформація отримує «визнання» та впливає на широкі верстви населення через те, що вона вийшла за межі «бульбашки». Цей етап дозволяє отримати певну «легалізацію» дезінформації через те, що публікація поруч з реальними новинами додає достовірності й певним чином робить дезінформацію такою, що її стає неможливо відрізнити від правди. Багато прикладів російської дезінформації після широкомасштабного вторгнення 2022 року було направлено саме на нормалізацію та відмивання наративів. Це й приклад з «карт'є» (Linvill and Warren, 2023), «віллами міністра оборони України» (Osadchuk, 2023b), а також «віллою Біла Косбі, яку нібито «придбав» Президент Зеленський» (Copeland, 2025).

Ці концепції є важливими для розуміння того, «як» рухається російський дезінформаційний контент, що детальніше проаналізовано у четвертому розділі цієї роботи на прикладі кількох російських операцій. Однак, розглядаючи внутрішнє споживання та поширення цієї інформації місцевими акторами, слід додатково враховувати психологічні та алгоритмічні чинники. Однією з таких концепцій є поняття «ехо-камери», що описує те, як цифрові медіа-середовища сприяють формуванню інформаційно ізольованих спільнот, які зміцнюють уже наявні переконання (Jamieson and Capella, 2008, с.84). Дискусія всередині таких спільнот є певним чином замкненою та самозацикленою, підсилюючи вже наявні бачення світу та погляди, а також радикалізуючи погляди учасників всередині. У той же час, багато дослідників Guess (2021) спростовують, що у сучасному світі є абсолютна інформаційна ізоляція, адже лише невелика кількість населення є дійсно ізольованою, бо більшість користувачів стикається принаймні з певною частиною альтернативного контенту. Проте, навіть незважаючи на те, що ізольованість не є поширеною, не варто недооцінювати ізоляцію саме тих високоактивних та ідеологізованих спільнот, на які найактивніше цілять російські інформаційні операції впливу.

Важливим є приклад Агентства інтернет-досліджень (IRA) під час виборів 2016 року. Дослідники детально описали шляхи та методи впливу росіян на конкретні

американські спільноти. На прохання Спеціального комітету Сенату США з питань розвідки (SSCI) група дослідників (DiResta et al., 2019) проаналізувала контент IRA та виділила специфічні стратегії таргетування. Наприклад, для впливу на афроамериканські спільноти росіяни відправляли повідомлення, які були зосереджені на делегітимізації участі у виборах. Для християнських спільнот — вони будували контент на фреймах релігійної свободи та мобілізації проти ЛГБТІК+, а для спільноти прихильників права володіти зброєю — розробили меми та повідомлення, орієнтовані на наратив про загрозу Другій поправці Конституції США, яка гарантує це право. Для ЛГБТІК+ спільнот росіяни таргетували як підтримуючий контент, так і анти-ЛГБТІК+ повідомлення, що свідчить про мету суспільної поляризації.

У свою чергу, Kate Starbird (2018) зазначає в аналізі діяльності IRA важливу деталь, зокрема, яким чином ця група брала участь у #blacklivesmatter русі на платформі Twitter (Arif et al., 2018). Так, дослідження показали, що IRA імперсоніфікували (брали роль) активістів як лівого, так і правого ідеологічного спрямування. Такий підхід дозволяє ще більше поляризувати суспільство й дискурс щодо тем, які його розколюють (Bail et al., 2020; Golovchenko et al., 2020). Отже, російські інформаційні операції інфільтруються в спільноти, видаючи себе за інших їхніх членів, завойовуючи довіру та збираючи аудиторію, мімкруючи під найактивніших їх представників. Далі ці операції починають використовувати цю довіру для досягнення інших цілей, наприклад, для сіяння розбрату та радикалізації. Розділення суспільства є логічним продовженням тактики «розділяй й володарюй», адже розділеним суспільством набагато легше маніпулювати. Іншою метою таких операцій може стати використання довіри для формування позицій в інших питаннях (Howard et al., 2019). Наприклад, групи IRA у ідеологічно правому крилі дискурсу почали підтримувати тоді кандидата у президенти Дональда Трампа, а ліві – критикувати його основну опонентку Гілларі Клінтон або ж підтримувати її опонентів у Демократичній партії.

Дезінформація також працює через складну інтеграцію повідомлень. Це не лише контент рідною мовою споживача, а й «експорт» внутрішньої російської пропаганди

назовні або ж зворотна адаптація іноземних наративів для самих росіян. Хоча межі між типами контенту наразі є досить умовними, а його автоматичний переклад та адаптація в російських інформаційних операціях стали тривіальними, наслідки таких процесів є вкрай серйозними. Наратив, який було створено російською мовою російськими державними медіа, має безперечний дефіцит довіри у більшості цільових груп за кордоном. Цей контент сприймається як «біла» пропаганда, бо її походження легко ідентифікується, й будь-які твердження піддаються сумніву (хоч і не завжди). Але цей же наратив, якщо він «перепакований» як такий, що походить від «незалежного» джерела й відшліфований для локальної аудиторії задля підбурення політичних невдоволення, постає не як іноземна пропаганда, а як місцевий політичний діалог. Тут варто зазначити, що у ролі такого джерела можуть бути як «корисні ідіоти», так і спеціально створені медіа, проте таке запозичення й розповсюдження можуть підпадати під категорію DIMI (domestic information manipulation & interference), на противагу класичному FIMI.

Іншим важливим напрямом сучасних досліджень дезінформації є безпосередньо контент. Наразі активно розповсюджуються штучно-згенеровані матеріали на додачу до класичних новин. Категорія «синтетичних» повідомлень охоплює надзвичайно широкий спектр контенту, створеного або зміненого за допомогою штучного інтелекту (ШІ). Одним із прикладів є діпфейк-відео, тобто відео контент, у якому обличчя та голос людини (або і те, і інше) замінено чи змінено за допомогою методів машинного навчання. Такий відеоконтент варіюється за рівнем складності, адже це може бути анімація статичних фото з очевидними слідами генерації, повна генерація або «ліпсинк» (синхронізація губ із текстом). Паралельно, в інформаційних операціях використовуються статичні ШІ-зображення, згенеровані дифузійними моделями (Nano Banana, Stable Diffusion) чи мережами GAN. Мережі GAN є ключовим інструментом для створення профілів у соцмережах під час операцій впливу (Chenrose, 2024) через свою простоту та низьку ціну. Стрімке покращення якості генерації синтетичних медіа суттєво впливає на оцінку загроз у сфері дезінформації. По-перше, різке зниження

вартості створення правдоподібного синтетичного контенту призводить до його широкого використання шкідливими акторами. По-друге, наявність цього інструменту дозволяє значно розширити спектр маніпуляцій, які є доступними для зловмисних акторів у межах їхнього бюджету. Як наслідок, виявлення таких синтетичних медіа стало пріоритетним напрямком досліджень у сфері дезінформації. Ця сфера спирається на комп'ютерні науки й підходи комп'ютерного зору, моделювання та аналіз соціальних мереж (SNA). Наприклад, Tolosana et al. (2020) представили широку таксономію методів генерації діпфейків та відповідних підходів до їх виявлення. Проте прогрес генерації штучного контенту не стоїть на місці й подальші дослідження відстежують динаміку ескалації між можливостями генерації та її детекції.

Окрім штучно згенерованих відео, важливим елементом онлайн-субкультур та, як наслідок, інформаційних операцій є поширення мемів, про що згадувалось в підрозділі 1.2. Schifman (2013, с.41) визначає меми як групу цифрових одиниць, які поділяють спільну характеристику контенту чи форми, існують з розумінням інших мемів, а також набувають поширення через імітацію та трансформацію користувачами. Мем фактично постає як одна з найбільш значущих комунікативних форм у сучасному дискурсі, а також як один із форматів, який досить активно експлуатується в операціях впливу (Pamment and Tsurtsumia, 2025). Меми поєднують у собі здатність комунікувати складні сенси у простому гібридному форматі «зображення та текст» із високим віральним потенціалом. Поширення мемів забезпечується їхньою впізнаваністю та багаторазовістю, а також низькою вартістю виробництва, особливо після розповсюдження генеративних моделей. Важливим елементом мемів є їхня певна стійкість до перевірки фактів, бо вони зазвичай мають значення, яке є прихованим або закодованим у культурних відсилках. Такі елементи досить важко розбивати як неправдиві факти, бо вони не викладені мовою конкретних тверджень. До того ж, меми можуть слугувати інструментами, які сигналізують ідентичність. Зокрема, якщо раніше споживання певних медіа (Carey, 1989) демонструвало приналежність до певної групи, нині меми в сучасному світі можуть сигналізувати про належність до певної позиції,

групи чи субгрупи. Умовно, негативні меми про Україну чи військово-політичне керівництво у коментарях під постами іноземних політиків чи інституцій можуть свідчити про певну позицію чи скоординовану неавтентичну поведінку, яка є частиною інформаційних операцій впливу.

Використання усталених форматів для мемів (зображень з реакцією, зациклених анімацій чи відео) для генерації нового контенту забезпечує швидке виробництво, адаптацію для нового наративу, а також негайне впізнавання ідеологічно узгодженого контенту спільнотою. Наприклад, операції Пригожинського Агентства інтернет-досліджень (IRA) значною мірою інвестували у використання мемних візуальних форматів, спеціально розроблених для їх прийняття та адаптації цільовими спільнотами (DiResta et al., 2019), на які чинився вплив. Завдяки стратегії шаблонізації створюється ефект наративного щеплення. Впізнавані візуальні маркери полегшують сприйняття нової інформації, інтегруючи її у вже сформовані когнітивні фрейми реципієнта.

Такий приклад впливу на мотивацію до поширення контенту як способу вираження ідентичності має важливі наслідки для успішності інформаційних операцій. Коли така операція впливу успішно додала мемні шаблони в цільові спільноти, власна органічна поведінка спільноти щодо поширення контенту буде тиражувати ці шаблони безвідносно до того, хто цю картинку додав у дискурс, як це було з відео у ТікТок про колишнього міністра оборони Олексія Резнікова, де сотні коментарів та тисячі поширень були зроблені реальними користувачами (Osadchuk, 2023b). Отже, вбудовані в меми наративні фрейми без додаткових операційних витрат отримали поширення серед людей, які мають недовіру до уряду. Поширюючи меми, що відповідають ідентичності, учасники спільнот одночасно зміцнюють власні ідеологічні переконання та сигналізують їх своїм контактам через свої органічні соціальні мережі. Така динаміка є найбільш ефективним використанням ресурсів операцій впливу, бо наративне посилення здійснюється або впливовими учасниками, або звичайними членами спільноти, які поширюють контент, який їм близький.

Іншим елементом сучасних досліджень дезінформаційних операцій є злиття з операціями у кіберпросторі або ж кіберзлочинами. Під такими операціями розуміють технічне проникнення, експлуатацію мереж та порушення роботи інфраструктури. Інформаційні операції впливу, на перший погляд, не мають нічого спільного з кіберзлочинами. Проте підтверджена практика російських державних суб'єктів, зокрема підрозділів Головного розвідувального управління (ГРУ) 26165 (Fancy Bear/APT28) та 74455 (Sandworm), демонструє інтеграцію технічних кіберможливостей та інформаційного впливу в межах оперативних структур РФ (Greenberg, 2019).

Rid та Buchanan (2015) стверджували, що найбільш значущі кібероперації отримують свою стратегічну цінність не лише від технічних результатів, а й від політичних сигналів та маніпуляцій в інформаційному середовищі, які стають можливими завдяки технічному проникненню. Минуле десятиліття задокументованих російських операцій повністю це підтверджує. Так, від операції зі зламу та витоку даних Національного комітету Демократичної партії США (DNC) у 2016 році, які були опубліковані через Wikileaks й отримали широке розповсюдження під час виборів 2016 року у США (Mueller, 2019), до атаки NotPetya у 2017 році, що призвела до порушення роботи цифрових систем в уряді України. Російські кібероперації вбудовуються для досягнення інформаційного ефекту, адже вони часто використовуються для створення наративів та делегітимізації персоналій та інституцій. Таким чином, кібер домен операцій доповнює й розширює інформаційні операції впливу. Наприклад, атаки на енергетичну інфраструктуру України у 2015–2016 роках, здійснені угрупованням Sandworm, були першими задокументованими деструктивними кібератакими проти цивільних електромереж. Ці атаки ілюструють значущий вимір інтеграції кібер- та інформаційних операцій — використання атак, що руйнують інфраструктуру, як механізм посилення наративу. Відключення електроенергії були технічною демонстрацією російських кіберможливостей, але їхня цінність для інформаційних операцій слугувала доказом російської сили й вразливості українських інституцій, також

неспроможності Заходу захистити своїх партнерів. Ці інформаційні наслідки фактично підсилювали безпосередній фізичний вплив.

Схожі операції відбуваються й після початку широкомасштабного вторгнення. Наприклад, росіяни запускають дезінформацію щодо відключень перед обстрілами, або ж поширюють дезінформацію, щоб уникнути відповідальності за воєнні злочини, як, наприклад, у випадку з завданням ракетного удару по Краматорському залізничному вокзалу у 2022 році (Digital Forensic Research Lab, 2022a).

Іншим пріоритетним напрямом досліджень є використання великих мовних моделей та штучного інтелекту у інформаційних операціях. Варто зазначити, що повна інтеграція можливостей великих мовних моделей (LLM) у російські операції на державному рівні залишається відкритим питанням, адже є докази роботи IRA, які використовували ручну роботу задля публікацій. Проте за останні роки є кілька задокументованих випадків, що підтвердили операції із використанням ШІ. У звіті OpenAI про аналіз загроз за жовтень 2024 року задокументовано видалення кількох акаунтів, пов'язаних з російською операцією, зокрема, виданням Stop News. Один актор з Російської Федерації використовував модель ChatGPT (OpenAI, 2024) для генерації контенту медіа англійською та французькою мовами, з інтенцією впливати на країни Африки. Також інші актори використовували LLM для генерації коротких коментарів у Twitter/X.

У той же час, окрім генерації контенту, ШІ дозволяє створювати правдоподібних синтетичних персонажів. Так, ботоподібні акаунти, що існували до появи великих мовних моделей (LLM), розпізнаються за поведінковими ознаками, включаючи регулярність публікацій, повторюваність контенту тощо (Varol et al., 2017). Персонажі, створені на базі LLM, можуть генерувати оригінальний контент, що є більш правдоподібним, а також можуть більш динамічно адаптувати свій стиль спілкування до різних контекстів та співрозмовників. Операції впливу активно використовують синтетичних персонажів у своїй діяльності. Так, у звіті Meta за другий квартал 2024 року згадується кілька російських операцій, частина з яких використовувала «згенерованих»

особистостей за допомогою GAN (Franklin et al., 2024) й розповсюджувала згенерований за допомогою ШІ контент.

Фінальним аспектом поточних досліджень є «гібридизація» російських інформаційних операцій, тобто дедалі більша інтеграція номінально приватних або громадських суб'єктів у державну екосистему інформаційних операцій. Гібридизація одночасно розширює оперативні можливості російського державного інформаційного апарату, приховує реальні державні витрати на пропаганду та дезінформацію, додає операціям «правдоподібного заперечення» (plausible deniability), а також ускладнює механізми юридичної відповідальності. Таке середовище інформаційних операцій фактично стирає межі між державними діями та недержавною поведінкою.

2.3 Методологія дослідження російських інформаційних операцій

Для дослідження реалізації російської стратегії інформаційної операції було обрано 3 різні кейси на різних платформах, які демонструють різні тактики для розповсюдження й публікації контенту, але водночас послуговуються генеральними лініями стратегії російських ІО. Ці три приклади не охоплюють усього обсягу ІО РФ, але показують, як саме виглядають ці операції після повномасштабного вторгнення 2022 року, коли традиційні медіа були заблоковані.

Операція «Двійник»

Перший кейс-стаді (операція «Двійник») демонструє використання рекламних можливостей платформ Meta, тобто Facebook та Instagram, для запуску реклами з нещодавно створених сторінок й досягнення реальних користувачів без побудови аудиторії. Тобто операторам ІО не потрібно робити зусиль, щоб публікувати цікавий контент і набирати підписників, а достатньо просто заплатити кошти, щоб негативний контент досяг цільової аудиторії. Проаналізована операція також демонструє використання технологічних інструментів для введення користувачів в оману, а саме демонстрації негативних публікацій під виглядом респектабельних медіа, як-от УНІАН

чи РБК-Україна, тобто створення двійників реальних медіа. Цей приклад було обрано через незвичність технічного підходу до розповсюдження неправдивої інформації через рекламу та підробку реальних медійних сайтів. Авторський корпус для цієї операції складає **649 скриншотів**. Цей корпус було зібрано вручну з мобільної та веб-версій платформи Facebook.

У рамках аналізу операції «Двійник» для цієї роботи протягом січня–липня 2024 року автором було зібрано скриншоти для аналізу *методом покрокового огляду стрічки*, який концептуалізували дослідники з Університету Солфорда (Великобританія) та з Університету Конкордії (Канада) (Light et al., 2016; Duguay and Gold-Apel, 2023). Цей метод передбачає покрокове вивчення та документування інтерфейсу соціальної мережі, аналізуючи її елементи. За допомогою цього методу було опрацьовано веб-версії та мобільний застосунок Facebook, де поширювалися рекламні повідомлення з фокусом на користувачів в Україні. Цей метод дозволив «налаштувати» стрічку та алгоритм соціальної мережі таким чином, щоб отримати якомога більше дезінформаційних повідомлень та реклами від російських акторів інформаційного впливу. Цей процес не можна назвати лінійним, адже він включав як звичне користування платформою та пошук публікацій, так і маніпуляції алгоритмом для показу контенту, релевантного для дослідження. Всі публікації було знайдено та задокументовано вручну, тобто щоразу, коли у стрічці з'являлися підозріла публікація або реклама, вона була проаналізована за наявністю схожих патернів до операції «Двійник» й у подальшому була задокументована через кілька знімків екрану. За можливості, збирались реклама, сама сторінка, прозорість сторінки (інформація про сторінку). Це дозволило зібрати масив даних, який опрацьовано у розділі 4.1.

Комерційна Facebook-реклама в Україні майже ніколи не зберігається у бібліотеці реклами після видалення, а сторінки, які запустили рекламу операції «Двійник», були тимчасовими та теж зникли з платформи. Це призвело до того, що іншої можливості для ефективного зберігання такої реклами, окрім як роблячи скриншоти, не було. Отже, *скриншоти екрану як метод*, тобто знімання екрану девайсу під час демонстрації

реклами, був чи не єдиним способом презервації ефемерного контенту, зокрема, реклами, яка зникає. Цей метод детально описується у роботі дослідників Університету Квінсленду (Австралія) (Hayden et al., 2024). Більше того, іноді патерни назв сторінок теж змінювалися, що ще більше ускладнювало пошук. Таким чином, впродовж більш ніж півроку автору вдалося зібрати 649 унікальних та неопублікованих раніше знімків екрану сторінок Facebook, які запустили рекламу, та самих рекламних чи наративних повідомлень, які ці сторінки розповсюджували. Ці знімки включають прозорість сторінок, фото рекламного повідомлення, інформацію про сторінку або ж комбінацію цих варіантів. Ця добірка є унікальним доробком, який не зберігся на платформі, не був описаний до цього та проливає світло на активності операції «Двійник» в Україні. Загалом, скриншоти охоплюють 251 унікальну сторінку Facebook.

Цей архів у цій роботі опрацьовано *методом аналізу цифрових артефактів*, який передбачає аналіз медіафайлів (картинок та відео), які розповсюджують користувачі соціальної мережі. Цей метод застосовували для аналізу публікацій у соціальних мережах дослідники з Оксфордського та Гарвардського університетів (Krafft та Donovan, 2020). Усі файли систематизовані за сторінками у Facebook та перейменовані для зручної навігації. Контент усіх сторінок опрацьовано *методом контент-аналізу* (Krippendorf, 2019) та *дискурс-аналізу* (Fairclough, 2013; Taranenko, 2023) з метою віднесення сторінок до певної наративної групи, яка об’єднує рекламні повідомлення за змістом. Це дозволило синтезувати основні цілі та повідомлення, які сторінки розповсюджували. До того ж, були проаналізовані патерни назв сторінок для виявлення закономірностей та еволюції у підході зловмисних акторів. Цей масив є унікальним, адже він не зберігся на самій платформі та існує виключно у вигляді скриншотів. Додатково, усі наративи опрацьовані задля визначення того, про що говорять рекламні повідомлення та який «порядок денний» намагаються сформувати у соціальних мережах.

У рамках аналізу цього унікального масиву було сформульовано гіпотезу щодо того, які цілі переслідують росіяни та що намагаються досягти.

- **Гіпотеза 1:** Російські інформаційні операції впливу в українському сегменті соціальних медіа спрямовані на деморалізацію населення України шляхом систематичного підриву довіри до державних інституцій та міжнародних союзників через встановлення негативного «порядку денного» засобами рекламних повідомлень і меметичних конструкцій.

Цю гіпотезу буде перевірено через *синтез знахідок унікального архіву* та його зіставлення зі стратегічними цілями російського впливу, які стали відомі завдяки публікації внутрішніх даних російських дезінформаційних підрядників Департаментом юстиції та ФБР США (Department of Justice, 2024a). Така перехресна перевірка дозволить перевірити, чи російські дезінформаційні актори продовжують використовувати ті самі цілі або ж змінили пріоритети з часом. До того ж, буде здійснено *пошук однакових цифрових артефактів*, які поширюються одразу на кількох платформах. Це буде зроблено задля пошуку зв'язків між акторами в рамках різних дезінформаційних операцій. Детальний аналіз представлено у Розділі 4 цієї дисертації. До того ж, у рамках розслідувань аналітичного центру «Лабораторії цифрових досліджень» Атлантичної Ради (DFRLab), в якому автор брав участь як аналітик, було проведено додаткову роботу й знахідки, які інформують та доповнюють це дослідження. Зокрема, у рамках дослідження 2022 року (DFRLab, 2022) автор аналізував набір з 1 633 облікових записів користувачів соціальних мереж задля виявлення неавтентичної поведінки та патернів, які використовували російські оператори. Було виявлено використання GAN-згенерованих зображень (фото користувачів, які були згенеровані штучним інтелектом), а також зафіксовано крадіжку фотографій реальних користувачів з соціальної платформи Vkontakte. У рамках іншого дослідження (Châtelet та Osadchuk, 2024) автор аналізував інфраструктуру підробки сайтів, тобто як генерувалася «штучна сторінка», коли користувач знаходився в іншій географічній зоні, та як саме реклама перенаправляла користувачів на потрібний сайт. Ці розвідки також використовуються у цьому дослідженні та детальніше описані у розділі 4.

Операція у TikTok

Другий кейс являє собою аналіз матеріалів дезінформаційного характеру в соціальній мережі коротких відео TikTok. Цей приклад було обрано через популярність цієї платформи та можливість навіть маргінального чи нового контенту сторінки з мінімальною кількістю підписників стати віральним. Таким чином, російські оператори ІО можуть продукувати й публікувати велику кількість контенту з розрахунку, що якась частина стане віральною. До того ж цей кейс демонструє, як контент з однієї платформи може знаходити аудиторію на інших платформах через дифузію контенту за допомогою розповсюдження з боку звичайних користувачів. Технологічно цей приклад є унікальним, адже демонструє відеоконтент, що відрізняється від текстових способів впливу. У рамках цього дослідження вручну було задокументовано у вигляді скриншотів 30 облікових записів та виявлено дифузію двох відео на інші платформи.

У рамках другого кейсу аналізу дезінформаційних повідомлень, представленого у розділі 4, було проаналізовано масштабну операцію РФ у соціальній мережі коротких відео TikTok. Методом покрокового огляду стрічки соціальної мережі Twitter/X автор знайшов розповсюдження відео з TikTok, яке звинувачувало тодішнього Міністра оборони України (2021–2023), Олексія Резнікова, у корупції через приклад купівлі будинку для доньки. Відео було задокументовано у вигляді знімків екрану, а також пошуку розповсюдження цього контенту на інших платформах, де він зберігся. Після побаченого було синтезовано припущення.

- **Гіпотеза 2:** Виявлені TikTok-відео є частиною координованої мережі неавтентичних акаунтів та відповідної операції впливу, а не ізольованим випадком дискредитації посадової особи.

Щоб перевірити ці припущення, було використано *мультимодальний метод детекції місінформації* (Barve et al., 2023), тобто метод аналізу відео, фото та звуку у повідомленнях соціальних мереж. Контент у цьому випадку зібраний у вигляді слайдів, які використовували скриншоти посадової особи та начитку голосом ШІ-помічника. Додатково, було використано *методи розвідки відкритих даних* та *верифікації фактів у мультимедійних документах* (Khan et al., 2025) задля аналізу відео на автентичність,

пошуку «нульового пацієнта» (оригінальної першої публікації відео), а також пошуку схожих відео та публікацій у інших форматах (текстовому та у форматі зображень). Задля аналізу акаунтів, які поширювали ці відео, було використано *розвідувально-послідовний змішаний метод досліджень* (exploratory, sequential mixed methods design - англ.) (Creswell, 2014), який має на меті всесторонній аналіз медійного артефакту. У рамках цього методу були виділені основні якісні характеристики акаунтів та відео, включаючи їхні неавтентичні характеристики, а також аналіз біо, хештегів, опису відео задля того, щоб потім зібрати масив подібних даних. Тобто, розпосюдження цього конетнту, а також пошук інших облікових записів операції було здійснено за допомогою встановлення характеристик першого відео та облікового запису з подальшим пошуком хештегів, біо та опису відео на платформі TikTok.

Для аналізу наративних патернів знайдених відео було використано *методи цифрової гуманітаристики*, а саме сегментацію відео та синтез історії, яку намагаються передати відео. За допомогою дискурс-аналізу, було концептуалізовано наративи, які просуваються операторами ІО в рамках цієї операції.

Згідно з *методологією аналізу дифузії неправдивої інформації у соціальних мережах*, яку використовували Vosoughi та ін. (Vosoughi et al., 2018), було проаналізовано приклади розповсюдження кількох відео у соціальних мережах поза оригінальними публікаціями на платформі TikTok. Тобто, реверсивний пошук зображень, а також пошук за ключовими словами з відео дозволили знайти той самий матеріал на кількох платформах.

Задля збереження ефемерного контенту частина відео та акаунтів була збережена у вигляді знімків екрану (Hayden et al., 2024), що дозволило авторові проаналізувати зібрані дані навіть після того, як платформа TikTok після звернення BBC видалила 12 800 акаунтів, які були частиною операції «Двійник».

Варто зазначити, що у рамках цього дослідження було проаналізовано унікальний набір даних у мережі TikTok, зібраний автором самостійно. Він включав кілька десятків відео (до 30 у вигляді скриншотів, та 20 у вигляді опису контенту). Після підготовки

відповідної авторської публікації в аналітичному центрі DFRLab (Osadchuk, 2023b), до організації звернулися представники організації BBC Verify, які досліджували цю ж операцію незалежно. Вони зібрали близько 800 відео кількома мовами. Співпраця в рамках цього дослідження в основному стосувалася обговорення патернів, які побачили дослідники обох організацій, а також можливості об'єднати зусилля для повідомлення платформі TikTok про скоординовану поведінку та планування одночасної публікації для широкого загалу. Фінальний продукт дослідження був різним, адже BBC сфокусувалася на одному відео та отримали коментар від осіб у відео, зокрема, у дочки екс-Міністра оборони України (Robinson et al., 2023), у той час як аналітичний доробок автора був направлений на виявлення патернів у відео та доведення кросплатформного характеру цієї російської операції, що продемонстровано у дисертації. Більшість знімків екрану, представлені та проаналізовані у цій роботі, є унікальними, адже вони не збереглися на платформі ТікТок та дозволяють оцінити елементи дезінформаційної операції, якої вже немає на основній платформі розповсюдження. До того ж, всі знайдені унікальні патерни (біо, хештеги) та приклади поширення на платформах, окрім TikTok, є унікальним доробком автора, який можна застосовувати для подальших досліджень.

Коментарі у соціальних мережах

Третім кейс-стаді є приклад інформаційного впливу у коментарях. Коментарі є досить старим методом впливу РФ в інформаційному середовищі, але згідно з документами АСП вони залишаються важливим вектором ІО. До того ж, імітація дискусії у соціальних платформах дозволяє операторам ІО здійснювати горизонтальний вплив на думку цільових аудиторій, створюючи ілюзію консенсусу задля провокування спіралі тиші.

У рамках третього кейс-стаді, описаного у розділі 4, було використано комп'ютеризований метод аналізу тем у коментарях соціальних мереж Telegram, Twitter/X та Facebook корпусу, що складався з **32561 коментаря.**

В рамках оригінального групового дослідження колективу дослідницької організації DFRLab, автор з іншими дослідниками зібрали 580000 коментарів з

платформ Telegram, X, Facebook через платформу моніторингу O'Savul протягом жовтня–листопада 2024 року (Osadchuk et al., 2024). Це дослідження стосувалось виключно пошуку повторюваного контенту й можливих патернів координованої неавтентичної поведінки.

Дисертаційне дослідження якісно й кількісно відрізняється від командного через аналіз меншого набору даних (за коротший період часу), застосування іншого методу (тематичне моделювання) та іншої мети – виділення наративів, які промотували неавтентичні коментатори. У рамках цього дослідження кількість коментарів була зменшена для репрезентативної вибірки у період з 22 листопада до 1 грудня 2024 року, а також дозібрано матеріал, який не був безпосередньо використаний у дослідженні DFRLab (кінець листопада й початок грудня).

Емпіричний матеріал було зібрано за допомогою платформи моніторингу O'Savul. Обирались акаунти за прапором платформи O'Savul «неавтентична поведінка» з коментарями українською та російською мовами. Це зроблено для того, щоб аналіз було проведено виключно щодо тих повідомлень, які містили повторювані дезінформаційні наративи та являли собою неавтентичні облікові записи з тематичним фокусом на Україну. Після фільтрування та очищення у фінальному наборі даних залишилося **32561 коментарів** задля аналізу тем та наративів у цьому корпусі.

У роботі для аналізу цього кейсу також використано *автоматизоване тематичне моделювання текстових корпусів коментарів* з платформ Telegram, Twitter/X та Facebook для виявлення та класифікації повторюваних наративних патернів у зібраних наборах даних соціальних мереж без попереднього маркування або наперед визначених таксономій. Було сформульовано гіпотезу.

- **Гіпотеза 3:** Скоординована діяльність у коментарях у досліджуваному корпусі переважно реалізує стратегію перенесення відповідальності за війну з Російської Федерації на Україну та країни Заходу й дискредитацію військово-політичного керівництва України.

Відтак, у рамках дисертаційного дослідження проаналізовано головні теми вибірки з 32,561 коментаря з трьох платформ соціальних мереж за допомогою *BERTopic* (Turton et al., 2021; Grootendorst, 2022), тобто *модульного підходу тематичного моделювання на основі трансформера* (нейронної мережі, яка базується на увазі). Цей підхід використано для індуктивного виявлення тематичних кластерів у корпусі коментарів російською та українською мовами у Telegram, який було попередньо зібрано за допомогою аналітичного інструменту O'Savul. Обробка й аналіз інтегрують чотири послідовні обчислювальні етапи, а саме: 1) семантичне векторне представлення; 2) зниження вимірності за допомогою UMAP; 3) кластеризацію на основі щільності за допомогою HDBSCAN; 4) репрезентацію тем.

Семантичне векторне представлення

Спочатку необроблений текст перетворюється на щільні числові представлення (ембединги або ж векторну репрезентацію понять), які фіксують семантичний зміст слів. У дослідженні застосовується *багатомовна модель трансформера paraphrase-multilingual-mpnet-base-v2* (Hugging Face, 2019). Вона формує 768-вимірне представлення для текстів більш ніж 50 мовами у спільному векторному просторі. Цей підхід забезпечує розташування семантично подібних висловлювань різними мовами поруч у просторі, незалежно від лексичних розбіжностей. Зокрема, однаковий текст чи поняття українською та російською мовами будуть знаходитися поруч та будуть визначені як частина єдиного кластера. Для аналізу зібраного набору даних це є ключовою перевагою, оскільки масив включає коментарі обома мовами. Перед подальшою обробкою, ембединги проходять L2-нормалізацію для забезпечення можливості порівняння документів.

Зниження розмірності за допомогою UMAP

Високовимірні простори ембедингів можуть охоплювати найменші зміни у тексті, проте вони не зовсім підходять для кластерного аналізу через те, що документи стають надзвичайно розкиданими у просторі, а кластери - менш інформативними. Для вирішення цієї проблеми відбувається *зниження кількості вимірів ембедингів за*

допомогою UMAP (Uniform Manifold Approximation and Projection; McInnes et al., 2018). UMAP зберігає глобальні топологічні зв'язки й зв'язки між сусідніми домукентами у просторі. Це робить його особливо корисним для наступної кластеризації на основі щільності. У цьому дослідженні застосовується *п'ятивимірна проєкція* (n_components = 5), де параметр n_neighbors = 15 регулює баланс між локальною та глобальною структурою, а min_dist = 0,0 - максимізує компактність кластерів. Ці характеристики дозволяють зменшити 768-вимірний простір до 5-вимірного, що спрощує подальший аналіз й кластеризацію, зберігаючи цілісність зв'язків між повідомленнями у багатовимірному просторі. Варто відзначити, що параметр n_neighbors вказує на кількість сусідніх точок, які алгоритм UMAP враховує під час побудови апроксимації у цьому дослідженні. Це компромісне значення, визначене автором, з огляду на те, що якщо взяти меншу кількість, то вона призведе до більш ізольованих наративних кластерів, які невірно передадуть інформаційний простір. З іншого боку, занадто велика кількість призведе до того, що кластери будуть всеохопними та не передаватимуть корисний сигнал. Відтак, доцільним для аналізу обрано п'ятивимірну проєкцію.

Кластеризація на основі щільності за допомогою HDBSCAN

Наративні кластери виявляються за допомогою HDBSCAN (Hierarchical Density-Based Spatial Clustering of Applications with Noise; Campello et al., 2013). Це ієрархічне розширення алгоритму DBSCAN, який динамічно виявляє кластери змінної щільності й не потребує від дослідника попередньо задавати кількість тем. При обробці векторів документи, що не належать до жодної достатньо щільної ділянки простору ембедингів, автоматично відносяться до класу шуму (тема −1). Це зберігає аналітичну цілісність решти кластерів, не створюючи зайвих документів у штучних угрупованнях. Мінімальний розмір кластера встановлено на рівні 50 документів. Це означає, що кластери з менше ніж 50 документами (коментарями) будуть відкинуті до шуму. Такий підхід у цьому дослідженні дозволяє уникнути надмірної деталізації та необхідність аналізу мікрокластерів. Обмеженням HDBSCAN у високовимірних текстових умовах є схильність відносити значну частку документів до класу шуму. Для мінімізації втрати

інформації у дослідженні застосовується процедура зменшення викидів постфактум. Зокрема, документи, які були первісно класифіковані як «шум», перепризначаються до тематично найближчого кластера за допомогою косинусної подібності в оригінальному просторі ембедингів за умови дотримання мінімального порогу подібності 0,5. Цей поріг означає, що документи, які частково подібні, але обговорюють наратив під іншим кутом, будуть включені, а менш подібні залишаться в категорії «шум».

Репрезентація тем: c-TF-IDF та максимальна гранична релевантність

Наступним кроком після ідентифікації кластерів є характеризація теми за допомогою класового варіанта алгоритму TF-IDF (c-TF-IDF; Grootendorst, 2022). Він обчислює значущість термінів на рівні кластера, тобто слова в рамках кластеру подібних повідомлень. Алгоритм розглядає всі документи певної теми як єдиний документ, порівнюючи частоту термінів із рештою корпусу. Цей метод дає упорядкований перелік термінів, які є повторюваними в межах одного кластера та вирізняють його відносно інших. Для зниження надмірності у наборах ключових слів тем на етапі репрезентації додатково застосовано алгоритм максимальної граничної релевантності (Maximal Marginal Relevance, MMR; Goldstein & Carbonell, 1996), тобто алгоритм диверсифікації, який ітеративно обирає різні ключові слова, балансуючи між релевантністю до центроїда (центру кластеру у просторі) теми та схожістю з уже відібраними термінами.

Як результат, отримані наративні тематичні кластери було опрацьовано та згруповано задля визначення груп, які описують схожі наративи. Ці групи детально описані у розділі 4. Ці наративні теми було порівняно з оприлюдненими документами російських підрядників з виробництва дезінформації задля виявлення можливих перетинів та неспівпадінь або трансформацій.

На основі всіх трьох кейсів, представлених у розділі 4, автор виводить рамку того, як РФ впроваджує стратегію ІО в інших країнах, насамперед в Україні та проти її союзників, намагаючись маніпулювати інформаційним простором. Як результат, виділено основні повідомлення та цілі, які проходять перехресну перевірку із внутрішніми документами РФ.

Гіпотеза 4: Повідомлення, виявлені у трьох проаналізованих кейсах, корелюють із цілями, зафіксованими у внутрішніх документах російських дезінформаційних підрядників (АСП, Структура), що підтверджує їхню належність до спільної інституційної архітектури впливу.

Також проаналізована можлива координація між різними операціями російського впливу на багатьох платформах за допомогою зіставлення з опублікованими внутрішніми документами російських акторів, а також використано *крос-секційний аналіз для мапування стратегії впливу РФ* на різних соціальних платформах. Спираючись на досвід попередніх досліджень дезінформації та концепцію спадковості операцій, ця робота ґрунтується на теоріях встановлення «порядку денного» та «спіралі тиші». Такий методологічний підхід дозволяє концептуалізувати стратегію РФ, спрямовану на штучне підвищення популярності маргінальних поглядів в Україні та Європі з метою поглиблення суспільного розколу та поляризації. Враховуючи описані методи протидії дезінформаційним операціям минулого українськими та іноземними дослідниками, патерни, описані у цьому досліджені, можуть бути використані задля додаткових порад щодо аналізу та протидії новітнім операціям РФ. Відтак, на основі проведеного аналізу сформульовано рекомендації щодо протидії деструктивному впливу на інфраструктурному, наративному та когнітивному рівнях. Запропоновані заходи узгоджуються з методологією планування інформаційних операцій, яка застосовується в США та країнах НАТО.

У дослідженні виявлено емпіричні патерни всіх трьох досліджуваних кейсів (наративні кластери, спільний візуальний матеріал, дифузію між платформами тощо), які у свою чергу співставлено з оприлюдненими внутрішніми документами російських дезінформаційних підрядників (АСП, Структура). Для підтвердження впевненості у зв’язку кейсів з документами, у роботі застосовується адаптована трирівнева шкала аналітичної впевненості. Ця шкала відповідає традиції аналітики розвідувальних організацій при аналізі операцій та подій. Цю рамку вперше запропонував Шерман Кент (Kent, 1964) й застосував для використання оцінки впевненості щодо певних подій. Для

оцінки впевненості у цьому дослідженні використовується адаптований підхід на основі роботи Кента та сучасного аналітичного стандарту розвідки США (Office of the Director of National Intelligence, 2023, ICD 203). Використання такого розрізнення впевненості обумовлено тим, що три досліджувані кейси спираються на якісно різні типи доказів. Деякі кейси поєднують виявлену активність із задокументованими акторами через технічні артефакти (технології, інфраструктура), а інші лише через тематичну й тактичну узгодженість.

Висока впевненість атрибуції спирається на конкретні технічні докази, що поєднують виявлену дезінформаційну активність із задокументованими інституційними акторами. До таких доказів належать: спільна технічна інфраструктура (домени, IP-адреси, інструменти управління трафіком та фільтрації користувачів), унікальний візуальний чи текстовий матеріал, який зустрічається одночасно у різних кампаніях. Також до цього рівня включаються URL-адреси та облікові записи, які прямо зафіксовані у внутрішніх документах акторів, або ж операційні артефакти на кшталт шаблонів назв сторінок та метаданих публікацій. Будь-які альтернативні пояснення зв’язку між операціями на цьому рівні впевненості є малоймовірними. Середня впевненість атрибуції спирається на тематичну, тактичну та хронологічну узгодженість виявлених операцій, а також активності, що співвідносяться з документованими цілями та *modus operandi* російських дезінформаційних акторів. Проте, на цьому рівні технічні докази прямого зв’язку частіше відсутні. Через це, цей рівень не виключає альтернативного пояснення зв’язку між операціями, проте зменшує вірогідність такого пояснення з огляду на сукупність ознак. Низька впевненість атрибуції спирається переважно на узгодженість виявленої активності з типовим порядком денним російських інформаційних операцій, тобто тематичне співпадіння з патернами російських інформаційних операцій. На цьому рівні альтернативні гіпотези щодо походження активності, як-от органічна підтримка проросійських поглядів реальними користувачам або активність інших проросійських акторів поза АСП/Структурою, не можуть бути повністю виключеними у межах наявних даних.

Застосування цієї шкали забезпечує більшу точність висновків і запобігає помилці, поширеній у дослідженнях інформаційних операцій, щодо змішування різних за силою типів атрибуції в єдину тезу.

Обмеження дослідження. Перед переходом до аналізу доктринальної та емпіричної частин, викладених у Розділах 3 та 4 цієї дисертації, необхідно зафіксувати низку обмежень обраної методології, які впливають на інтерпретацію результатів та межі їхнього узагальнення. Ці обмеження не знецінюють отримані результати, проте окреслюють коректні умови їхнього застосування та водночас формують підвалини подальших досліджень.

Обмеження вибірки операції «Двійник»

Авторський корпус 649 скриншотів рекламних повідомлень, зібраних протягом січня–липня 2024 року методом покрокового огляду стрічки (Light et al., 2016; Duguay and Gold-Apel, 2023), є вибіркою доступності. Така вибірка обумовлена закритістю платформ, нерівністю доступу до інформації про контент на платформах та алгоритмічністю платформ у видачі контенту (Ruths and Pfeffer, 2014). Тому це обмеження у дослідженні соціальних платформ є досить очікуваним, адже асиметрія доступу до даних не може бути подолана дослідником. Таким чином, ця вибірка не може претендувати на репрезентативність щодо всієї операції «Двійник» у глобальному масштабі або навіть у її повному обсязі в українському сегменті, адже операція відбувалась як мінімум 3,5 роки й продовжується надалі у тому чи іншому вигляді. Корпус дослідження репрезентує лише той зріз контенту, який алгоритм Facebook доставляв одному дослідницькому профілю, налаштованому на отримання дезінформаційного матеріалу, або який дослідник шукав самостійно у бібліотеці реклами на території України у визначений період. Із цього випливають кілька наслідків для інтерпретації результатів.

По-перше, оцінки відносної ваги окремих наративних кластерів (мобілізаційного, корупційного, антизахідного та ін.) є оцінками їхньої частки у фактичному авторському корпусі, а не репрезентацією всієї операції у інформаційному просторі. По-друге,

рекламні повідомлення та наративи, які алгоритм Facebook за тих чи інших причин не доставляв саме цьому профілю чи які не потрапляли у пошук в бібліотеці реклами, не потрапили до корпусу для аналізу та могли залишитись невиявленими. По-третє, тривалість збору та закритість алгоритму стрічки Facebook не дають змоги коректно реконструювати варіативність контенту операції та оцінити реакцію дезінформаційних акторів на конкретні політичні чи військові події.

Обмеження тематичного моделювання

Параметри обчислювальної схеми (n_neighbors = 15, min_dist = 0,0, n_components = 5 для UMAP; min_cluster_size = 50 для HDBSCAN) обрані з огляду на типові рекомендації для коротких текстів кількома мовами (McInnes et al., 2018; Campello et al., 2013), проте у межах цієї роботи не проводилося формального аналізу чутливості, тобто впливу змін параметрів на фінальний результат. Незначні зміни цих параметрів, наприклад, зменшення мінімального розміру кластера до 30 чи його збільшення до 100, здатні впливати на загальну кількість виявлених тем та на перерозподіл окремих документів між кластерами. Надійність 7-кластерного групування 125 тем, яке виконав автор у ручному режимі, не була верифікована через тестування надійності між кількома кодувальниками через відсутність інших кодувальників. Це може вплинути на надійність результату.

Багатомовна трансформерна модель paraphrase-multilingual-mpnet-base-v2 (Hugging Face, 2019) була натренована переважно на стандартних текстових корпусах (переклади великих наукових та інформаційних текстів). Таким чином, ця модель може демонструвати нижчу точність векторного представлення для коротких емоційних коментарів, які можуть містити обсценну лексику, меми та іронію, змішувати різні мови або використовувати нестандартну орфографію. Це може системно впливати на точність кластеризації окремих типів повідомлень, що особливо стосується коментарів, які активно використовують специфічну мову певної спільноти.

У дослідженні не використано корпус базового рівня органічних коментарів за аналогічний період, який дозволив би провести статистичне порівняння виявлених

наративних кластерів з тим, як розподіляються ці та інші теми у відповідному двомовному дискурсі. Внаслідок цього висновки аналізу корпусу слід інтерпретувати як такі, що описують внутрішню структуру наративів у корпусі координованих коментарів неавтентичних облікових записів, проте не дають розуміння статистичної різниці між досліджуваним корпусом та органічною дискусією. Зокрема, для тем на кшталт «Київська Русь належить РФ» (432 документи) чи «Гасло «Слава Україні!» є нацистським» (994 документи) у межах цього дослідження неможливо встановити, чи свідчить така частота саме про координований характер їхньої появи, чи про їхню загальну, в тому числі органічну, поширеність в екосистемі коментарів.

Аналізований період (22 листопада — 1 грудня 2024 року) обумовлений одночасно доступністю даних аналітичного інструменту O'Savul та збігом з кількома подіями українсько-європейського політичного порядку денного, серед яких візит єврокомісарів до Києва 1 грудня 2024 року (EU Commission, 2024), що спричинило сплеск коментарів у соціальних мережах українського сегменту щодо «зовнішнього контролю». Цей зріз становить близько дев'яти днів та не є випадковою вибіркою з ширшого часового горизонту операцій АСП. Відповідно, висновки щодо тематичної структури виявлених наративних кластерів не можуть бути екстрапольовані на середньостроковий та довгостроковий характер дезінформаційних кампаній російських акторів. Проте корпус є достатньо репрезентативним для аналізу повсякденної роботи та реакції операторів дезінформації на конкретний випадок політичного порядку денного у короткостроковій перспективі.

Атрибуція та класифікація облікових записів та коментарів як неавтентичних здійснювалися на основі даних аналітичного інструменту O'Savul, чиї алгоритми визначення не є предметом аналізу цієї роботи. Більше того, вони не публікуються розробниками інструменту у відкритому доступі через комерційну таємницю. Це обумовлює потребу стриманої інтерпретації корпусу як такого, що з доволі високою ймовірністю містить ознаки координованої неавтентичної поведінки, проте не як доведений й підтверджений корпус неавтентичних повідомлень, адже фінальну оцінку

завжди надає соціальна мережа, яка видаляє чи залишає акаунт на платформі. Для якісного підтвердження релевантності інструменту автором проведено ручну валідацію підвибірки з 50 облікових записів, 45 з яких підтверджують вердикт інструменту, що є прийнятним для дослідження.

Запропонована трирівнева аналітична рамка передбачає окремий когнітивний рівень як один із трьох вимірів дослідження сучасних російських інформаційних операцій. У межах цієї дисертації когнітивний рівень не операціоналізовано через експериментальний або опитувальний дизайн із залученням споживачів дезінформаційного контенту, через фінансові та етичні обмеження такого дослідження. Таким чином когнітивний вимір операцій спирається на дві опори: (1) наявну психологічну літературу про механізми сприйняття та поширення дезінформації (Lewandowsky et al., 2012; Kahneman, 2013; Pennycook and Rand, 2021; Ecker et al., 2022); (2) реконструкцію задумів та інтенцій операторів пропаганди, відображених у внутрішніх документах АСП та Структури (Department of Justice, 2024a; Pamment and Tsurtsumia, 2025). Вимірювання ефекту досліджуваних операцій на установки, переконання та поведінку реципієнтів виходить за межі цієї дисертації та визначене як один із пріоритетних напрямів подальших досліджень.

Зазначені обмеження окреслюють межі інтерпретації результатів та водночас формують підходи до подальших досліджень, серед яких: (а) розширення вибірки операції «Двійник»; (б) формальний аналіз стабільності тематичних кластерів за умови варіювання параметрів підходу; (в) побудова контрольних корпусів органічних коментарів для статистичних порівнянь; (г) валідація узагальненої наративної таксономії між кількома кодувальниками; (д) експериментальне вимірювання когнітивного впливу досліджуваних кампаній на цільові групи разом із контрольними групами. Ці напрями обговорюються детальніше у висновках.

РОЗДІЛ 3

СТРАТЕГІЯ РОСІЙСЬКИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

3.1 Методи інформаційних операцій від «активних заходів» до сьогодення

Дослідження сучасних російських інформаційних операцій часто страждає на упередження «нещодавнього». Сучасний вигляд операцій сприймається як феномен, що виник довкола виборів президента США 2016 року під впливом епохи соціальних мереж та є продуктом сучасної епохи. Це прочитання викривлює аналіз цих операцій та можливої стратегії протидії, спонукаючи дослідників фокусуватися виключно на технічній новизні платформних інструментів, а політиків пропонувати підходи до протидії, які зачіпають лише технологічний рівень. Таким чином, ці підходи фактично ігнорують інституційні основи феномену російських інформаційних операцій.

Натомість російські інформаційні операції становлять цілісну стратегічну традицію. Вони є сукупністю інституційних принципів, доктрин, структур та організаційних практик, які були опрацьовані раніше й просто адаптувалися до науково-технічного прогресу за умови збереження внутрішньої логіки. Ця традиція бере початок у революційній агітації більшовиків, але була систематизована й розширена до глобальних масштабів завдяки інфраструктурі «активних заходів» Радянського Союзу.

Доктрина «активних заходів» була формально систематизована у Першому головному управлінні КДБ наприкінці 1950-х. Створення нового підходу спиралося на оперативний досвід часів Сталінського режиму та традиції довоєнного Іноземного відділу Об’єднаного державно-політичного управління (ОДПУ). На додачу до цього, вона покладалась на теорію рефлексивного управління, що паралельно розвивалася у військовій науці. Основним інституційним осередком впровадження став Відділ «Д» (Дезінформація), створений 1959 року й пізніше реорганізований у Службу «А» у 1968 році під керівництвом Івана Агаянца.

«Активні заходи» систематично інтегрували розвідувальну діяльність з операціями впливу й використовували розвідувальні ресурси для збору інформації та формування інформаційного середовища супротивника. Замість того, щоб впроваджувати наратив напряму через одне дезінформаційне повідомлення, операції впливу використовували комплексну систему наративного нашарування. Вона починалася зі збору розвідувальних даних про вразливості та уподобання впливових цілей, що дозволяло краще зрозуміти цільову аудиторію. Надалі агенти готували сфабриковані документи для створення «доказової» бази майбутньої операції. Ці матеріали потрапляли у ЗМІ, які не мали формальних зв'язків з СРСР або радянськими агентами. Таким чином, операції створювали видимість незалежного журналістського відкриття. Наступним кроком було підсилення повідомлень через відомих людей чи лідерів думок, тобто локальних «агентів впливу» за кордоном. Вже на останньому етапі у гру вступали радянські офіційні джерела та медіа, які повторювали повідомлення й цитували попередні джерела. Цей підхід дозволяв створювати правдоподібне заперечення та підсилювати оригінальне повідомлення. Незважаючи на те, що всі джерела були частиною скоординованої операції, загальним результатом такого підходу ставав наратив, що мав видимість «незалежного» й підтвердженого кількома авторитетними джерелами (Bittman, 1985, с.56–60). Ця багатоетапна архітектура зробила такі операції складними для виявлення й протидії, відрізняючи їх від класичної пропаганди.

Щоб продемонструвати масштабність «активних заходів» варто розглянути найбільш ретельно вивчену радянську операцію «Інфекція» (з нім. Infektion), яка відома також як операція «Денвер». Ця кампанія була розпочата у 1983 році з метою відвернути увагу від порушення СРСР Женевської конвенції щодо нерозповсюдження біологічної зброї. В рамках операції радянські агенти поширили твердження про те, що ВІЛ/СНІД було створено як біологічну зброю військовими США на базі Форт-Детрік (Department of State, 1987, с.33–42; Boghardt, 2009; Rid, 2020). Перший етап кампанії розпочався 17 липня 1983 року із розміщення анонімного листа у газеті «Patriot», індійському

англомовному нішевому виданні, яке отримувало фінансування від СРСР. Лист від «анонімного читача» стверджував, що ВІЛ/СНІД може «поширитися» в Індії внаслідок американських експериментів, фреймуючи ВІЛ/СНІД як біологічну зброю. Стаття використала підхід «зерна правди», поєднавши реальні факти про ВІЛ/СНІД та минулі біологічні програми США з неправдивими відомостями. У свою чергу, вибір маловідомого індійського видання забезпечив правдоподібне й не пов'язане з СРСР походження скандального твердження. Початково матеріал не отримав поширення й три роки «висів у повітрі», аж поки 1985 року не був реактивований у «Літературній газеті», яка цитувала «Patriot» як першоджерело. Інформаційні агенції СРСР поширили заяву на міжнародному рівні у той час, коли розвідки союзних СРСР країн надали «наукові матеріали» на підтвердження «лабораторного» походження вірусу. У свою чергу, СРСР активно підключило дипломатичний корпус використовуючи радянські посольства як розповсюджувачів матеріалів в країнах-цілях. Навіть після розкриття ролі радянських спецслужб у цій операції Євгеном Примаковим у 1992 році (Rid, 2020, с. 337), наратив залишився впливовим серед країн так званого Глобального Півдня та афроамериканців у США (Boghardt, 2009).

Приклад операції «Денвер» демонструє засадничі принципи інформаційних операцій впливу, які зберігають актуальність у цифрову епоху. Багатоетапна архітектура інформаційного «відмивання» від непомітного розміщення у периферійному медіа до створення удаваного консенсусу структурно є ідентичною сучасним багатоплатформним російським операціям впливу. Ця архітектура постійно присутня у російських операціях після 2014 року й описана Linvill & Warren (2023) та Meleshevich & Schaefer (2018) як тріада «посів–нашарування–інтеграція». Орієнтація на існуючі переконання аудиторії (антиамериканські, постколоніальні) ілюструє підтверджувальне упередження (Kahneman, 2013), тобто факт, що люди радше вірять у те, що співпадає з їхньою точкою зору, а не у те, що підтверджується доказами.

Над контрольованими майданчиками для «посіву» розташовувався другий шар відмивання — видання та журналісти, які симпатизували СРСР та мали ідеологічно

близьку до СРСР редакційну орієнтацію, але не отримували фінансування напряму. Зазвичай це були газети лівого спрямування, журнали руху за мир та антиколоніальні часописи, які видавалися у Західній Європі, Азії та Латинській Америці. Ці журналісти фактично були «корисними ідіотами» (або «попутниками»), що підхоплювали та передруковували наративи з контрольованих видань. Вони розмивали розуміння радянського походження наративу й створювали ілюзію того, що він досяг незалежного міжнародного поширення. У сучасних дослідженнях цей рівень називають «нашаруванням» (Meleshevich & Schafer, 2018). Ефект цього шару часто був більш значущим, ніж у первинного «посіву», оскільки такі незалежні видання у Західній Європі та Північній Америці мали ширшу й впливовішу аудиторію, ніж видання, які використовувалися для початкового розміщення.

Третім, найвпливовішим шаром було вербування журналістів і редакторів у країнах-цілях як агентів КДБ. Завербовані журналісти зазвичай мали вразливості, пов’язані з ідеологічними симпатіями, фінансовою скрутою чи мали певні вади, які СРСР міг використати у вигляді компромату. КДБ цілило у людей, які займали посади з реальними редакційними повноваженнями, що робило виявлення таких агентів надзвичайно складним. Andrew & Mitrokhin (2000) описали десятки прикладів успішно завербованих журналістів у Західній Європі, зокрема, у AFP, головній інформаційній агенції Франції, працювало щонайменше 6 агентів і 2 контактів СРСР (там само, с.577).

Сучасні російські операції впливу відтворюють схожу логіку. Хоча значна частина випадків залишається непублічною, окремі приклади ілюструють збереження практики. Наприклад, задокументовані погрози журналістам після публікацій про російський вплив (Spike, 2026) або приховане фінансування Росією медіакомпанії в Теннессі через двох співробітників RT. У 2024 році Міністерство юстиції США (Department of Justice, 2024b) висунуло звинувачення за участь у схемі на 10 мільйонів доларів, яка фінансувала об’єднання коментаторів та інфлюенсерів, які публікували проросійський контент для американської аудиторії.

Іншим елементом російських інформаційних операцій, що продовжує використовуватись активно й досі, є фронт-організації. Це мережа номінально незалежних міжнародних організацій, які таємно керувалися СРСР та отримували звідти фінансову підтримку, водночас позиціонуючи себе як справжніх представників міжнародного громадянського суспільства. Упродовж 1970–1980-х мережа охоплювала десятки організацій з мільйонами індивідуальних членів. Ці організації функціонували у сферах пропаганди миру, прав робітників, студентської політики, прав жінок тощо. Координацію забезпечував Міжнародний відділ ЦК КПРС, який підтримував прямі відносини з комуністичними партіями за кордоном, у той час, коли Служба «А» КДБ забезпечувала фінансову підтримку та конкретні завдання. Серед найвідоміших організацій - Всесвітня рада миру (ВРМ), Всесвітня федерація демократичної молоді, Всесвітня федерація профспілок, Всесвітня рада церков, Міжнародний союз студентів та Міжнародна демократична федерація жінок (Department of State, 1987, с.1–2, 12; Rid, 2020, с.165, 286).

Розпад Радянського Союзу спричинив інституційний хаос і тимчасову деградацію системи інформаційного впливу. Сформована десятиліттями глобальна мережа фронт-організацій та «агентів впливу» була позбавлена фінансування та занедбана разом із самою радянською державою. Попри ці виклики, три процеси дозволили РФ вберегти оперативну експертизу та інфраструктуру в часи інституційної нестабільності. Дослідник Chatham House Keir Giles (2016a) задокументував теоретичну спадковість російської доктрини. Він проаналізував концептуальний апарат сучасних російських операцій впливу, який включав теорію рефлексивного управління та уявлення про інформаційний простір як стратегічний домен. Джайлз продемонстрував інтеграцію інформаційних операцій з військовою та дипломатичною стратегією, яка була адаптована з радянських коренів і оновлена у російських академічних та військових колах протягом 1990-х.

До того ж, вже з 2000-х років російська система іномовлення побачила свій розквіт. Почала відбуватись консолідація медіа, орієнтованих на зовнішню аудиторію.

Головним прикладом цієї стартегії є державний медіахолдинг «Росія Сьогодні», створений указом президента в грудні 2013 року шляхом злиття інформаційної агенції РІА Новини та Радіо «Голос Росії» (яке стало Sputnik). Призначення головної редакторки медіахолдингу Маргарити Симоньян означало посилення уваги до зовнішньої комунікації та координації між державою й медіа, що згодом проявилося під час початку Росією тимчасової окупації Криму та війни на сході України. До холдингу також увійшли пропагандистські видання російською мовою, орієнтовані на Україну (Україна.ру) та балтійські країни (Балтньюс). Координація між державними медіа та спецслужбами (ФСБ, СЗР, ГРУ) у проведенні операцій впливу очевидна у окремих прикладах, але недостатньо задокументована через їхній таємний характер. Публічне визнання такої координації могло б підірвати видимість редакційної незалежності російських медіа, що є необхідним для їхнього функціонування за кордоном.

Найбільш задокументований приклад операцій ГРУ — втручання у вибори президента США 2016 року. Цю кампанію також активно підсвічували RT і Sputnik. Ймовірно пов'язаний з ГРУ користувач *Guccifer 2.0,* опублікував персональне листування Комітету Демократичної партії США та представників президентської кампанії Гілларі Клінтон. У той же час, RT надавало платформу Джуліану Ассанжу, платформа якого опублікувала листування, й систематично висвітлювало витоки цих матеріалів (RT, 2016). RT негативно зображало Клінтон у своїх матеріалах, що зафіксовано у документах Офісу директора Національної розвідки США (Office of the Director of National Intelligence, 2017). Крім цього, телеканал RT підсилював інфраструктуру ботів та коментарів, висміюючи звинувачення у російському впливі. Зокрема, RT публікували у себе на сайті повідомлення акаунту *ten_gop* (RT, 2016), який зміг ввести в оману багатьох інфлюенсерів та політиків Республіканської партії США (Nimmo, 2017). Ця взаємодія не може бути просто випадковістю. У результаті Міністерство юстиції США заочно засудило 12 агентів російської розвідки з частин 26165 та 74455 ГРУ (Department of Justice, 2018).

Перехід російських інформаційних операцій на платформи соціальних мереж став якісним еволюційним кроком, який надав можливості, недоступні через «білі» джерела (Aleksejeva et al., 2019, с.4-7). Соціальні медіа забезпечили прямий доступ до іноземних аудиторій без потреби найму місцевих журналістів, а швидкість і тип контенту відповідали новим патернам споживання інформації. Таким чином, кожен матеріал отримував вірусний потенціал, а тисячі акаунтів користувачів могли взаємодіяти одне з одним та органічно поширювати такий контент. Систематична експлуатація Twitter/X, Facebook та Instagram неавтентичними акаунтами, пов'язаними з Росією, була детально задокументована у звітах Комітету з розвідки Сенату США (DiResta et al., 2019), в яких простежили розвиток операцій Агенції інтернет-досліджень Євгена Пригожина у соціальних медіа до масштабу, що охопив орієнтовно 126 мільйонів користувачів Facebook під час виборів 2016 року. Деякі акаунти IRA були настільки видімі й популярні, що їх поширювали політики та навіть родичі кандидата у президенти Дональда Трампа (Nimmo, 2017). Отже, сучасна мережа російських інформаційних операцій виходить далеко за межі RT та Sputnik, які є лише видимою «верхівкою айсбергу», що включає «фейкові медіа, створені для імітації справжніх новинних ресурсів, які засівають свої стрічки новин неправдивими або провокаційними матеріалами, пов'язаними з російськими наративами» (Giles, 2016b, с.46).

Сучасна форма російських інформаційних операцій після широкомасштабного вторгнення в Україну сформована трьома каталізаторами. По-перше, блокування «білої» інфраструктури RT та Sputnik у ЄС та США (European Council, 2022; Darcy, 2022) змусило Росію переорієнтуватися на онлайн-операції з допоміжними сайтами для впливу на союзників України. По-друге, зросла оперативна необхідність: інформаційні операції перетворилися зі стратегічного інструменту на пріоритет військових зусиль, адже російському режиму потрібно було продумувати інформаційне «алібі», заохочувати своїх союзників до підтримки, деморалізувати союзників України задля зменшення допомоги та отримання переваги на полі бою. По-третє, з 2022 року моделі генеративного штучного інтелекту прискорили роботу дезінформаційних агентів,

вирішуючи одразу кілька недоліків — мовну некомпетентність, обмеження людських ресурсів та фінансові обмеження, що історично сприяли викриттю дезінформаційних кампаній. Швидкий розвиток синтетичних медіа адекватної якості ускладнює аутентифікацію людиною, а скоординовані кросплатформні кампанії перевищують спроможність аналізу.

Після широкомасштабного вторгнення росіяни запустили кілька паралельних операцій, серед яких «Двійник» (Doppelganger, яка детально проаналізована у Розділі 4 цієї дисертації та підрозділі 3.3), «Перевантаження» (Overload), «Шторм-1516», «CopyCop» та «Portal Kombat». Операція «Перевантаження» (Atanasova et al., 2024), задокументована Reset Tech та CheckFirst, цілила не на широкий загал, а на факт-чекерські та дослідницькі організації. Росіяни, виробляючи дезінформаційний контент у великих обсягах, намагалися перевищити спроможності перевірки факт-чекерів, відволікаючи їх від роботи безглуздими перевірками заздалегідь неправдивої інформації. Дослідники зафіксували щонайменше 221 імейл, надісланий 20 журналістським організаціям, із таким контентом у різних форматах та мовах. У дослідників навіть складалося враження, що оператори хотіли публікації самих перевірок, оскільки це поширювало неправдивий наратив навіть у рамці його розбиття — спираючись на ефект забуття про джерело й «ефект сплячого» (пригадування факту, але не джерела чи контексту). Часто на перевірку надсилалися відео з логотипами реальних медіа на матеріалах, які ті ніколи не публікували.

Microsoft досліджував діяльність й ідентифікував зловмисну російську групу «Шторм-1516», яка активно працювала під час виборів президента США 2024 року (Zadrozny, 2024; Microsoft, 2024). Microsoft визначили основними методами групи «Шторм-1516» впливу виробництво коротких синтетичних відео, які були створені за допомогою згенерованих ШІ матеріалів та клонування голосу. У цю групу входять сфабриковані відео західних політиків, а також відео людей, які обговорювали вигадані події, зокрема «придбання Картьє Оленою Зеленською» (The Economist, 2024). До того ж, деякі відео були ліпсинк ШІ-відеозаписами, у яких висловлювання реальної людини

змінювалися через маніпуляцію нижньою частиною обличчя людини, що говорить. Хоч якість відео була посередньою - це не завадило цим відео поширюватись, сіючи неправдиві наративи (Microsoft, 2024; Warren et al., 2024). Серед задокументованих тем у рамках цієї операції: корупція українських і західних політиків, дискредитація Камали Гарріс та підсилення антиміграційних настроїв у США. Повідомлення цієї групи «відмивалися» через мережу журналістів RT, інфлюенсерів, ботів та «корисних ідіотів». Окремим напрямом та платформою для публікації була мережа підроблених сайтів, які використовували назви реальних старих газет, як-от Boston Chronicle, London Crier, DC Weekly, Miami Chronicle (Warren et al., 2024; Viginum, 2025). Згідно зі звітом французької урядової організації «Viginum», операція має зв'язки з Головним управлінням Генерального штабу ЗС РФ. Цей факт вчергове доводить, що попри перехід до системи підрядників, сучасні російські інформаційні операції впливу все ще керуються розвідкою.

Пов'язаною з групою «Шторм-1516» була операція «CopyCop». Саме вона включала інфраструктуру підроблених сайтів для впливу на західні аудиторії. Вперше цю операцію описала група «Insikt» компанії Recorded Future у травні 2024 року (Recorded Future, 2024a). Дослідники визначили механізм роботи цих сайтів, що фактично використовував ШІ для переробки контенту легітимних медіа. Цей підхід дозволяв сайтам на поверхні зберегти зовнішні ознаки журналістських сайтів та блогів. Архітектура операції (Recorded Future, 2024a; 2024b) майже не потребувала людського втручання через те, що автоматичні скрипти самостійно моніторили новинні джерела англійською, французькою та російською мовами. Наступним кроком автоматична система надавала статтям «ідеологічної» обробки через серію інструкцій для мовних моделей. Вже оброблені матеріали автоматично публікувалися через мережу приблизно 130 фейкових сайтів під місцеві бренди за назвами старих газет, на кшталт «London Crier» чи «San Francisco Chronicles» зі згенерованими ШІ-логотипами. Публікування сотень новин щодня демонструє новий рівень автоматизації. При чому, це інформаційне «відмивання» російських наративів одночасно зберігало ілюзію якості, адже навіть

підробні видання використовували імена журналістів з вигаданими біографіями. Згідно з дослідженнями Recorded Future, понад 1000 підроблених журналістських профілів використовувалися у системі під час американських виборів 2024 року. Ідеологічне упередження, що просувалося за допомогою великих мовних моделей, вдалося викрити завдяки частинам промптів (запитів), які росіяни забули видалити зі статей. Ці упередження були антиукраїнськими, критичними щодо підтримки України та Ізраїлю й ворожими щодо Демократичної партії США.

Ще одним прикладом операції російського інформаційного впливу є операція «Portal Kombat», яка включала мережу сайтів «Pravda», описану французькою урядовою організацією Viginum (Viginum, 2024a; Viginum, 2024b), а також CheckFirst та DFRLab, які створили дашборд для відстеження публікацій цієї мережі (CheckFirst & DFRLab, 2025). Ця розгалужена система проксі-медіа РФ видає себе за новинні ресурси країн-цілей. У певний момент свого існування вона налічувала понад 150 фейкових сайтів, які функціонували в 49 країнах кількома мовами, із характерною структурою «назва мови або країни + Pravda». Станом на квітень 2026 року всі домени мережі опублікували понад 7,5 мільйона статей. Серед головних тем - російсько-українська війна із висвітленням російського вторгнення як позитивного факту, а України - як «корупційної» та «нацистської». Контент підсилювався у соціальних медіа через скоординовані неавтентичні акаунти, а на інших платформах — через асоціацію за ключовими словами, адже сайти були добре оптимізовані під пошукові системи й опинялися в топі видачі за вузько специфічними запитами. Крім цього, українські канали мережі з приставкою «-news.ru» до назви міста були ехо-камерами російської пропаганди для місцевого населення. В інших країнах сайти міксували пропаганду з локальними новинами та, наприклад, інформацією про спорт. Джерелами для публікацій слугували російські державні видання, Telegram-канали цих видань та пов’язаних з Кремлем організації. Однак, неочевидною загрозою цих сайтів є їхня адаптивність та мімікрія під легітимні новинні джерела. Реальні користувачі можуть натрапити на ці матеріали через пошуковики, коли запитують про нішеві теми. У той же час великі мовні

моделі (чатботи) враховують та цитують ці джерела у відповідях на вузькі запити користувачів, що знижує правдивість висновків чатботів (NewsGuard, 2024). Це явище отримало назву llm-poisoning, тобто отруєння великих мовних моделей, в якому активну участь беруть безпосередньо ці сайти.

Отже, штучний інтелект та великі мовні моделі є важливими інструментами російських дезінформаційних операцій останніх років, оскільки вони спростили та здешевили виробництво контенту. Поява генеративного ШІ не запровадила принципово нової стратегії, а слугує методом розширення існуючих підходів через подолання обмежень людських та часових ресурсів. Великі мовні моделі нівелюють обмеження знання мов через якісний переклад на велику кількість мов, дозволяють автоматизувати створення облікових записів у соціальних мережах, а також забезпечують різноманітність візуального та текстового контенту. Раніше для поширення інформації за моделлю «потоку брехні» росіяни потребували значних людських ресурсів. Так, Пригожинське «Агентство інтернет-досліджень», за оцінками 2015 року, налічувало близько 1000 співробітників (Sciutto et al., 2017), які потребували позмінної роботи та великих бюджетів. У свою чергу, дослідження ризиків від ШІ для інформаційних операцій (Goldstein et al., 2023) виявило, що таке зменшення ціни виробництва контенту підвищить роль різноманітних підрядників, які зможуть продавати ці послуги державам. У майбутньому з’являться нові патерни поширення, які активно уникатимуть детекції, а контент стане більш якісним. Звіт OpenAI з аналізу загроз задокументував вісім активних операцій впливу, що використовували моделі OpenAI. Дві з цих операцій були пов’язані з Росією та використовували моделі для виробництва багатомовного контенту в соціальних мережах та перекладу статей (OpenAI, 2024). До того ж, дослідники зафіксували генерацію картинок для дискредитації Олімпійських ігор у Парижі та синтез зображень для фотографій профілів неавтентичних акаунтів.

Таким чином російська стратегія «активних заходів» продовжує існувати у новій формі, адаптуючись до вимог часу й нових доктрин, які будуть розглянуті у підрозділі 3.3. Нові операції завдяки новим інструментам можуть розгортатись впродовж годин, а

не років як це було раніше. У той же час, способи дискредитації опонентів, масової підробки документів, а також фреймінгу подій, використання «корисних ідіотів» та фальшивих аналітичних центрів залишилися майже незмінними. Проте інтенсифікація цих методів та відсутність будь-яких кордонів у цифровому просторі призводять до тривіалізації та здешевлення таких операцій впливу. Це спрощення робить активну протидію з боку демократичних держав необхідною умовою інформаційної стійкості.

3.2 Еволюція протидії російським інформаційним операціям

Реконструкція історії російських інформаційних операцій, викладена в попередньому підрозділі, показує інституційну спадкоємність «активних заходів» та сучасних гібридних форм протягом щонайменше століття. Хоча методологічний каркас цих операцій базувався на старих підходах, їхні технологічний та когнітивний рівень значно зріс завдяки глибшому розумінню механізмів і вразливостей людського мислення. До того ж, росіяни продукували нові документи й стратегії, що оглянуто у наступному підрозділі. Натомість історія протидії інформаційним операціям є істотно коротшою. Систематичні інституційні та концептуальні відповіді на дезінформацію як стратегічну загрозу формуються переважно за останні 20 років, а структурна архітектура такої протидії формується лише з другої половини 2010-х років. До цього на «активні заходи» відповідали розвідки чи державні інституції інших країн. Така асиметрія обумовлює сучасний інституційний ландшафт протидії інформаційним загрозам, який демонструє риси нестабільної системи, що знаходиться в процесі формування. Характерними рисами цієї системи є фрагментованість термінології, різноманіття організаційних традицій, нерівномірне фінансування й безперервна зміна базових концептів.

Нижче продемонстровано поверхневу реконструкцію цієї еволюції, розділену на чотири умовні історичні фази, що фокусуються на ключових інституційних подіях і методологічних проривах. Цей опис є стислим та не є вичерпним, а радше слугує містком до емпіричної частини дисертації (Розділ 4), у якій будуть надані рекомендації для протидії на основі конкретних російських операцій впливу 2022–2025 років.

Перша фаза: преінституційний період (до 2014)

Перші структуровані й окремі від журналістських редакцій організації, які займаються верифікацією фактів, виникають в англомовному просторі наприкінці 1990-х — на початку 2000-х років. Перші проєкти та організації, як, наприклад, проєкт «Snopes» (Snopes, 2026), заснований у 1994 році, були орієнтовані переважно на міські легенди й містифікації, а згодом - ставали факт-чекінговою платформою. Сайт FactCheck.org Центру публічної політики Анненберга при Університеті Пенсільванії було створено у 2003 році (RAND Corp, 2026). Це була перша ініціатива, яка спеціалізувалася на верифікації політичних заяв. Такі організації досить тривалий час функціонували як журналістська практика на периферії, що не інтегрована з дискурсом безпеки й не сприймалася як інструмент протидії стратегічним загрозам. Дезінформація як концептуальна категорія залишалася переважно артефактом досліджень Холодної війни, що мали досить обмежену академічну увагу після 1991 року.

У когнітивно-психологічному вимірі визначальним академічним внеском цього періоду стала колективна стаття Lewandowsky та ін. (2012), яка вперше системно реконструювала ефекти тривалого впливу дезінформації, а також межі ефективності спростувань та психологічні чинники стійкості хибних переконань. Незважаючи на свою концептуальну вагу, ця робота протягом кількох років після публікації залишалася переважно теоретичним внеском у дослідження переконань, а не інструментом операційної протидії.

Друга фаза: інституційний розвиток (2014–2016)

Перші спеціалізовані інституції протидії дезінформації як стратегічній загрозі виникають у відповідь на російські інформаційні операції проти України та гібридну війну, частиною якої були ці операції. У березні 2014 року, безпосередньо після початку тимчасової окупації Криму, при Могилянській школі журналістики постає проєкт «StopFake» (Romaniuk, 2025). Він був створений з метою розвінчування кремлівської дезінформації щодо України під час історичних подій 2014 року. Поступово цей проєкт пройшов інституційну еволюцію, яка дозволила інтегрувати практику факт-чекінгу в

програму вищої освіти журналістів в Україні (Romanuk and Fedchenko, 2025) й сприяла розвитку практичних навичок майбутніх журналістів.

У тому ж 2014 році в Ризі (Латвія) розгортається діяльність Центру передового досвіду НАТО зі стратегічних комунікацій (NATO StratCom CoE), першого міжнародного інституційного майданчика, який фокусувався на посилення можливостей НАТО у стратегічних комунікаціях, але в той же час, орієнтованого на дослідження інформаційних операцій супротивників.

У У 2015 році Європейська служба зовнішніх дій (EEAS) заснувала Оперативну групу з стратегічних комунікацій, відому як East StratCom Task Force. Це був перший спеціалізований орган Європейського Союзу, створений для аналізу та протидії російській дезінформації (EEAS, 2015). У межах цього проєкту була створена база даних EUvsDisinfo, яка документує приклади дезінформації (Звоздецька, 2022). Того ж року Інститут Пойнтера заснував Міжнародну мережу перевірки фактів (IFCN) (Poynter, 2026), яка встановила міжнародні стандарти для акредитації фактчекінгових організацій. Цей механізм дозволяє відрізняти справжні організації перевірки фактів від псевдоорганізацій, що можуть використовуватися для політичних або інших цілей. Досвід російсько-української війни продемонстрував важливість цієї акредитації, оскільки Російська Федерація під час широкомасштабного вторгнення намагалася використовувати інструменти фактчекінгу для пропаганди у межах проєкту «War on Fakes» (Romero, 2022).

Важливою характеристикою цього періоду є те, що інституційна реакція на російські операції впливу випередила політичний шок країн Заходу на події 2016 року, зокрема, Brexit та президентські вибори у США. Відтак, організації країн Балтії та України функціонували у цей період як система раннього сповіщення для всієї євроатлантичної спільноти. Україна, в свою чергу, інституційно й методологічно випереджала більшість країн західної демократії у розумінні загрози та протидії їй, проте ціною перебування у стані фактичної гібридної війни та інформаційного протистояння з РФ.

Третя фаза: інституційна хвиля та операціоналізація когнітивних інтервенцій (2016–2022)

Президентські вибори у США 2016 року та референдум щодо Brexit стали каталізаторами масових інституційних змін у країнах, які раніше були пасивними у питанні дезінформації. У 2016 році Державний департамент США створив Глобальний центр взаємодії (Global Engagement Center, GEC) як аналітично-координаційний орган для ідентифікації іноземних дезінформаційних кампаній (Global Engagement Center, 2023). У 2018 році соціальні платформи вживають термін скоординована неавтентична поведінка (CIB) (Meta, 2018), яка стає основою для видалення акаунтів і мереж, пов'язаних з іноземним впливом.

Паралельно відбувається операціоналізація когнітивних інтервенцій. Кембриджська лабораторія соціального прийняття рішень під керівництвом Sander van der Linden та Jon Roozenbeek публікує серію робіт, які переводять теорію «щеплення» McGuire (1964) із суто теоретичного виміру у площину масштабованих інструментів протидії дезінформації. Фундаментальна стаття van der Linden та ін. (2017) щодо «щеплення» проти кліматичної дезінформації оцінює ефективність цього методу у протидії, а ігровий формат «Bad News» (Roozenbeek та van der Linden, 2019; Roozenbeek та van der Linden, 2020) виступає першим прикладом масштабованого інструмента для «щеплення» від дезінформації. У той же час дебанкінг отримує спростування щодо своєї неефективності. Масштабне реплікаційне дослідження «ефекту бумеранга» (Wood and Porter, 2019) переглянуло попередні припущення щодо зворотного ефекту спростування, підтвердивши ефективність факт-чекінгу. А експериментальна робота Pennycook та ін. (2021) продемонструвала, що навіть мінімальне когнітивне втручання у механізм поширення новин може бути ефективним методом протидії. Дослідники визначили, що пропозиція оцінити точність матеріалу суттєво зменшує ймовірність поширення неправдивої інформації користувачами в соціальних медіа.

Інституціоналізується й OSINT-методологія (розвідка відкритих джерел). Цей період характеризується появою та становленням таких організацій як: Bellingcat,

Лабораторія цифрових розслідувань Атлантичної ради (DFRLab), Conflict Intelligence Team тощо. Вони виробляють відтворювані протоколи аналізу відкритих джерел, які стають професійним стандартом дослідження інформаційних операцій впливу. Водночас, у цей період оголюється основна проблема, яка ускладнює координацію між учасниками протидії - проблема фрагментованої термінології. Велика кількість організацій впроваджує власні підходи до документування та представлення результатів розслідувань, що породжує розбіжності в понятійному апараті. Таким чином, те, що журналіст називає «дезінформаційною кампанією», військовий аналітик кодує як «інформаційну операцію», а представник соціальної платформи — як «приклад координованої неавтентичної поведінки». Спроба розв'язати цю проблему призведе до появи рамки DISARM.

Четверта фаза: методологічна консолідація (2022–2026)

Повномасштабне російське вторгнення в Україну 24 лютого 2022 року каталізувало потребу в інституціоналізації підходів до збору даних, які мали б супроводжуватись консолідацією методології. У 2022 році представлено рамку DISARM (Terp and Breuer, 2022), яка була розроблена на основі моделі кібербезпекової рамки MITRE ATT&CK. Цей крок було представлено як спільну мову для документування тактик, технік і процедур (TTP) дезінформаційних операцій. Подальша еволюція рамки сталася через інтеграцію з форматом обміну даних STIX, а також спроби стандартизації робочих процесів демонструють тенденцію до методологічної уніфікації як необхідної умови ефективної транснаціональної координації.

Європейська служба зовнішніх дій (EEAS) з 2023 року починає публікувати річні доповіді про іноземну інформаційну маніпуляцію та втручання (FIMI), а також вказувати на багаторівневу архітектуру протидії такому впливу. Ці звіти демонструють певну еволюцію: у першому звіті була представлена методологія аналізу інцидентів (EEAS, 2023), у другому - рамка реагування (EEAS, 2024), потім - матриця викриття (EEAS, 2025) та і підходи стримування з повноцінним розгортанням моделі FIMI-ISAC

(EEAS, 2026). Таким чином, ці звіти демонструють необхідність спільної аналітичної інфраструктури обміну даними про інциденти між організаціями та країнами.

У регуляторному вимірі визначальною подією стає набуття чинності Регламенту про цифрові послуги (Digital Services Act), який запроваджує зобов'язання платформ щодо прозорості рекламних бібліотек та дослідницького доступу до даних великих платформ.

Цей період характеризується спробами подолати наявну фрагментацію у протидії. Каленський і Ганхіярві (Kalenský and Hanhijärvi, 2025) пропонують модель «чотирьох ліній оборони», яка систематизує заходи для протидії дезінформації у вигляді 4 рівнів. Ці лінії передбачають виявлення й моніторинг загроз, підвищення обізнаності щодо таких операцій, структурні втручання в медіасередовище для виправлення розломів і слабкостей, а також санкційні інструменти проти шкідливих акторів. До того ж цей період визначається концептуалізацією українських акторів протидії дезінформації та інформаційним операціям для того, щоб проінформувати союзників України. Одне з таких досліджень було підготовлене на основі інтерв'ю з 22 фахівцями з державного, приватного та неурядового секторів України, які займаються протидією дезінформації (Kalenský and Osadchuk, 2024). Це дослідження зафіксувало українську спадщину та підходи до протидії дезінформації в умовах війни, які можуть допомогти у розбудові кращої архітектури протидії дезінформації у демократичних країнах Заходу.

У той же час стало очевидним, що система протидії інформаційним операціям і дезінформації є вразливою та залежить від фінансування й політичної волі. У грудні 2024 року Глобальний центр взаємодії (GEC) при Державному департаменті США припинив своє існування через зупинку фінансування. Попри важливість роботи цієї інституції для атрибуції та протидії лише кілька років тому. У той же час велика кількість академічних і громадських організацій зі сфери протидії дезінформації втратила фінансування (Myers, 2025). Після зміни президентської адміністрації США Meta оголосила про припинення співпраці з факт-чекерами щодо маркування

неправдивого контенту в інтернеті (Jingnan et al., 2025). Ці епізоди ставлять під сумнів стабільність системи протидії, яка залежить від політики країн і волі мінливих платформ.

Паралельно, новий технологічний стрибок, що з'явився з появою у широкому вжитку та інтеграцією великих мовних моделей у виробництво синтетичного контенту, створює фундаментально новий вимір та масштаб загроз, небачені до цього. Цей технологічний розвиток принципово перевищує темпи розвитку методологічного інструментарію досліджень й протидії загрозі дезінформації.

Реконструйована еволюція дозволяє сформулювати кілька загальних спостережень. По-перше, інституційна відповідь на російські інформаційні операції істотно «молодша» й структурно більш фрагментована, ніж ці операції, які спираються на майже столітню традицію розвитку. По-друге, сучасний інституційний ландшафт протидії становить різноманіття паралельних організаційних традицій, як-от: журналістської, безпекової, академічної, платформної та регуляторної. Ці підходи лише нещодавно почали інтегруватися у спільну аналітичну рамку та спільне бачення, хоч ця інтеграція є далекою від завершення, на відміну від стратегії інформаційних операцій РФ. По-третє, поточна методологічна інфраструктура, яка дозволяє документувати окремі інциденти, переважає над системною інфраструктурою для об'єднання виявленої активності у спільне аналітичне знання. Ця проблема артикульована у четвертій річній доповіді EEAS (EEAS, 2026).

На тлі інституційних змін у протидії у наступному підрозділі представлено огляд стратегічної рамки сучасних російських інформаційних операцій, яка є більш усталеною та сформованою кількома ітераціями військових доктрин.

3.3 Російські доктрини інформаційних операцій

Російські інформаційні операції (ІО) отримали велику увагу дослідників з 2014 року, проте значна частина цих досліджень розглядає це явище як повернення радянських «активних заходів» у цифровій формі або як імпровізований побічний продукт опортуністичної політики Кремля. Обидва підходи недооцінюють те, що чітко простежується в офіційних російських документах. Протягом трьох десятиліть після

розпаду Радянського Союзу РФ накопичувала дедалі більший масив документів стратегічного планування. У цих документах інформаційні операції трансформувалися з вузької компетенції спецслужб на ключову концепцію національної оборони РФ.

По-перше, російські інформаційні операції (ІО) можна розглядати як оперативне вираження концепції інформаційного протиборства. Значення та інституційна прив'язка цієї концепції простежуються в доктринах інформаційної безпеки, військових доктринах, Стратегіях національної безпеки та Концепціях зовнішньої політики (Eggen, 2025). По-друге, стратегію можна зрозуміти як послідок історичного розвитку за останні 30 років, який можна умовно розподілити на кілька етапів й які будуть розглянуті нижче.

Аналіз стратегії РФ базується на аналізі російських та іноземних джерел, які аналізують російські документи. Цей підхід дозволяє зрозуміти оригінальне значення, закладене в ньому, та за потреби порівняти його із західними концепціями. Важливо зазначити, що цитування російських документів здійснюється для наочності та необхідності уникнення викривлень.

Розуміння російських інформаційних операцій (ІО) ускладнюється відсутністю відповідності між російською та західною термінологією. Три російські терміни зазвичай зводяться до одного англійського терміну «information warfare» (інформаційна війна): «інформаційне протиборство», «інформаційна війна» та «інформаційна битва» (Lilly & Cheravitch, 2020, с.130). Найважливішим із цих трьох термінів є саме «інформаційне протиборство». Західні дослідники на основі російських документів визначають його як «цілеспрямоване використання наступальних або оборонних інформаційних засобів для досягнення політичних, економічних, військових та інших цілей у мирний, змагальний та воєнний час» (Grisé et al., 2022). Російська доктринальна література використовує термін «інформаційне протиборство» для позначення постійного стану суперництва в інформаційній сфері, який не обмежується формальним оголошенням війни. Тобто цей стан охоплює діяльність як у мирний, так і у воєнний час. Це поняття є відповіддю на концепції інформаційної війни США та НАТО. Проте воно

ширше за поняття НАТО «інформаційних операцій», які зазвичай виконують функцію допоміжного інструменту для кінетичних операцій.

Критично важливим для розуміння є поділ інформаційного протиборства на дві сфери: 1) інформаційно-технічне протиборство, що за широким значенням еквівалентне кібероперацій проти мереж, обладнання та даних; та 2) інформаційно-психологічне протиборство, що охоплює те, що можна назвати інформаційними операціями та пропагандою. Ці частини є компонентами єдиної інтегрованої практики. Існуючий поділ на дві сфери є радше аналітичною зручністю, яка трохи ускладнює розуміння суті явища (Giles, 2016b, с.7–9). Тобто для РФ цифрово-технологічні та когнітивно-психологічні інструменти є нерозривно пов'язаними. В українській науці Почепцов розглядав поняття «когнітивних атак» як невіддільне від технічних платформ їхнього здійснення (Pocheptsov, 2018).

Варто відзначити, що російські військові й безпекові доктрини сприймають інформаційні операції як форму когнітивної війни (Giles, 2016b, с.8–10), тобто систематичного ураження когнітивної архітектури, за допомогою якої демократичні суспільства формують політичні судження. У російських джерелах цей підхід називається рефлексивним контролем (Snegovaya, 2015), який є частиною концепції інформаційного протиборства, яке сприймає інформацію як ресурс для захисту власної аудиторії від ворожих впливів та досягнення «політичних, економічних та інших цілей за допомогою знищення інформаційних систем ворога та отримання контролю над його інформаційними ресурсами» (Grisé, 2022, с.7–10). Система інформаційного протиборства спирається на розуміння когнітивних упереджень (підтверджувальне зміщення, когнітивний дисонанс), напрацювань соціальної психології (соціальні ідентичності, поляризація) та алгоритмічної природи сучасних комунікаційних систем (алгоритмічна ампліфікація, фільтраційні бульбашки) й використовує ці інструменти для виявлення когнітивних вразливостей у демократичному суспільстві-цілі. Інформаційна війна спрямована на підрив суспільних інституцій, зокрема,

журналістики, науки, виборчих систем, судів тощо, які є основними джерелами політичних дискусій у демократіях, через створення системи абсолютної недовіри.

Важливо також термінологічно уточнити поняття «м'яка сила», яке зазвичай використовується для позначення стратегічних комунікацій та інструменту промоції культури. Проте російська доктрина з 2013 року послідовно визначає цей термін як евфемізм для позначення західної «інформаційної агресії» проти Росії. У Концепції зовнішньої політики 2013 року західна «м'яка сила» чітко характеризується як інструмент «деструктивного та незаконного використання» проти суверенних держав. Така асиметрія є стратегічною ознакою, адже описуючи власні еквівалентні за змістом дії, російська держава віддає перевагу термінам «підтримка співвітчизників» або «інформаційна безпека», але ніколи не вживає термін «м'яка сила» у сенсі теорії Джозефа Ная.

Період 1 – 1990-ті

У 1990-х роках було створено масив російськомовних теоретичних праць про інформаційну війну, які передбачили й сформували офіційну доктрину. Публікації Сергія Модестова, Олександра Караяні та інших ввели у російський військово-академічний дискурс термінологію «інформаційної зброї», «інформаційної агресії» та «інформаційного протиборства», спираючись як на радянських попередників так й доктрини США (Thomas, 2004; Giles, 2016b, с.5–7).

РФ створює концепцію національної безпеки у грудні 1997 року, з оновленою редакцією в січні 2000 року. Ці концепції ввели поняття «інформаційну безпеку» як визначену категорію національної безпеки. Концепція 1997 року поверхово визначила інформаційну безпеку як «безпеку її багатонаціонального народу» (Сайт президента России, 1997), проте вона заклала концептуальну основу для доктрини інформаційної безпеки 2000 року.

Період 2 – 2000 – 2008 рр.

Після приходу до влади Владіміра Путіна починається другий етап розвитку російських можливостей в інформаційній сфері. Вже в перший рік його президентства

було прийнято 2 важливі документи. У 2000 році було утверджено трохи оновлену концепцію 1997 року на офіційному рівні (Сайт президента России, 2000). Цей документ зазначив необхідність протидії загрозам в інформаційній сфері. Проте значно вагомішим був документ — Доктрина інформаційної безпеки Російської Федерації, (Garant, 2000). Цей документ виконує три функції, наслідки яких досі простежуються у Концепції зовнішньої політики 2023 року (Министерство инностранных дел РФ, 2023).

По-перше, він визначив «інформаційну безпеку» як захист «національних інтересів в інформаційній сфері». У цьому документі національні інтереси включали не лише критичну інформаційну інфраструктуру, а й «духовне життя», «традиційні моральні цінності» та «історичні, культурні та патріотичні основи» російської держави (Garant, 2000). Таке поєднання культурної та інфраструктурної сфер у межах однієї категорії безпеки стало основою доктрини, що можна визначити як концепт «залучення всього суспільства» (whole-of-society approach). По-друге, Доктрина 2000 року представила Росію як оборонного актора, що постає перед обличчям ворожого зовнішнього інформаційного середовища. Ця тема визначатиме майбутній фреймінг будь-яких агресивних дій та документів РФ.

Наступні документи цього етапу деталізували сформовану структуру. Концепція зовнішньої політики 2008 року формалізувала «інформаційний супровід» зовнішньої політики як пряме завдання Міністерства закордонних справ (Министерство инностранных дел РФ, 2008). Того ж року відбулося створення міжнародного телеканалу RT та суттєве посилення державного фінансування іномовних інформаційних продуктів.

Російсько-грузинська війна 2008 року стала переломним моментом для стратегії інформаційної війни РФ (Giles, 2016b, с.35–6), адже навіть росіяни визнавали, що попри успіхи на полі бою, Росія «програла інформаційну війну». Тбілісі ефективно сформував наративи для західних медіа під час цієї короткотривалої війни, й ця сприйнята поразка стала причиною наступного етапу реформування.

Період 3 – 2008 – 2013 рр.

До незаконної окупації Криму РФ активно почала реформувати свої можливості у сфері інформаційних операцій та протиборства. Цей етап розвитку системи був концептуалізований на трьох офіційних документах та одній статті. Першою є Військова доктрина прийнята у лютому 2010 року (Сайт президента России, 2010). Цей документ вийшов за межі загального визнання інформаційних загроз, притаманного доктрині 2000 року. Він визначив конкретні завдання Збройних сил в інформаційній сфері, а саме «розвиток сил і ресурсів для інформаційного протистояння».

Другим важливим документом є «Концептуальні погляди на діяльність Збройних сил Російської Федерації в інформаційному просторі», опубліковані Міністерством оборони у грудні 2011 року (Министерство обороны РФ, 2011). Цей документ часто вважають першою російською військово-кібернетичною прото-доктриною (Giles, 2012). «Концептуальні погляди» неодноразово апелюють до законності, запобігання конфліктам та заходів зміцнення довіри, тобто повторюють «лінію самозахисту». Водночас документ стверджує можливість ЗС РФ діяти наступально в інформаційному просторі у разі загрози російським інтересам.

Третім документом цього періоду є Концепція зовнішньої політики Російської Федерації 2013 року (Garant, 2013). Це перший документ, у якому «м'яка сила» визначена як окремий інструмент зовнішньої політики РФ та як категорія загрози, коли вона використовується ворожими державами для «політичного тиску на суверенні країни». Поєднання «Концептуальних поглядів» 2011 року й цієї концепції демонструє стратегію, в якій цивільні та військові інструменти інформаційного протистояння дедалі частіше уявляються як частини єдиного спектру інструментів ведення протиборства.

Проте найбільш відомим і водночас невірно трактованим текстом цього періоду є стаття начальника Генерального штабу Валерія Герасимова (Герасимов, 2013). Західні аналітики невірно інтерпретували цю роботу як «доктрину Герасимова». Цей термін у своєму блозі Марк Галеотті ввів у 2013 році, інтерпретувавши статтю як оголошення нової російської доктрини «гібридної війни». Згідно з цим підходом невійськові засоби, включно з інформаційними операціями, домінуватимуть у майбутніх конфліктах. У

2018 році сам Галеотті відмовився від цього терміна, визнавши, що стаття радше описувала те, що Герасимов вважав західним способом ведення війни. (Galeotti, 2018). Цю статтю краще доповнює та прояснює робота Сергія Чекінова та Сергія Богданова, які артикулювали конструкцію «війни нового покоління». Згідно з цією концепцією поєднання інформаційних операцій та інших невійськових засобів із військовою силою є вирішальним у сучасних конфліктах (Berzins, 2014, с.4–6).

Період 4 – 2013 – 2022 рр.

Період між нелегальним захопленням Криму та повномасштабним вторгненням в Україну створив архітектуру російського інформаційного апарату, який перетворив інформаційні операції на постійний елемент російського державного управління. У цей період було кілька ключових документів.

По-перше, воєнна доктрина від грудня 2014 року (Совет Безопасности Российской Федерации, 2014) містила принципово нові формулювання щодо інформаційної сфери. Стаття 12 пункт м визначав серед основних зовнішніх військових небезпек для РФ «використання інформаційно-комунікаційних технологій у військово-політичних цілях». Таке формулювання одночасно вказувало на небезпеку для РФ з боку «західної інформаційної агресії» та закладало стратегічну основу для дій у відповідь.

По-друге, стратегія національної безпеки 2015 року (Сайт президента России, 2015) внесла до офіційної стратегії РФ геополітичне бачення ворожості західної політики стримування як «протидії» самостійній російській політиці. У той же час, основні положення щодо інформаційної безпеки узгоджувалися з доктриною 2000 року. Пізніше, у стратегії 2021 року це бачення буде підсилено.

У свою чергу, доктрина інформаційної безпеки 2016 року (Garant, 2016) є найважливішим документом цього етапу, що замінив доктрину 2000 року. У цьому документі оновлено поняття інформаційної безпеки, яка має протидіяти ворожому «інформаційно-психологічному впливу на населення». Окремим пунктом зазначено, що ворожий вплив спрямований на молодь з метою «розмивання традиційних російських духовно-моральних цінностей». Ці доповнення є істотним розширенням меж

безпекового дискурсу, адже тепер РФ може вважати будь-яку комунікацію, що не збігається з інтересами держави, ворожою. Доктрина чітко визначає «сили та засоби інформаційного протиборства» як важливу складову спроможностей Збройних сил РФ у сфері інформаційної безпеки. Це формулювання отримало практичне підтвердження у публічній заяві міністра оборони Сергія Шойгу в лютому 2017 року (РБК, 2017). Шойгу заявив, що Росія має у складі Збройних сил спеціалізовані «війська інформаційних операцій», що мали фокусуватись на контрпропаганді та протидії хакерським атакам, знову підтверджуючи нерозривний характер кібер та інформаційних операцій у російській стратегії.

Стратегія національної безпеки від липня 2021 року (Сайт президента России, 2021) є вершиною російської інформаційної доктрини до широкомасштабного вторгнення до України. Окремий розділ цього документу присвячений «інформаційній безпеці». Він розглядає іноземну інформаційну діяльність як екзистенційну загрозу російському суверенітету, продовжуючи конспірологічну лінію захисту від зовнішніх загроз. Документ побічно згадує необхідність забезпечення захисту від контролю іноземних корпорацій над досутпом до мережі, фактично закладючи підвалини до створення «суверенного сегменту» інтернету. Документ також наводить приклади небезпеки через насадження «чужих ідеалів та цінностей», які можуть призвести до поляризації, що фактично описує те, що робить сама РФ в інших країнах. Таким чином, ця стратегія опрацьовує методи протидії інформаційним операціям та іншим інструментам, які сама РФ й використовує, що було описано підрозділі 1.1.

В монографії «Світова гібридна війна: український фронт» (Horbulin, 2017) дослідники висувають тезу про те, що російська інформаційна агресія є спадкоємницею «активних заходів». До того ж, вони концептуалізували стратегії РФ з використання історичної пам'яті та наративів ідентичності як інструментів когнітивних операцій. Насамкінець, українські дослідники доводять, що сучасну російську агресію слід розуміти як очолюване Росією втілення ширшого процесу «гібридизації світу». Згідно з

цим процесом, розмивання чітких часових і категоріальних меж між війною та миром стає структурною ознакою міжнародної системи (Horbulin, 2016).

Період 5 – 2022 – 2026 рр.

Повномасштабне вторгнення в Україну в лютому 2022 року зумовило появу двох документів стратегічного планування. Разом вони відображають еволюцію російської інформаційної доктрини у воєнний період. Першим документом є Концепція гуманітарної політики Російської Федерації за кордоном 2022 року (Сайт президента России, 2022), а другим — Концепція зовнішньої політики Російської Федерації 2023 року (Министерство инностранных дел РФ, 2023).

Концепція гуманітарної політики формує інституційну архітектуру, через яку Росія здійснює «гуманітарний» вплив за кордоном. Частинами цієї архітектури є «Росспівробітництво», фонд «Русский мир», мережа російських домів по світу тощо. Цей документ формалізує зв'язок між «підтримкою співвітчизників», захистом «традиційних духовно-моральних цінностей» та просуванням російських наративів. На думку американських аналітиків, цей документ є підґрунтям для оперативної практики використання інструментів гуманітарного характеру як платформ для здійснення впливу. У межах цієї мережі ідеологічна концепція «Русского мира» виступає в ролі сполучного елемента (Bergmann et al., 2022). До того ж, виокремлення захисту російськомовних громадян й врахування цього питання в рамках двосторонніх відносин з Грузією та Молдовою можуть свідчити про агресивний підтекст цієї політики, враховуючи російські інформаційні операції проти цих країн.

Концепція зовнішньої політики є найбільш консолідованим вираженням сучасного російського стратегічного підходу. Концепція характеризує Російську Федерацію як «державу-цивілізацію» й позиціонує Росію як головний полюс створюваного багатополярного устрою. Документ окреслює відносини з «США та їх сателітами» як доктринально закріплене й постійне протистояння (Министерство инностранных дел РФ, 2023). Цей документ впроваджує 3 особливості для інформаційних операцій. По-перше, він виокремлює «русофобію» як категорію

державної політики «недружніх країн», що постійно використовується як ярлик проти будь-яких дій інших країн, з якими РФ не погоджується. По-друге, у ньому міститься пряме посилання на «гібридну війну», яку нібито Захід розпочав проти Росії. Це надає РФ умовну санкцію на забезпечення безпеки й агресивним діям в інформаційному просторі проти країн Заходу. По-третє, документ визначає «формування більш справедливого, багатополярного світового устрою» разом зі зменшенням «гегемонії недружніх країн» пріоритетними завданнями російської дипломатії. Для досягнення цього результату інформаційні інструменти розглядаються як один із основних.

Еволюція офіційних документів РФ за останні 30 років супроводжується зрілістю інституційної архітектури, через яку здійснюються російські інформаційні операції (ІО). Для аналізу доцільно виокремити п'ять рівнів, які загалом узгоджуються з типологією «стовпів» Центру глобальної взаємодії (GEC, 2020) від 2020 року, але з урахуванням змін після 2022 року та специфіки класифікацій, розроблених в українській практиці моніторингу.

Серед головних акторів сучасних інформаційних операцій впливу — урядовці й дипломатична система РФ. Ці посадовці повторювали дезінформаційні наративи як, наприклад, повідомлення про «біолабораторії» (Digital Forensic Research Lab, 2022b). У свою чергу російські медіа, цитуючи посадовців, поширюють ці наративи далі та є другим рівнем. А представники російських дипломатичних установ дають інтерв'ю місцевим виданням, інтерпретуючи події РФ у вигідному ключі. Дослідження DFRLab показують планомірне використання дипломатичного корпусу для просування дезінформації «антиколоніального» характеру війни проти України серед країн так званого Глобального Півдня (DFRLab, 2023b; DFRLab, 2024).

Попри блокування основних медіа в ЄС та США, RT і Sputnik продовжують працювати в Латинській Америці, на Близькому Сході та в Африці, висвітлюючи «інший погляд» на світові події та зображуючи РФ як бастіон «традиційних цінностей». Окрім цього, росіяни також використовують проксі-видання, що відмивають заблокований

контент RT (Schafer et al., 2024), та аналітичні центри на кшталт Strategic Culture Foundation.

Третім рівнем можна вважати проксі-організації та гуманітарні механізми. До перших можна включити псевдоаналітичні організації як Центр стратегічної культури, а до останніх — Росспівробітництво, мережу культурних центрів «Русский дом», фонд «Русский мир» і т.і.

Четвертим рівнем є інформаційні операції військових та розвідувальних служб. Серед них офіційно визнані «війська інформаційних операцій» Збройних сил, підрозділи ГРУ № 26165 та № 74455, які були визначені у санкційних документах, а також непублічні підрозділи СЗР.

Фінальним рівнем є «комерційні» структури, як-от «Агенція інтернет-досліджень» Пригожина та більш сучасні Агенція соціального проєктування (АСД), група компаній «Структура національних технологій» (Структура) та АНО Діалог (Pamment & Tsurtsumia, 2025). Ці організації становлять «чорну» пропаганду РФ, виконуючи роботу тролів, ботів, виробництва контенту й підробок, та публікують повідомлення мовами країн-цілей, атакуючи демократичні інституції. Використання підрядників дозволяє Кремлю уникати прозорості у фінансуванні (бюджети RT, наприклад, були відомі) та створювати ілюзію правдоподібного заперечення. Зливи персональної інформації цих організацій демонструють неймовірний масштаб і географію роботи. Ці організації досліджують суспільства-цілі, шукають точки розлому й підсилюють їх контентом. Уся ця діяльність пов’язана й скоординована напряму з Кремлем, а саме — з Сергієм Кирієнко, першим заступником керівника Адміністрації Президента РФ.

Таким чином, засадничі документи РФ свідчать, що аналітичний поділ на «кібероперації» та «інформаційні операції» не має жодного підґрунтя в російській доктрині. Методології виявлення, які розглядають координовану неавтентичну поведінку, маніпулювання наративами та технічні втручання як окремі явища, і надалі ігноруватимуть інтегрований характер російських операцій. По-друге, жоден окремий документ не може свідчити про повноту російських операцій. Неіснуюча «доктрина

Герасимова» або будь-який інший документ не може повноцінно охопити весь спектр російських інформаційних операцій, що спонукає розглядати цілий корпус документів, оглянутих вище. До того ж документи виокремлюють нерозривний зв'язок інформаційного протиборства та внутрішньої безпеки РФ, що може свідчити про збільшення інформаційних операцій онлайн у разі збільшення відчуття «небезпеки» російського режиму.

Однак варто зазначити, що військові доктрини та інші офіційні документи рідко є дороговказом для реальних операцій. Так, вони вказують на пріоритети та загальний рівень військово-політичної думки, але не обговорюють імплементацію стратегії в реальному світі, де є звичайні користувачі, алгоритми та опоненти. Таким чином, для того, щоб побачити як ці установчі документи стратегії інформаційних операцій втілюються на практиці, потрібно дослідити роботи виконавців цих операцій. У наступному розділі буде опрацьований масив опублікованих внутрішніх документів організацій SDA та Структура, які були опубліковані у афідевіті Федерального бюро розслідувань, у кількох журналістських матеріалах та проаналізовані дослідницькими центрами.

3.4 Документи АСД та Структури як практична реалізація стратегії

З квітня 2023 року в публічному доступі почали з'являтися фрагменти масиву внутрішніх документів російських підрядників у сфері інформаційних операцій, які слугували джерелами для розуміння практичної діяльності цих організацій. Це стало можливим завдяки публікації внутрішньої документації російських організацій-підрядників у кількох незалежних джерелах.

Першим джерелом є серія з чотирьох статей, які видання The Washington Post опублікувало протягом року. Матеріали готувала Кетрін Белтон спільно з колегами на основі масиву, що містив понад сотню внутрішніх російських документів. Журналісти стверджували, що отримали документи від «європейської розвідувальної служби». У статтях і документах розкривається період функціонування підрядних організацій з травня 2022 року по серпень 2023 року. Перша публікація від 21 квітня 2023 року

зосереджена на підривній діяльності російських організацій проти Німеччини (Belton et al., 2023). Цей матеріал не зазначав назву операції чи підрядників, але вказував на зв'язок з Сергієм Кірієнко, першим заступником керівника Адміністрації Президента РФ. Другий матеріал від 30 грудня 2023 року описував операції проти Франції (Belton, 2023), які передбачали зменшення підтримки України. Стаття посилалася на технічний звіт урядової організації VIGINUM (Viginum, 2023). Сам звіт VIGINUM та й стаття Washington Post почали вказувати на дві компанії «Група компаній структура» (Структура) та «Агенція соціального проєктування» (АСП) як головних підрядників для проведення інформаційних операцій. Наступна стаття від 16 лютого 2024 року висвітлювала роботу команди «Центр С» проти України (Belton et al., 2024a). Цей центр фактично існував на перетині АСП та Структури й працював виключно проти української аудиторії. У матеріалі журналістів з'явилися також приклади дешбордів підрядних організацій, які привідкривали завісу контенту та його кількісних показників. Фінальна ж публікація від 8 квітня 2024 року присвячена операціям, спрямованим проти Сполучених Штатів та їхній підтримці України (Belton and Menn, 2024). Статті у The Washington Post мають вагоме значення як перше публічне свідчення внутрішніх методів роботи Агентства соціального проєктування (АСП). Водночас, як стверджують Паммент і Цурцумія, ці матеріали відображали лише частину діяльності АСП і не дозволяли бачити ширшу архітектуру інформаційних операцій (Pamment and Tsurtsumia, 2025).

Другим джерелом є підтверджене під присягою письмове свідчення (афідевіт) Федерального бюро розслідувань (ФБР) США. Цей документ був опублікований у вересні 2024 року на підтримку арешту 32 інтернет-доменів, які використовувала кампанія «Двійник» (Doppelgänger). Цей монументальний документ містить свідчення агента ФБР, а також близько 190 сторінок додатків, які є оригінальними та перекладеними англійською внутрішніми документами Агентства соціального проєктування (АСП). Цей невідфільтрований набір документів є найважливішим окремим масивом першоджерел щодо цієї операції, який наявний у відкритому доступі. В афідевіті чітко зазначено, що АСП, «Структура» та інша компанія, АНО «Діалог»,

здійснювали свою діяльність під керівництвом і контролем Адміністрації Президента РФ, а саме вищезгаданого у матеріалах Washington Post першого заступника керівника Адміністрації Президента РФ Сергія Кирієнка. Документ був підписаний спеціальним агентом ФБР і є доказом у судовому процесі, що робить цю документацію надійнішою, ніж витоки в медіа. (Department of Justice, 2024a).

Третім джерелом є публікації у вересні 2024 року про витік даних європейським консорціумом журналістів, до якого входили видання з Німеччини, Польщі, України та інших європейських країн. Консорціум отримав від анонімного джерела масив даних, що налічував тисячі окремих файлів (Morozova and Laine, 2024). Це саме той масив, який Паммент і Цурцумія згодом отримали та детально проаналізували для звіту Шведського агентства психологічного захисту «За межами операції "Двійник": оцінка спроможностей Агентства соціального проєктування» (Pamment and Tsurtsumia 14–16).

Разом ці три джерела забезпечують можливість триангуляції та дослідження стратегії РФ крізь призму російських підрядників у сфері інформаційних операцій у воєнний час. Перш за все, ці документи слід розглядати як стратегічні свідчення діяльності РФ у інформаційному просторі. Серія публікацій The Washington Post, афідевіт ФБР та викриття європейського консорціуму, окремо один від одного, можуть сприйматися як описи окремих «інформаційних операцій». Проте, заважаючи на розглянуту вище доктринальну базу стратегії РФ в інформаційному просторі, ці документи розкривають, яким чином вона була імплементована в умовах воєнного часу 2022–2025 років.

Ці документи дозволяють переосмислити проблему системи та стратегії інформаційних операцій. У публічному дискурсі, що сформувався після першого викриття з боку компанії Meta та тривав до вересня 2024 року, коли було опубліковано афідевіт, поняття «двійник» («Doppelgänger») функціонувало як синонім усього комплексу діяльності Агентства соціального проєктування (АСП, SDA – англ.) та компанії «Структура». Причиною цьому стало те, що дослідники-аналітики, фактчекери та групи з автентичності платформ фокусували свої дослідження на інфраструктурі

дзеркальних сайтів. Це було цікавою тактикою, але ці дослідження були ізольованими прикладами даних, які не мали доказів стратегічного рівня (Pamment and Tsurtsumia, 2025, с.15) й не бачили весь масив стратегічної імплементації.

Внутрішні документи АСП не використовували термін «двійник» («Doppelgänger»), адже вони структурували свою діяльність за допомогою іншої термінології та проєктів. Основними проєктами у внутрішніх документах є «Міжнародна комплексна контркампанія» та «Європейська комплексна контркампанія», яка стала головним європейським проєктом з 2023 року. У масиві документів є також проєкти «Українська комплексна контркампанія» та «Інша Україна / Справжня Україна», який будувався навколо Віктора Медведчука, а також низка менших операцій, спрямованих на конкретні країни (Pamment and Tsurtsumia, 2025, с.58–116).

Дзеркальні сайти, які були ідентифіковані спільнотою з протидії FIMI як операція «Двійник», у документах АСП виступають лише одним із кількох інструментів доставки контенту в межах зазначених контркампаній. Таким чином, підвищена увага саме до цього єдиного методу поширення дезінформації є помилковою, адже вона ігнорує цілий спектр підходів. У той же час російські підрядники використовують концепцію контркампанії, натякаючи на природу стратегії інформаційних операцій. У внутрішніх документах SDA описує свою роботу як протидію західній інформаційній агресії, а не як пропаганду чи інформаційну операцію. Ця дивна інверсія є вираженням стратегії, що проявлялася у Доктринах інформаційної безпеки 2000 та 2016 років, Стратегії національної безпеки 2021 року та Концепції зовнішньої політики 2023 року. Таким чином, російська стратегія інформаційних операцій навіть у внутрішніх документах позиціонується як оборонна протидія.

Центральна ідея цього підрозділу та практичної частини дисертації полягає в тому, що оприлюднені документи розкривають реалізацію стратегічної доктрини. Так, організації підрядників стали настільки включеними в реалізацію стратегії, що під час широкомасштабного вторгнення та виконання державного підряду вибудовують навколо неї власну внутрішню звітність.

Усі джерела, що проливають світло на документацію підрядників, вказують на однакову структуру командування. В афідевіті головним посадовцем-куратором мережі названо Кирієнка Сергія, першого заступника керівника Адміністрації Президента РФ. Він перебуває під санкціями OFAC й в офіційному роз'ясненні Міністерства фінансів США описується як «куратор внутрішньої політики Путіна» (U.S. Department of the Treasury, 2022). Оприлюднені протоколи зустрічей дозволили дослідникам ідентифікувати ще кількох осіб, що керують роботою підрядників від Адміністрації Президента РФ (Pamment and Tsurtsumia 41–46).

Головними виконавцями виступають дві організації — «Агентство соціального проєктування» (АСП) і група компаній «Національні Технології Структура» (Струкура). Агентство управляється політтехнологом Іллею Гамбашидзе, а Структура знаходиться під керівництвом Миколи Тупікіна. Ці дві юридичні особи-підрядники становлять операційне ядро цієї мережі інформаційних операцій. У підтвердження цього та важливості цих організацій у структурі російської пропаганди, Європейський Союз запровадив санкції проти цих організацій та їхніх керівників (European Commission, 2023). У березні 2024 року це зробило і Міністерство фінансів США (United States Department of State, 2024).

Незважаючи на формальний поділ, АСП та Структура не є "чужими" структурами. Фінансові документи та списки співробітників у оприлюднених матеріалах показують, що вони працюють як єдина організація (Pamment and Tsurtsumia, 2025, с.46–49). Внутрішній розподіл роботи має суто функціональний характер. АСП займається створенням контенту, розробкою наративів, соціологічним та політичним аналізом країн-цілей, а також взаємодією з інфлюенсерами. «Структура» забезпечує підтримку операцій на технічному рівні. Тобто вони займаються реєстрацією доменів, закупівлею реклами та управлінням мережею ботів у соцмережах. В афідевіті згадуються дві окремі команди. А саме, «Команда І», яка зосереджена на міжнародних кампаніях, і «Центр С». Останній є спільною групою з представників АСП і «Структури», що працює над українською «контркампанією» (Department of Justice, 2024a).

Ці витоки також документують екосистему автономних некомерційних організацій (АНО), які функціонують як організаційна оболонка для суміжної діяльності. Трьома найбільш значущими організаціями є АНО «Діалог» та її регіональна дочірня структура АНО «Діалог Регіони». Офіційно вони спеціалізуються на проєктах у сфері цифрових публічних комунікацій, проте на практиці функціонують і як інструмент управління внутрішніми російськими наративами. Третьою організацією є АНО «Інститут розвитку інтернету» (IPI), відповідальна за державне фінансування онлайн-контенту. Ця організація, хоч і не була названа напряму, але за свідченням Паммента та Цурцумії (2025) була ключовою у впливі на Латинську Америку. Цю операцію Центр глобальної взаємодії (GEC) описав у своєму звіті у листопаді 2023 року. (United States Department of State, 2023).

Річний бюджет цієї системи пропаганди оцінюється у 600 мільйонів євро (Pamment and Tsurtsumia, 2025, с.19). Це фінансування охоплює організації приватного та некомерційного секторів. У той же час бюджет трьох найбільших пропагандистських медіа (RT, ВГТРК і Росія Сьогодні) у 2023 році склав понад 800 мільйонів доларів (Debunk.org, 2023). Тобто, на операції онлайн Кремль витрачає майже стільки ж, скільки на ТБ та медіа як всередині, так і назовні країни. Ці фінансові дані документують зміну пріоритетів Кремля після 2022 року. А саме переведення фінансування пропаганди з традиційних інструментів державних медіа на користь приватизованої екосистеми гнучких підрядників, чий зв'язок із державою можна правдоподібно заперечити.

У витоку даних вказані кілька окремих операцій, які утворюють операційне портфоліо мережі АСД та «Структура». Кожну з операцій слід розглядати як конкретну реалізацію певної стратегічної цілі у конкретному театрі дій. Далі буде розглянуто кілька кампаній, які націлені на Європу та Україну.

З середини 2023 року росіяни розгорнули профільну кампанію, зосереджену на майбутніх виборах до Європейського парламенту. Стратегічна мета цієї кампанії полягала в тому, щоб змусити понад половину громадян Німеччини «не хотіти жертвувати своїм благополуччям заради перемоги над Росією». Це формулювання

встановлює чітку вимірювану ціль для кампаній. Додатковою ж метою операції був підрив європейської підтримки України.

В межах цієї кампанії простежувалися кілька аспектів, які можна ідентифікувати у витоках даних. По-перше, напрям впливу на вибори. АСП сфокусувалися на явній підтримці ультраправих та євроскептичних партій, від яких очікували високих результатів на європейських виборах 2024 року. Інформаційні операції мали на меті підвищити електоральні рейтинги «Альтернативи для Німеччини» (AfD) та французького «Національного об'єднання» ставлячи за ціль 20% голосів для AfD (Morozova and Laine, 2024). Другий аспект — це теми, на які спрямовували свої зусилля пропагандисти. Вони використовували кілька головних наративів: 1) санкції проти Росії шкодять європейцям більше, ніж самій Росії; 2) Україна є корумпованою та не варта отримання європейських ресурсів, тощо. Тобто, вони намагались підірвати підтримку України та зірвати запровадження санкцій проти РФ. Фінальний аспект — це способи донесення та обсяги контенту. Один з проєктів АСП визначав квоти на виробництво контенту, а за 4 місяці 2024 року оператори АСП та Структури згенерували 33,9 мільйона коментарів (Morozova and Laine, 2024).

Українська контр-кампанія є найбільш операційно амбітною в усьому портфоліо, до якої здебільшого залучена підгрупа «Центр С». Стратегічних цілей у цієї кампанії було 4: 1) підірвати довіру до Президента Володимира Зеленського та військово-політичного керівництва воюючої України; 2) деморалізувати Збройні Сили України; 3) Дезорганізувати цивільне населення, на яке вони спираються; 4) розколоти політичні еліти (Department of Justice, 2024a).

Ця кампанія методологічно відрізняється від європейських зустрічних кампаній, адже використовує попередні знання про українське суспільство та тривалі довоєнні інвестиції у російськомовний український медіапростір (значна частина якого була пов'язана з телевізійними активами Медведчука до 2021 року). У цьому розумінні українська «контр-кампанія» є такою, де АСП володіє найглибшими компетенціями щодо суспільства-цілі. Афідевіт також демонструє обсяги створеного контенту,

включаючи коментарі, відео та меми, що поширювалися на різних платформах. Це свідчить про широкий спектр методів, використаних АСП і Структурою.

Важливою частиною цих операцій було те, як саме будувалася робота організацій, які впливали на велику кількість країн та цільових аудиторій. Організаційно, діяльність АСП складалася з чотирьох стовпів – моніторингу, аналітики, виробництва та розповсюдження

Моніторинговий рівень АСП спирається на дашборди, які генерують великі обсяги звітів про моніторинг медіа. Моніторингова група АСП відстежує понад тисячу конкретних лідерів думок як у проросійському, так і в антиросійському дискурсах. До того ж моніторинг контенту охоплює основні західноєвропейські мови, а також російські та українські інформаційні простори та медіа в них (Pamment and Tsurtsumia 126–142; Department of Justice, 2024a). В українському просторі вони відстежують сентимент в коментарях, основні віральні теми, та основні публікації медіа. Ця звітність є значною за обсягом, але досить поверхневою за суттю. Вона орієнтується радше на здивування замовника, а не на розуміння цільової аудиторії.

Другий рівень, аналітичний, поєднує в собі медіаметрики (покази та реакції) із соціологічними дослідженнями. Останні включають опитування громадської думки та експертні панелі. Незважаючи на поверхневу складність та витонченість, інструменти не є ідеальними. Скоріше за все вони репрезентують глибину зусиль для замовників (Кремля), радше ніж дають чітке розуміння успішності операцій, окрім як наочних цифр переглядів специфічних публікацій.

Третій рівень (креатив та контент) є напрямом, де АСП працює найкраще й продукує неймовірну кількість контенту. У витоках підрозділу «Центр С» можна побачити план з «виробництва» сотень публікацій різного формату від відеороликів та мемів до коротких публікацій та коментарів. За даними журналістів, у період із січня по квітень 2024 року АСП та Структура створили 39 899 «одиниць контенту», з яких 4641 — це відеоролики, а 2 516 — меми та графічні елементи. (Department of Justice, 2024a;

Morozova and Laine, 2024). Такий промисловий масштаб демонструє наявність серйозної інфраструктури, здатної виробляти великі об'єми контенту.

Особливої уваги заслуговують дві операційні характеристики виробництва. По-перше, виробництво чітко регульоване за кількістю й типами продукції. У документах з витоку визначено точну кількість коментарів, мемів та відео, які мають бути створені протягом кожного циклу кампанії. По-друге, темпи реалізації й створення є надзвичайно швидкими, адже навіть у проаналізованому наборі даних була реклама, що обговорювала події всередині України не пізніше ніж через 48 годин після того, як ці події сталися. Така комбінація швидкості й об'єму призводить до реалізації військової стратегії інформаційних операцій та чітко відповідає моделі «потоку брехні».

Рівень доставки контенту є найрізноманітнішим та технічно просунутим, що саме й привернуло увагу багатьох дослідників до витоків даних. В цілому, доставку контенту можна розділити на кілька важливих частин. На першому рівні мережа використовує інструменти платного просування, а саме рекламу на платформі Facebook. На цьому ж рівні застосовується генерація коментарів і підсилення потрібного контенту ботами. Оскільки більшість контенту буде видалено досить швидко, система розповсюдження робить ставку на точкове потрапляння в стрічку якомога більшої кількості людей. Таким чином, використання реклами з широкими фільтрами цільової аудиторії дозволяє досягати широкого кола користувачів. А паразитування на відомих каналах та сторінках, під якими тролі й боти залишають коментарі, дає надію на додатковий контакт з аудиторією. Оскільки постійне й стабільне переконання в такій системі неможливе, АСП та Структура намагаються радше підтримувати «інформаційне тло», в якому поступово нормалізуються російські наративи.

На другому рівні мережа використовує дзеркальні сайти провідних видань країн-цілей з географічним фільтруванням (традиційний підхід операції «Двійник»), сайтів бренду Reliable Recent News й інфраструктуру, яка підтримує ці сайти. Ці вебсайти працюють на окремі аудиторії. Так, клони клони авторитетних медіа можуть спрацювати для широкого загалу, використовуючи авторитет цих видань. У свою чергу

альтернативні медіа направлені на користувачів, які не довіряють офіційним ЗМІ. Таким чином, оператори інформаційних операцій можуть впливати на ширше коло користувачів.

Фінальний і найбажаніший рівень всіх інформаційних операцій — це підсилення наративів і підробок політиками, інфлюенсерами та авторитетними медіа. Коли повідомлення підхоплює обліковий запис з сотнями тисяч підписників – це створює рівень розповсюдження, який недоступний більшості облікових записів та сайтів АСП та Структури. Причому, що парадоксально, в своїх документах АСП та Структура збирають згадки й розслідування про себе у звітах організацій, що протидіють інформаційним операціям, і використовують їх як підтвердження успіху (Department of Justice, 2024a). Частковим поясненням цього парадоксу може слугувати те, що стратегія не тільки у тому, щоб розповсюджувати різні наративи, а й у тому, щоб підтримувати образ «всемогутності» російської інформаційної машини впливу на демократії. Таким чином, чим більше матеріалів про АСП та Структуру, тим більше враження, що РФ є грізним суперником.

Зіставляючи доктринальні джерела з попереднього підрозділу та витік документів АСП, можна побачити, яким чином інформаційні операції в межах доктрини «інформаційного протиборства» реалізуються під час повномасштабного вторгнення. По-перше, інформаційні операції, які атакують інші країни, отримали фрейм захисту. Цей підхід чітко простежується як ознака кожного стратегічного документу Росії й відтворюється у внутрішньому організаційному лексиконі АСП, бо кампанії визначаються як «контркампанії» навіть у внутрішніх звітах. Це свідчить про доктринальну узгодженість на рівні операційної культури та про єдину стратегію.

По-друге, перманентне протистояння в рамках «інформаційного протиборства», яке згадано у доктринальних документах, на рівні АСП реалізується у вигляді моделі безперервного виробництва. Фактично, безперервне виробництво контенту операторами АСП та Структури є постійним і підтримує рівень протистояння «проти всіх» із загальними магістральними цілями.

По-третє, традиція рефлексивного управління операційно виражається в архітектурі доставки контенту АСП та в управлінні когнітивним середовищем цільових аудиторій. Мережа АСП та Структури займається конструюванням інтерпретації певних подій, у межах яких цільові аудиторії ухвалюють рішення, що сумісні з російськими інтересами. Наприклад, цілі по дискредитації України за кордоном намагаються вплинути на сприйняття країни, сформувавши інформаційне тло, на фоні якого думка про припинення допомоги Україні буде логічною.

По-четверте, загальносуспільний підхід до «захисту», адже РФ у своїх доктринальних документах розглядає інформаційне протиборство як наскрізну відповідальність держави загалом. Підрядна модель SDA реалізує цю доктрину у формі єдиної екосистеми, що поєднує функції, розподілені між рекламним агентством, політичною консалтинговою фірмою, соціологічною компанією, медіаструктурою та спецслужбою. Інтеграція цих кількох рівнів в рамках однієї організації, де «реклама перетинається зі шпигунством та інформаційною війною» (Pamment and Tsurtsumia, 2025, с. 185) ілюструє аналітичний виклик, адже інтеграція різних за своїм характером організацій і є новою стратегією російських інформаційних операцій.

Саме тому вивчення матеріалів операцій АСП є важливим академічним та практичним завданням дослідників російських інформаційних операцій. Розуміння практик таких організацій дозволить реконструювати ширшу стратегію інформаційних операцій РФ, яка на рівні стратегій і доктрин не є конкретною та відкритою для розуміння. Операції АСП та Структури не є повним спектром інформаційних операцій РФ, проте дозволяють зрозуміти вектор розвитку інформаційної машини РФ, яка має багату історію «активних заходів» та інформаційних операцій з метою впливу на інші країни.

РОЗДІЛ 4

АНАЛІЗ СУЧАСНИХ РОСІЙСЬКИХ ОПЕРАЦІЙ ВПЛИВУ В УКРАЇНІ ТА КРАЇНАХ ЗАХОДУ

Сучасна інформаційна війна відбувається переважно в інформаційному просторі — сфері суперництва, яка охоплює соціальні мережі, традиційні та цифрові медіа. Однак такі операції інформаційного впливу не обов'язково супроводжуються відкритими деклараціями чи видимою агресією, що, у свою чергу, ускладнює їхнє атрибутування та протидію.

Російські кампанії та документи останніх двох десятиліть доводять, що сучасна інформаційна війна є комплексом різних дій, які включають психологічні операції, кібератаки та заходи впливу, спрямовані на маніпулювання думкою громадян, дестабілізацію суспільств і підрив демократій. Росія застосовує власні державні потужності разом з недержавними акторами, які нерідко діють на контрактній основі як підрядники для проведення операцій впливу. Вони експлуатують цифрові екосистеми, використовуючи автоматизовані облікові записи, тролів та ботоферми для маніпулювання наративами та сіяння розбрату (Zannettou et al., 2019; Starbird et al., 2019).

Повномасштабне вторгнення Росії в Україну у 2022 році додатково продемонструвало важливість дезінформації та інформаційних операцій як невід'ємних і взаємодоповнювальних компонентів кінетичної війни. Наприклад, напередодні вторгнення розгорнулася масова кампанія наративів «під фальшивим прапором», покликаних виправдати агресію та сфабрикувати *casus belli* (Gigitashvili and Osadchuk, 2022). А саме, російські державні ЗМІ поширювали твердження про підготовку України до нападу на Донбас, фабрикували заяви про підготовку хімічних атак та інші безпідставні провокації, розроблені для легітимізації вторгнення.

Як продемонстрував аналіз доктринальних документів та внутрішніх документів підрядників у попередніх підрозділах, в умовах російсько-української війни інформаційний аспект залишається ключовим у стратегії Москви. Російські державні та

проксі-актори діють у кількох напрямках. По-перше, вони намагаються впливати на поведінку українського суспільства, підриваючи моральний дух людей, руйнуючи довіру до керівництва країни та заохочуючи українську капітуляцію. Водночас, вони спрямовані на вплив щодо прийняття рішень міжнародними партнерами України. Застосовуючи скоординовані кампанії впливу проти західних аудиторій, Росія прагне підірвати політичну та соціальну згуртованість союзників України і знеохотити їх від продовження військової та гуманітарної підтримки. Ці операції ілюструють використання Росією інформаційних операцій як важливої складової ведення бойових дій.

Цей розділ фокусується на трьох кейс-стаді, які детально розглядають імплементацію стратегії російських інформаційних операцій у різних форматах та на кількох платформах соціальних мереж. Всі кейс-стаді є в рамках досліджень, які проводились не тільки автором, проте кожне з них висвітлює унікальний аспект операцій чи їх підмножину, що стосувались діяльності АСП та Структури, а також Центру С, описаних у підрозділі 3.4. Зібрані автором дисертаційного дослідження дані охоплюють публікації, включно з їх метаданими та характеристиками залученості на кількох платформах. Ця інформація для визначення виявлених операцій до стратегії РФ, описаної у підрозділах 3.3 та 3.4. Триангуляція підмножини практичних операцій з наявною документацією РФ дозволяє порівняти практичну реалізацію із задокументованою стратегією росіян до інформаційних операцій та, з різним рівнем впевненості атрибутувати реальні приклади до підрядників, які стоять за цими операціями. Насамкінець, у цьому розділі концептуалізуються можливі зв’язки між російськими кампаніями та дезінформаційними операціями, які не мають очевидного зв’язку.

Кейси відбиралися за двома основними критеріями: для демонстрації новизни тактик та для висвітлення перехресних доказів, що вказують на збіг акторів або координацію між кампаніями. Хоча витоки російських документів, результати журналістських розслідувань та інформація з афідевітів Міністерства юстиції США

підтверджують залученість взаємопов'язаних суб'єктів до цих кампаній, вони рідко розкривають характер взаємодії між окремими операціями впливу на рівні реалізації. Як наслідок, у дослідницькому середовищі такі операції та їхні учасники часто розглядаються як ізольовані елементи, що не є коректним, враховуючи внутрішні документи Структури та АСП.

Аналіз кожного кейсу в цій частині дослідження структурований у кілька складових для забезпечення систематичного та порівняльного вивчення кампаній. Перша частина кожного кейсу оцінює контекст, окреслюючи походження, хронологію та обставини кампанії, які її супроводжують. Цей підрозділ кожного кейсу формується із зовнішніх джерел. У цій частині також розглядаються цифрові платформи, що використовувалися для поширення. Цей розділ також демонструє як пов'язані з Росією зловмисні актори модифікували свої методи у відповідь на видалення з платформ, санкції та посилення виявлення, якщо це можливо.

Друга частина кожного кейс-стаді зосереджується на аналізі унікального набору даних для кожного прикладу. Ці набори даних були зібрані автором та проаналізовані для синтезу основних повідомлень і наративів, дедукції поведінки акторів, виділення патернів і характеристик облікових записів, які використовувалися у кампаніях.

Наприкінці розділу результати знахідок у всіх трьох кейсах співставляються із доступними оприлюдненими документами та між собою для виділення схожих патернів поведінки і повідомлень у спробі з'єднати ці різні кампанії як частину єдиного цілого, а саме стратегії РФ, синтезованої на основі документів Структури та АСП. Атрибуція до стратегії РФ оцінюватиметься через співпадіння у цілях, задекларованих у документах, через схожі поведінкові та інфраструктурні патерни, а також співпадіння наративів. Для підтвердження зв'язку з РФ використовуються офіційні звіти прозорості платформ соціальних мереж, розслідування урядових та неурядових організацій, а також внутрішні документи АСП, які демонструють оперативне планування та ключові меседжі.

Дослідження надає детальний аналіз лише трьох інформаційних кампаній як репрезентації частини зусиль РФ у цій сфері. Проте масштаб дезінформаційних зусиль Росії виходить далеко за межі обраних кейсів і методів впливу. По-перше, у цій практичній частині не аналізується діяльність традиційних медіа. По-друге, це дослідження не включає російські інформаційні операції у країнах Глобального Півдня, де вони адаптують свої інформаційні зусилля та наративи до специфіки регіону (DFRLab, 2024). Це виключення є необхідним заходом для демонстрації детальних зусиль на невеликій вибірці матеріалів для реконструкції стратегії інформаційних операцій РФ проти України та її союзників. До того ж методи протидії дезінформації в демократіях Заходу та в країнах так званого Глобального Півдня можуть відрізнятися через різні інституційні та історичні передумови.

4.1 Операція «Двійник» (Doppelganger)

4.1.1 Контекст операції «Двійник»

Операція «Двійник» (Operation Doppelganger, OD) є однією з найбільш масштабних російських операцій впливу, виявлених у Європі після початку повномасштабного вторгнення в Україну. Кампанію, яка охопила кілька європейських країн, зокрема Україну, Францію, Німеччину та Італію, приписують афілійованим з державою російським акторам (АСП та Структура). Стратегічна мета операції загалом полягала в підриві підтримки України Заходом шляхом зображення України як «держави, що не відбулася, корумпованої і нацистської» (Alaphilippe et al., 2022). Операція поширювала інформацію про «катастрофічні» наслідки санкцій проти Росії, а також підсилювала внутрішні дискусії та проблеми задля переконання в тому, що ці проблеми важливіші, ніж допомога Україні. Кампанію вперше виявили у серпні 2022 року представники EU DisinfoLab, DFRLab та корпорації Meta (DFRLab, 2022a; Nimmo and Torrey, 2022; DFRLab, 2022c). Операція «Двійник» стала показовим прикладом еволюції дезінформаційних тактик Росії у відповідь на заборони RT і Sputnik у Європейському Союзі, запроваджені раніше того ж року.

Кампанія в основному відома через те, що вона використовувала клоновані веб-сайти, що імітували легітимні авторитетні медіа в країнах-цілях. На початковому етапі операція також включала ідентичні неавтентичні сторінки у соціальних мережах, що копіювали логотипи відомих видань. Операція застосовувала подібні до легітимних домени, які мали незначні зміни у доменах верхнього рівня (наприклад, unian[.]pm замість unian[.]ua). Ці вебсайти були абсолютними копіями оригіналів, які навіть зберігали імена реальних журналістів. Однак публіковані на них статті містили хибну, упереджену або сфабриковану інформацію, критичну щодо України або Заходу, яка ніколи не з'являлася в оригінальних виданнях (Alaphilippe et. al, 2022). Операція «Двійник» також активно використовувала для розповсюдження платну рекламу у Facebook. Зміст цих рекламних матеріалів нерідко мав песимістичний, спотворений або сенсаційний характер, а також містив скандальні твердження на кшталт звинувачень Збройних Сил України у «вбивстві дітей».

Операція «Двійник» була якісним переходом від звичайного підсилення повідомлень з використанням ботів до механізмів платного просування. Агенти АСП використовували рекламу у Facebook для того, щоб обійти традиційне нарощування підписників. Натомість вони купували охоплення через рекламну інфраструктуру платформи, фактично перетворюючи інструменти Meta на метод поширення дезінформації. Хоча представники платформи Meta оперативно видаляють значну кількість цих облікових записів і рекламних матеріалів, деякі з них встигають набрати значне охоплення. Так, згідно з європейськими дослідниками, окремі оголошення зібрали десятки тисяч переглядів до видалення (Alaphilippe et al., 2022).

Кампанія також поширилася на платформі Twitter/X, де була застосована тактика розповсюдження посилань через коментарі. Ці акаунти відповідали на публікації популярних акаунтів або цитували початкові публікації інших ботоподібних акаунтів. Контент таких публікацій являв собою наративи, узгоджені з позицією Кремля, які оператори АСП намагалися просунути у мейнстрім (Nimmo and Torrey, 2022). Використовуючи можливості верифікації акаунтів на платформі, АСП просувала

відповіді своїх акаунтів вище за відповіді інших. Цей перехід відображає якісну адаптацію росіян до вразливостей платформи, що виникли після зміни власника Twitter/X.

Зображення та тексти в рекламі операції «Двійник» були провокаційними, щоб підштовхнути до переходу за посиланням і прочитати більше на сфальшованому сайті. На цих сайтах, окрім карикатур або зманіпульованих портретів провідних європейських політиків, були критичні тексти щодо політики чи рішень цих посадових осіб. Зважаючи на те, що блог був на відомому сайті, це мало заохотити користувачів повірити у матеріал (Châtelet and Osadchuk, 2024). Операція «Двійник» демонструє розвиток «активних заходів» та імплементацію нової стратегії через рекламні технології, що поєднують обман і імперсонацію. Ці підходи демонструють якісний перехід від відкритої пропаганди до прихованих маніпуляцій інфраструктурою платформ.

Операція «Двійник» також набула значного розголосу та публічного висвітлення після масштабних розслідувань у медіа в Європі та США наприкінці 2022 року. Звіти медіавидань, Meta та аналітичних центрів привернули безпрецедентну увагу до мережі. У відповідь на цей тиск оператори кампанії були змушені адаптувати технічну інфраструктуру з метою уникнення виявлення - ще одна деталь у підході Росії до підтримки правдоподібного заперечення та оперативної стійкості.

Починаючи з 2023 року автор з іншими колегами зафіксували, що веб-сайти, пов’язані з «Двійником», мігрували на нову цифрову інфраструктуру. Вони почали використовувати Keitaro - комерційну платформу управління трафіком, що зазвичай застосовується в онлайн-маркетингу, однак тут використовувалась для прихованого таргетування (Qurium Media Foundation, 2022). Це оновлення дозволило учасникам операції сортувати та фільтрувати користувачів за географічним розташуванням на підставі IP-адреси. Як наслідок, користувачі Facebook, яким демонструвалася спонсорована реклама «Двійника», перенаправлялись на підроблені статті ЗМІ лише в тому разі, якщо їхні IP-адреси відповідали цільовій країні. Натомість користувачі, які намагалися відвідати ті самі URL-адреси з інших регіонів, отримували або порожню

сторінку, або сторінки із беззмістовним текстом-заповнювачем (Châtelet and Osadchuk, 2024).

До 2024 року учасники операції «Двійник» додатково вдосконалили її технічні можливості, щоб уникнути виявлення. Ампліфіковані операцією вебсайти почали включати гнучкі системи, здатні виявляти не лише аномалії й невідповідності IP-адрес. Вони почали ідентифікувати автоматизоване сканування, таке як архівування або спроби аналізу, ускладнюючи роботу дослідників. Коли дослідники або фахівці з відкритих джерел застосовували інструменти архівування на кшталт Wayback Machine і намагалися отримати доступ до клонованих доменів, система негайно перенаправляла зміст сайту на повну копію легітимного авторитетного місцевого видання, замінюючи сфабриковану статтю. Ці новації призвели до кількох наслідків. По-перше, це ускладнило проведення розслідувань дослідниками, бо стало складніше архівувати первинні матеріали задля документації доказів. По-друге, це додало підвищеної уваги до операції, адже ця надбудова до технічних можливостей привернула ще більшу увагу медіа та держаЗважаючи на те, що АСП збирали про себе матеріали у західних виданнях, це могло працювати на користь пропагандистів і їхньої стратегії. Загалом ці результати підтверджують, що АСП функціонувала як гібридний актор, який поєднував технічні підходи до поширення контенту зі стратегічними цілями Кремля. Ця співпраця є прикладом ширшої стратегії в рамках гібридних операцій Росії, коли номінально приватні компанії виконують політично вмотивовану роботу з впливу від імені державних замовників (як це відбувалося з ПВК «Вагнер»), підсилюючи правдоподібне заперечення для Москви щодо свого глобального пропагандистського охоплення.

4.1.2 Дослідження архіву реклами операції «Двійник»

У 2023-2024 роках операція «Двійник» була в активній фазі в Україні та країнах Європи, використовуючи рекламу на платформах Meta як основу для своєї дистрибуції. Протягом січня-липня 2024 року автором було зібрано унікальний масив рекламних публікацій цієї російської операції. Унікальним цей набір робить те, що Meta видаляла

повідомлення, коли знаходила рекламу, яку запускали росіяни. Однак, у випадку реклами на території ЄС — ця реклама зберігалася у бібліотеці реклами Meta, й вона доступна й досі. У випадку з Україною та іншими країнами — така реклама зникала з платформи, як й будь-які сліди її існування. Таким чином, цей архів, який збирався протягом 6 місяців у 2024 році, є унікальним свідченням, яке ніде не оприлюднювалося, й лише окремі реклами могли з'являтися у деяких дослідженнях, незалежно від автора.

Цей масив скриншотів включає не тільки рекламні повідомлення, а й скриншоти сторінок, які їх розповсюджували, та розділ Facebook, який називається «прозорість сторінки», який надає дані про дату створення сторінки тощо. Деякі рекламні повідомлення мають лише частковий набір цих частин через швидке видалення з платформи. Тобто, наприклад, деякі сторінки матимуть лише скриншот публікації на сторінці, інформацію про сторінку, але не реклами на платформі Meta Ads, адже остання вже була видалена.

Першим кроком у обробці цих напівструктурованих даних було їх сортування за унікальними прикладами реклами та сторінок. Цей крок дозволив згрупувати 649 зображень (скриншотів) у 251 групу за унікальними назвами сторінок, що містяться у масиві (у Додатку 2 є посилання на весь масив). Остаточний набір даних складається з 251 унікальної сторінки, кожна з яких запускала як мінімум одне рекламне повідомлення, й кількох зображень для кожної з них. Усі файли масиву даних було перейменовано за назвами сторінок у Facebook, щоб спростити навігацію та виділити патерни назв.

Наступним кроком ці сторінки було класифіковано за основним «стратегічним» повідомленням, яке об'єднує ці зображення й повідомлення. Загалом було виділено 7 парасолькових груп, які включали різні схожі повідомлення. Таким чином, кожна Facebook-сторінка була віднесена до наративної групи, яка є найближчою до рекламного повідомлення, яке ця сторінка розповсюджувала. Слід зазначити, що деякі рекламні повідомлення могли увійти у більше ніж 1 групу, але вони були включені лише до однієї з наративних груп, щоб уникнути дуплікації. В цілому, всі повідомлення можна

розділити на такі категорії: 1) анти-мобілізаційні повідомлення; 2) корупція; 3) неминучий програш у війні чи втома українців від війни; 4) зрада України країнами Заходу та НАТО; 5) наративи проти діаспори чи біженців; 6) економічний колапс України; 7) повідомлення, які атакують Президента Зеленського чи уряд.

Анти-мобілізаційна група наративів є найбільшим кластером у наборі даних. Він охоплює 89 сторінок і 230 файлів, що становить приблизно 35% загального обсягу унікальних сторінок. Присутність цієї групи відображає стратегічний пріоритет операції «Двійник», що співпадає із внутрішніми документами АСП, тобто дискредитація ЗСУ та, як наслідок, підрив оборонної спроможності України. Ця група намагалася дискредитувати мобілізаційні процеси, створюючи образ того, що справедливої мобілізації немає, та лякала тим, що це незворотний та безальтернативний негативний процес. Контент у цій групі фокусувався на кількох окремих темах. По-перше, на негативному зображенні територіальних центрів комплектації та соціальної підтримки (надалі - ТЦК) та їхньої роботи. Наприклад, контент операції демонстрував фото, на яких військовослужбовці у формі фізично заштовхують чоловіків до транспортних засобів. По-друге, зманіпульована статистика втрат України у війні та час виживання новобранців, що мало на меті залякування новобранців і спонукати потенційних рекрутів до відмови від вступу на службу. Сюди ж можна включити прямі заклики до уникнення служби. По-третє, повідомлення подавали «свідчення» від фіктивних персон, які описують страждання на передовій, а саме умови перебування. Фінальною підгрупою були економічні повідомлення, які пов’язували мобілізацію з фінансовим руйнуванням родини.

Ця група також включала такі повідомлення, як: «Забирають навіть будівельників фортифікацій» (акаунт *AdelaidaVernadskaia*), «В окопи відправляють навіть інвалідів» (*AdrianaAleksutina*), «Сховатись від мобілізації не вдасться» (*Best Flowers AKT*), «Демобілізації не буде, лише труна» (*Fashion QDI*) тощо. Таким чином, поступово підсилювались негативні настрої щодо ТЦК та заходів загальної мобілізації.

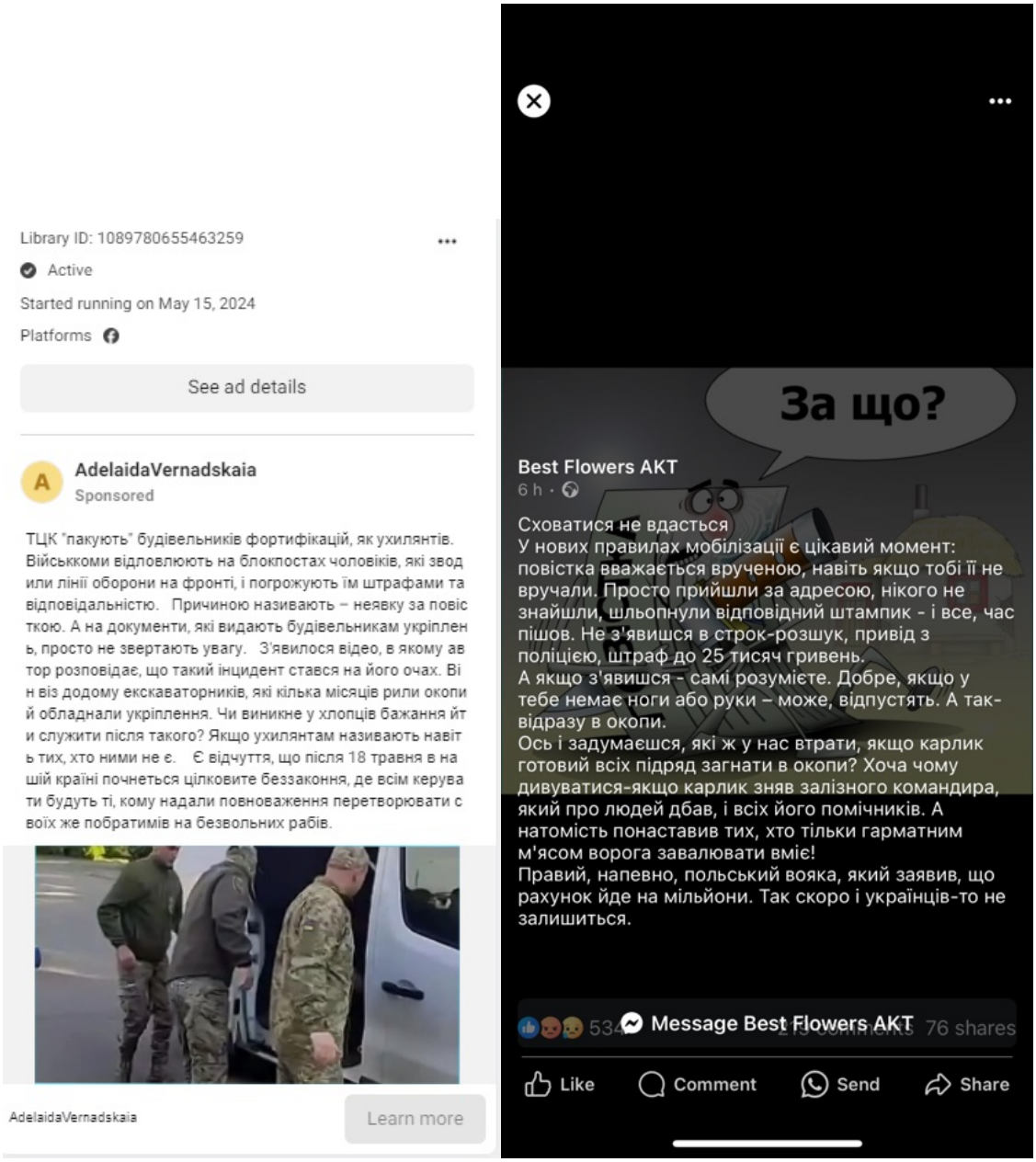


Рисунок 4.1. Скриншоти рекламної публікації сторінки *AdelaidaVernadskaia_2* (зліва) та публікації *Best Flowers AKT_3* (справа) (Джерело: власний архів)

Як можна побачити із зображень на Рисунку 4.1, повідомлення використовують короткий негативний текст, який фреймує реальність як безвихідь, де навіть люди з документами не можуть уникнути «несправедливої мобілізації». Що характерно, повідомлення використовують різні візуальні стилі для привернення уваги. Зокрема, зображення зліва демонструє скриншот, який виглядає як кадр з відео, імпліцитно натякаючи на процес мобілізації. Інше ж зображення використовує ілюстрацію із

зображенням повістки (*Best Flowers AKT*). Окрім цього, перше рекламне повідомлення має помилки в тексті, а саме - використання пробілів для розривання слів, як «повістка». Такий метод підготовки контенту використовувався, ймовірно, для того, щоб уникнути блокування за ключовими словами, які використовують платформи, а також детекції дослідниками, які використовують ключові слова для пошуку реклам.

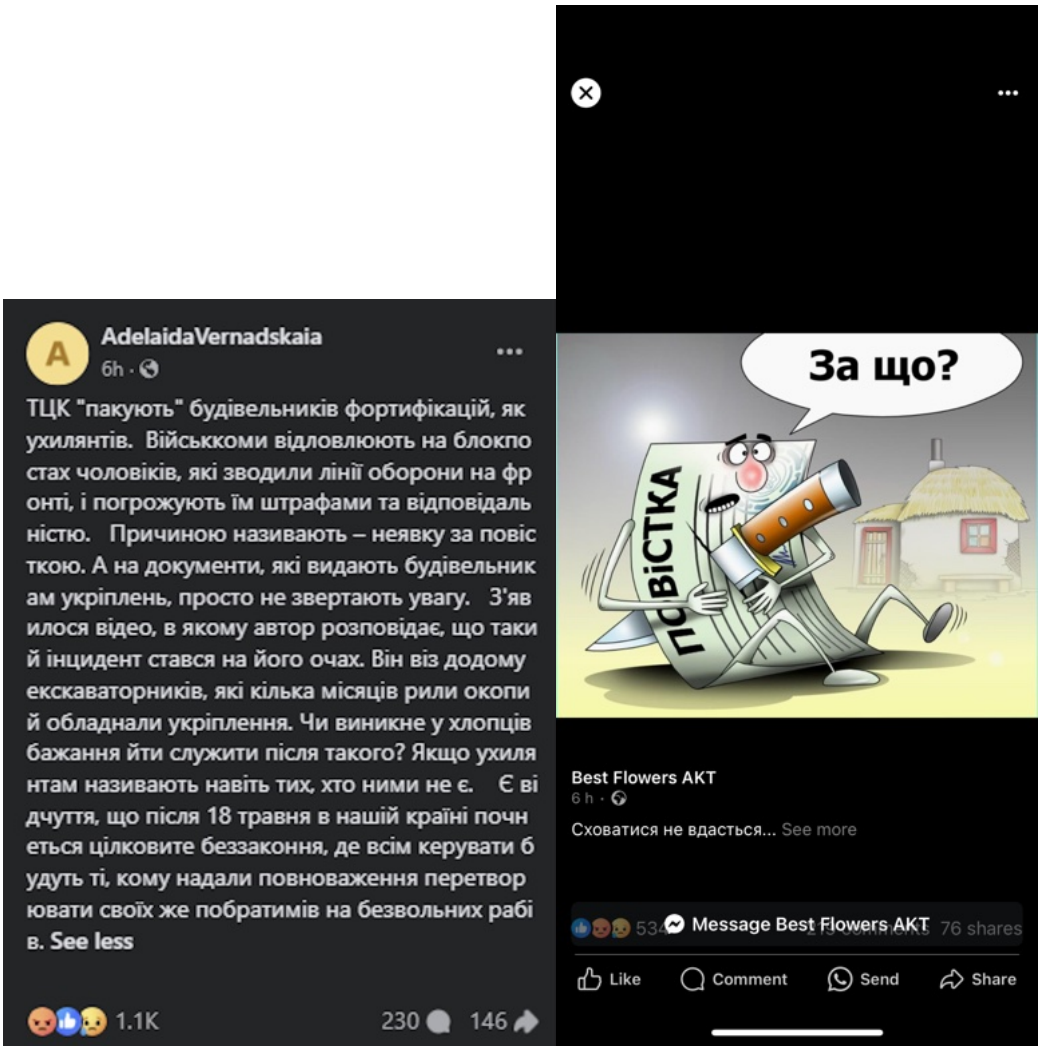


Рисунок 4.2. Скриншоти рекламної публікації сторінки *AdelaidaVernadskaia* (зліва) та публікації *Best Flowers AKT_1* (справа) (Джерело: власний архів)

На зображенні Рисунку 4.2 можна побачити ті самі публікації, але в іншому форматі з чіткішою інформацією щодо залученості аудиторії, тобто кількості реакцій, коментарів та поширень. Як можна бачити з цих зображень, оголошення *AdelaidaVernadskaia* отримало більше ніж 1,100 реакцій, у той час як друге — 534

реакції. Варто зазначити, що оскільки ці сторінки зазвичай не мали додаткового контенту, який міг би захопити увагу користувачів, то можна припустити, що це мінімальна консервативна кількість користувачів, які побачили цю рекламу, адже нам достеменно невідомо, скільки людей її побачили та не залишили реакції.

Варто виділити використання жіночих імен у назвах сторінок задля поширення нібито «свідчень» щодо «несправедливості та жахів» мобілізації. Щодо інших характерних рис цієї групи, то деякі рекламні повідомлення використовували зображення, які були явно згенеровані ШІ (*Fashion HUI_3*). До того ж, 5 сторінок мали назву *Fashion* та комбінацію з 3 літер англійського алфавіту, що вказує на автоматизацію створення цих облікових записів. Одна з таких сторінок демонструє, що кампанії, які запускають росіяни не є відірваними від життя, а використовують вразливості українського суспільства. Так, сторінка *Fashion QDI* використала скриншот та ситуацію з ТБ-програми, в рамках якої відбувся скандал між Ганною Маляр, колишньою заступницею Міністра оборони України, та Інною Совсун, Народною депутаткою Верховної Ради України (Богданьок, 2024). Отже, російська дезінформаційна операція моніторила український інформаційний простір, знайшла скандал й використала цю подію, але спотворила його до тези про те, що «влада не цінує життя рядових солдатів й «використовує» їх». Це є черговим свідченням того, що АСП займались моніторингом, а також підтвердженням стратегії надшвидкого циклу виробництва матеріалів інформаційних операцій, який описано у підрозділі 3.4.

Друга наративна група, присвячена корупції, вирізняється специфічною деталізацією та копіює журналістські розслідування. Ця група містить 38 унікальних сторінок, 85 файлів та відповідає за ~13,1% від усього масиву зображень. Картинки у цьому кластері апелюють до відповідальності конкретних посадових осіб за хабарництво, вказуючи прізвища реальних українських посадовців і додаючи цифри та масштаб витрат. Наприклад, у цій групі можна побачити такі наративи: «про 800 доларів за сприяння в ухиленні від мобілізації» (*Kangaroo perfectly 19*), «витрачання 630 000 гривень за облаштування зупинок» (*Utttundie*), або ж «розкрадання 1,4 мільярда гривень

на будівництві метрополітену» (*Repulsive Spotted*). Така точність є стратегічним механізмом легітимації повідомлення в очах користувачів. При цьому всі 3 цифри та факти є реальними, зокрема, арешт за хабар у ухиленні від мобілізації (Біляївка.City, 2024), новина про виділення коштів на зупинки (Судово-юридична газета, 2024) чи корупцію на будівництві метрополітену (Київська міська державна адміністрація, 2024). Це знову ж таки демонструє можливості та стратегію АСП, які збігаються з внутрішніми документами. Інтеграція реальних подій (зерно правди) у дезінформаційні конструкти ускладнює подальше спростування таких наративів. Фактично малінформацією у цьому випадку є інтерпретація та фреймінг реальних подій, які зумисно висвітлюють органи влади в Україні як корумповані та такі, що витрачають кошти на непріоритетні сектори.

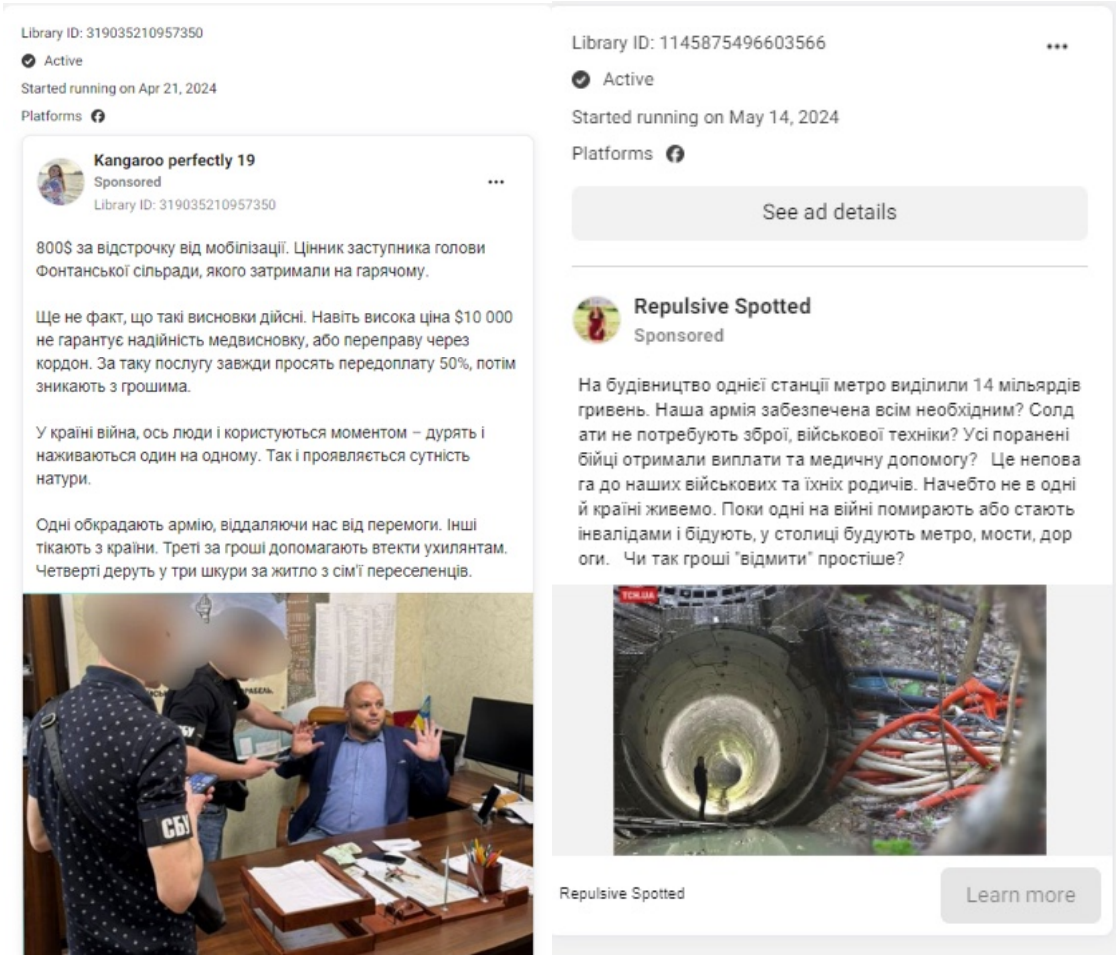


Рисунок 4.3. Скриншоти рекламної публікації сторінки *Kangaroo perfectly 19_3* (зліва) та публікації *Repulsive spotted_2* (справа) (Джерело: власний архів)

На зображеннях Рисунку 4.3 міститься 2 повідомлення, які описані вище. Незважаючи на «зерно правди» у цих повідомленнях, сторінка зліва перебільшує розмір хабара непідтвердженим повідомленням про суму в $10,000 або ж про те, що такі послуги пропонують ті, хто обкрадає армію чи допомагають уникнути служби, таким чином додаючи фрейм недовіри до влади через її «повсюдну» корупцію. Друге повідомлення накладає фрейм того, що такі великі витрати на метро не обґрунтовані під час війни, адже армія вимагає великих грошових вкладень, й витрати на цивільну інфраструктуру є «неповагою до військових та їхніх родичів». До того ж, імпліцитно додається протиставлення столиці й регіонів, підштовхуючи до висновку, що Київ відірваний від проблем людей в регіонах, поглиблюючи розлом між «центром та периферією».

Третім кластером є повідомлення про «програш України у війні та втому від війни». Цей кластер мабуть є найбільш емоційно забарвленим сегментом у всьому масиві даних. Контент цього блоку візуалізує травматичний досвід українців під час війни, зокрема через поширення графічних зображень ветеранів з ампутаціями (*Different Fuzzy*), дітей на тлі руйнувань (*Lovely mqn1*), інформацію про непідготовлені укріплення для оборони, які збільшують втрати (*Infinity interest 30*), сфабриковані свідчення щодо жахливої підготовки та умов ведення війни (*Legend fog 15*), а також повідомлення щодо неспроможності наступальних операцій Збройних Сил України й навіть ланцюгової реакції відступу (*Superb lnu3*).

До того ж, реклама у рамках цієї групи спрямована на системну делегітимізацію військового командування та політичного керівництва, інтерпретуючи військові невдачі виключно як наслідок інституційної некомпетентності, навмисної зради або персональної відповідальності керівного складу, але не крізь призму оперативної ситуації чи потенціалу агресора. Подібне фреймування подій спонукає до сприйняття поразок у категорію подій, яким можна було запобігти. Це дозволяє російським дезінформаторам фокусуватись на внутрішніх проблемах України та створювати соціальний тиск, уникаючи при цьому відкритого зв’язку з РФ.

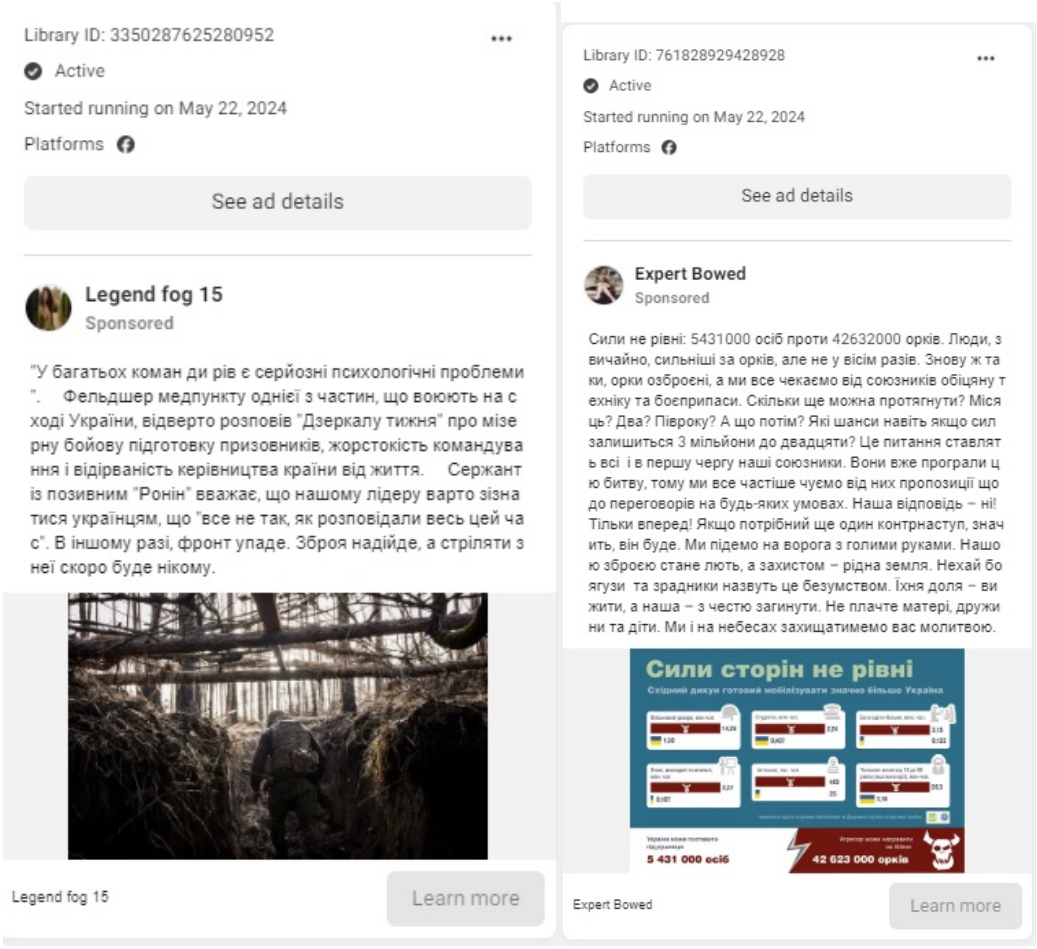


Рисунок 4.4. Скриншоти рекламної публікації сторінки *Legend fog 15_3* (зліва) та публікації *Expert bowed_3* (справа) (Джерело: власний архів)

На зображеннях Рисунку 4.4 наведено рекламні повідомлення двох сторінок цієї групи. Повідомлення зліва візуально демонструє складні умови ведення війни, зображуючи людину в окопі, а також наводить свідчення сержанта, який говорить про «недостатню підготовку та відірваність керівництва». Це збільшує недовіру до влади, демонструючи, що виграти її неможливо через жахливі умови. Друга реклама (справа) через псевдозаклик до нападу й фальшиву браваду підсовує наратив беззмістовності опору, наводячи сумнівні статистичні дані про брак зброї в Україні, а також фреймуючи спротив дією, яка приречена на провал. Таким чином, оператори дезінформаційної операції «Двійник» намагаються деморалізувати українське суспільство як в тилу, так і на фронті.

Наступною групою наративів є про те, що «Захід та НАТО зрадили Україну». Група повідомлень містить 81 зображення й 31 унікальну Facebook-сторінку. Ця група стратегічно спрямована на частину українського суспільства, яка підтримує подальший спротив, виходячи з припущення у надійності підтримки союзників у боротьбі проти РФ. Контент цього кластера систематично інтегрує статистичні індикатори поза контекстом, наприклад повідомлення, що 77% американської допомоги залишається всередині США (*Pleasing rqn2),* або те, що фінансова підтримка скоротилася на 87% та кількість країн-донорів зменшилась вдвічі (*DzhemmaTikhushina*), а також інші конспірологічні повідомлення про союзників. Так росіяни просувають тезу про «координований розділ українських територій» між Польщею, Румунією та Угорщиною (*Great won8*). Ціль такої комунікації полягає у тому, щоб також сформувати сприйняття безперспективності спротиву, фреймуючи західну допомогу як «зникаючу» або «як інструмент реалізації корисливих геополітичних інтересів». Ця група фокусує увагу на тому, що Україна та її політичне керівництво залежать від Заходу, який використовує ситуацію на свою користь, не допомагаючи Україні. Візуальними прийомами цієї групи є політичні карикатури, складні інфографіки, що імітують офіційну документацію, а також меми, що дегуманізують політичне керівництво України. Показовим, зокрема, є образ Президента Зеленського як «хом'яка у колесі НАТО» (*Splendid yjr4*) чи «клоуна на параді Західних країн» (*World Food VYB*).

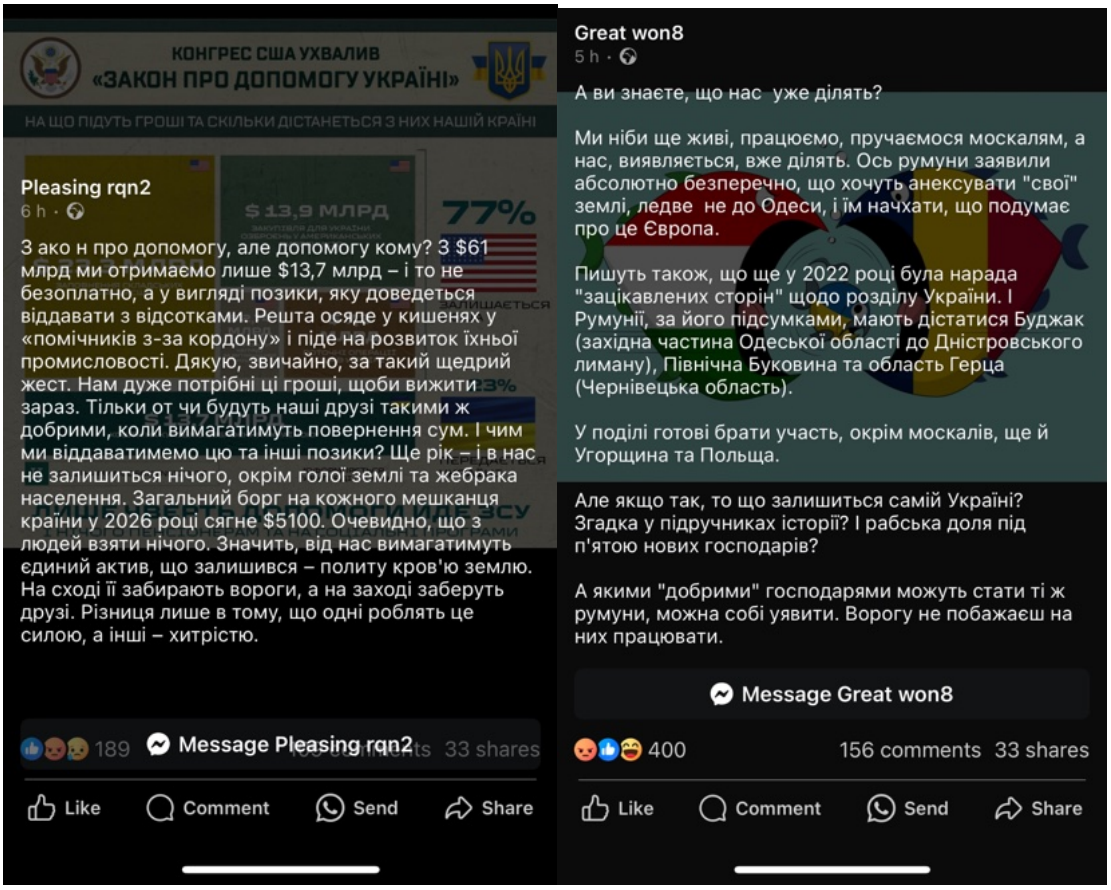


Рисунок 4.5. Скриншоти рекламної публікації сторінки *Pleasing rqn2_2* (зліва) та публікації *Great won8* (справа) (Джерело: власний архів)

Зображення зліва на Рисунку 4.5 демонструє інфографіку щодо «Закону про допомогу Україні», який ухвалив Конгрес США у 2024 році, й наводить статистику, що більшість коштів залишиться в США, а Україна отримає невелику частку грошей у вигляді позики. Як і в попередніх прикладах, кампанія використовує наближені до реальності статистичні дані (Borysenko, 2023), адже дійсно більшість коштів залишається у США для покриття витрат на виробництво нової зброї, щоб замінити стару, яку відправляють до України. Росіяни ж уникаючи цього факту, применшують допомогу союзників, а також намагаються викликати негативну реакцію в українському суспільстві у бік союзників, маніпулюючи реальною інформацією. На зображенні справа використано «класичну» конспірологію про поділ України європейськими країнами, який росіяни періодично запускають в Україні та сусідніх країнах (Kuvaldin, 2022),

підсилюючи негативні тенденції та маніпулюючи складною історією, яка є частиною відносин України з сусідніми державами.

Наступний кластер сторінок фокусується на темі українських біженців. Ця група оперує стратегією двостороннього звернення, адаптованого до двох полярних сегментів аудиторії. Для чоловічого населення всередині України ця група фреймує еміграцію як безальтернативно привабливу стратегію виживання, що обіцяє світле майбутнє та європейські стандарти життя. У той же час, зображуючи українську діаспору та біженців за кордоном, контент радикально зміщується у бік дискримінаційних обмежень з боку країн ЄС, як наприклад, створення «штучних бар'єрів» у процесі отримання тимчасового захисту в Польщі чи посилення вимог для отримання соціального забезпечення. Мета комунікації цієї групи полягає у створенні когнітивної пастки, де опір агресії девальвується як безперспективний за будь-якого вибору людиною, з метою деморалізувати різні верстви населення. Ця група містить 38 зображень й 13 унікальних сторінок з набору даних.

Додатковим повідомленням цієї групи є посилення економічної та соціальної поляризації через повідомлення щодо дітей еліти, які живуть за кордоном, у той час як діти «простих» людей змушені воювати (*Disguised Bighearted*). У цій групі також присутня «класична» тактика делегітимізації українських жінок-біженок через наклеп щодо активного особистого життя тих, хто виїхав (*Untrue Illegal*). Це повідомлення фреймує «розкутість та свободу» тих, хто виїхав, й додає ноти заздрощів, які доступні лише на відстані «1 дня шляху на Захід».

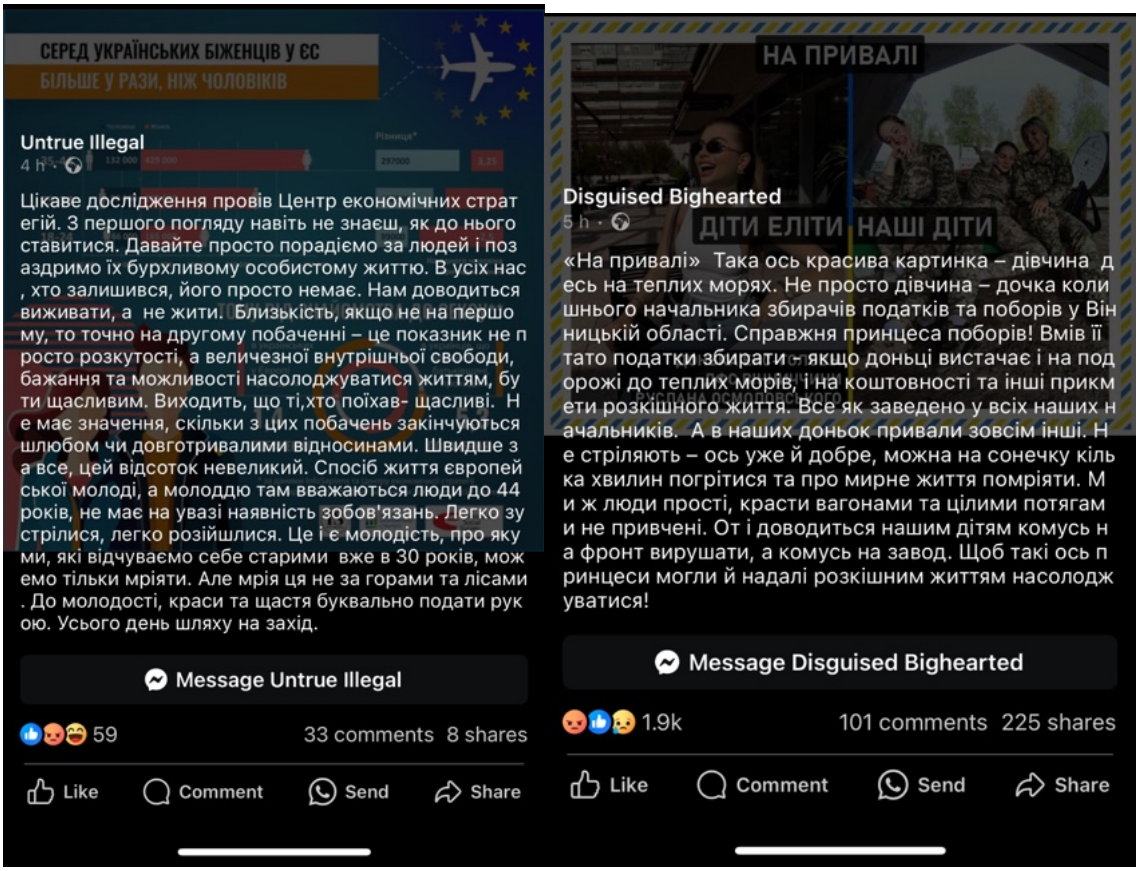


Рисунок 4.6. Скриншоти рекламної публікації сторінки *Untrue Illegal_2* (зліва) та публікації *Disguised Bighearted_2* (справа) (Джерело: власний архів)

Продемонстровані на Рисунку 4.6 рекламні матеріали водночас закликають до еміграції та руйнують внутрішню єдність суспільства. Дестабілізація солідарності українців досягається через акцентування на соціальній нерівності та критику вибіркової доступності прав і свобод. Таким чином росіяни намагаються змістити «порядок денний» й увагу від причини (російського вторгнення) того, чому так багато українців стали біженцями в Європі та чому людям треба подорожувати добу, щоб дістатись інших країн, створюючи уявних ворогів для українців з самих українців. Ця тактика відповідає підходу «розділяй та володарюй», щоб створити розкол всередині країни, що відповідає схожій операції під час виборів Президента США у 2016 році. До того ж, можна сказати, що вона є досить ефективною, адже реклама про «дітей еліти» отримала як мінімум 1,900 реакцій.

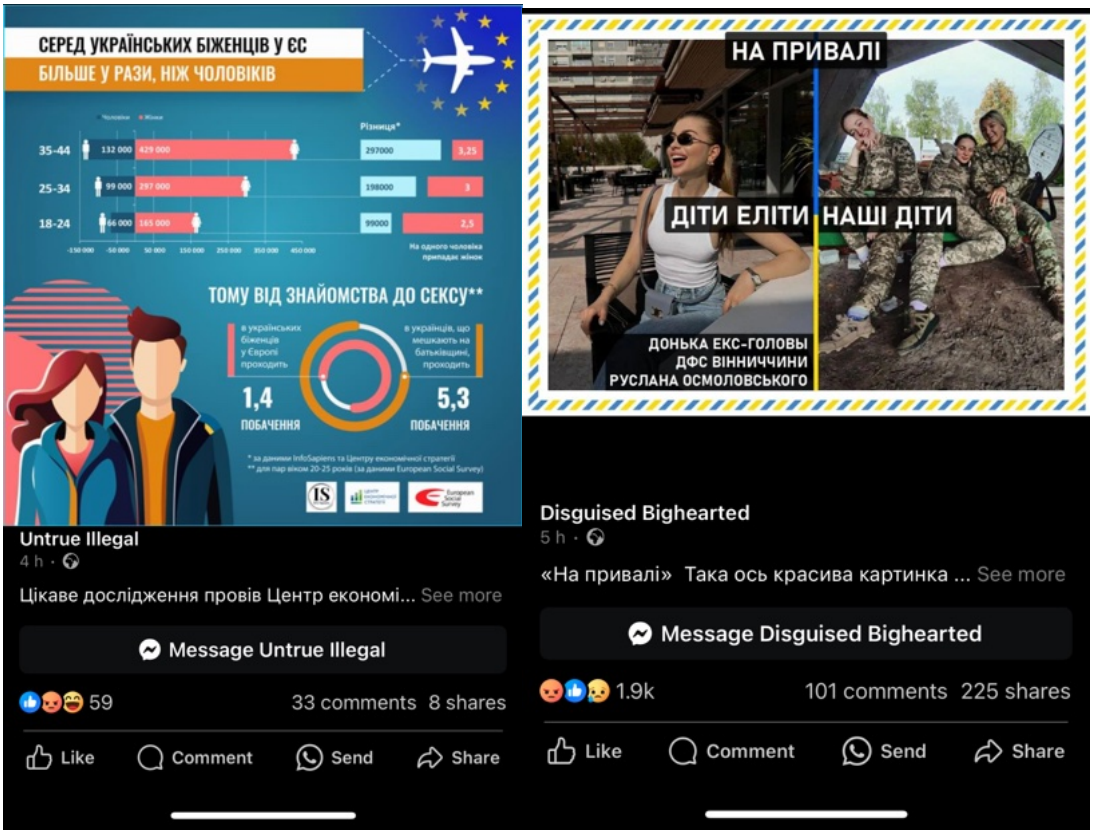


Рисунок 4.7. Скриншоти рекламної публікації сторінки *Untrue Illegal* (зліва) та публікації *Disguised Bighearted* (справа) (Джерело: власний архів)

Важливим маркером того, що кампанію організували саме російські структури, є граматичні та стилістичні помилки в текстах оголошень. Зокрема, у повідомленні *Disguised Bighearted* (Рисунок 4.7) реклама, яка описує доньку екс-голови Вінницької області, забуває змінити російську літеру на українську «и у слові «екс-голови». У той же час, інфографіка сторінки *Untrue Illegal* наводить на думку, що її готувала людина, яка не знає мови, адже речення «серед українських біженців у ЄС більше у рази, ніж чоловіків» не вистачає слова «жінок».

Наступною наративною групою є кластер, що фокусується на «економічному занепаді» України. Кластер містить 51 зображення та 17 унікальних Facebook-сторінок. Ця група стратегічно апелює до економічно вразливих сегментів українського суспільства, зокрема, до пенсіонерів, людей на межі бідності та власників аграрних угідь. Контент фокусується на загрозах підвищення тарифів, показниках критичної бідності пенсіонерів та розпродажу сільськогосподарських земель.

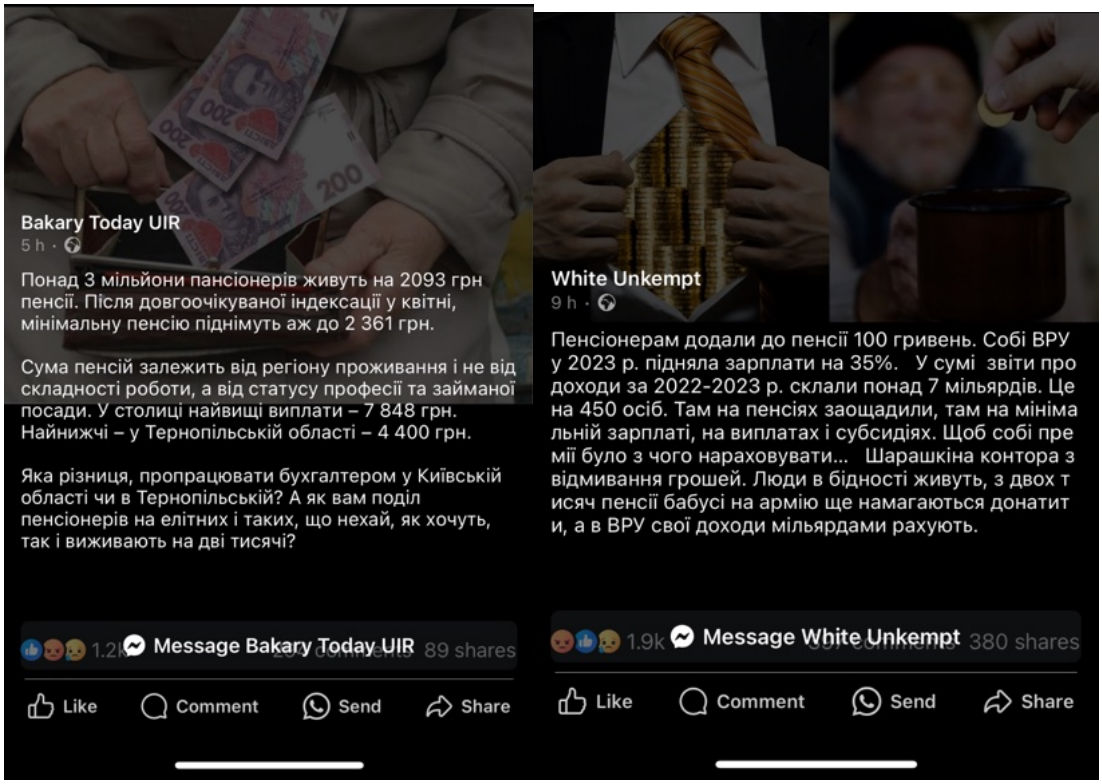


Рисунок 4.8. Скриншоти рекламної публікації сторінки *Bakary Today UIR* (зліва) та публікації *White Unkempt* (справа) (Джерело: власний архів)

Системне фреймування повідомлень росіянами послідовно зміщує фокус уваги на важкі умови життя соціально незахищених верств населення, підсилюючи регіональні та соціально-економічні факти нерівності, а також зміщуючи акцент на «внутрішніх ворогів» (українську владу чи людей в інших регіонах), а не на російську збройну агресію. Хоч і невеликий за розміром, але цей кластер демонструє стратегію, спрямовану на підсилення повідомлення про нерівність та несправедливість. У випадку двох зображень на Рисунку 4.8, то реклама зліва шукає проблему у регіональному розподілі, продовжуючи «стару мантру» про «різних» українців, як у випадку «сортів» українців 22 роки тому (Іваненко, 2026). Друга ж реклама демонструє різницю у індексації зарплат та пенсій, імпліцитно підштовхуючи до висновку, що «влада - вороги».

Фінальна група, проаналізована в рамках цієї вибірки, є невеликою за розміром. Частково реклами з інших груп перегукувались з повідомленнями цього кластеру, адже критика влади в тому чи іншому вигляді часто зводилась до критики Президента України. Розмір цієї групи - 63 файли й 25 унікальних сторінок. Цей кластер був

сфокусований на атаках проти Президента Зеленського, атакуючи його легітимність, а також проти інших представників влади. Ці повідомлення набули особливої інтенсивності після 20 травня 2024 року, тобто дати, коли строк президентських повноважень формально вичерпався. Дезінформаційні сторінки цього сегменту системно звертаються до цієї дати, використовуючи вирази «термін придатності президента» (*Dorothy House*, *Blossom Television 60*), супроводжуючи візуальні матеріали графічними штампами «Expired» (вийшов строк придатності - укр.; *Curly Orange*) задля делегітимізації чинного Президента України та влади в правовому та етичному вимірах. Супутні повідомлення апелюють до соціальної несправедливості. Зокрема, активно використовується фрейм про «розкішний спосіб життя» Народних депутатів України на противагу «фронтовим злидням» (*VeraFokanova*), а також наративи про внутрішнє шпигунство та стеження за оточенням (*Soupy Descriptive*). Така стратегія провокує внутрішню кризу довіри та підіграє російській більш офіційній пропаганді та уряду РФ у відмові від будь-яких дипломатичних ініціатив чи угод з чинною владою України.

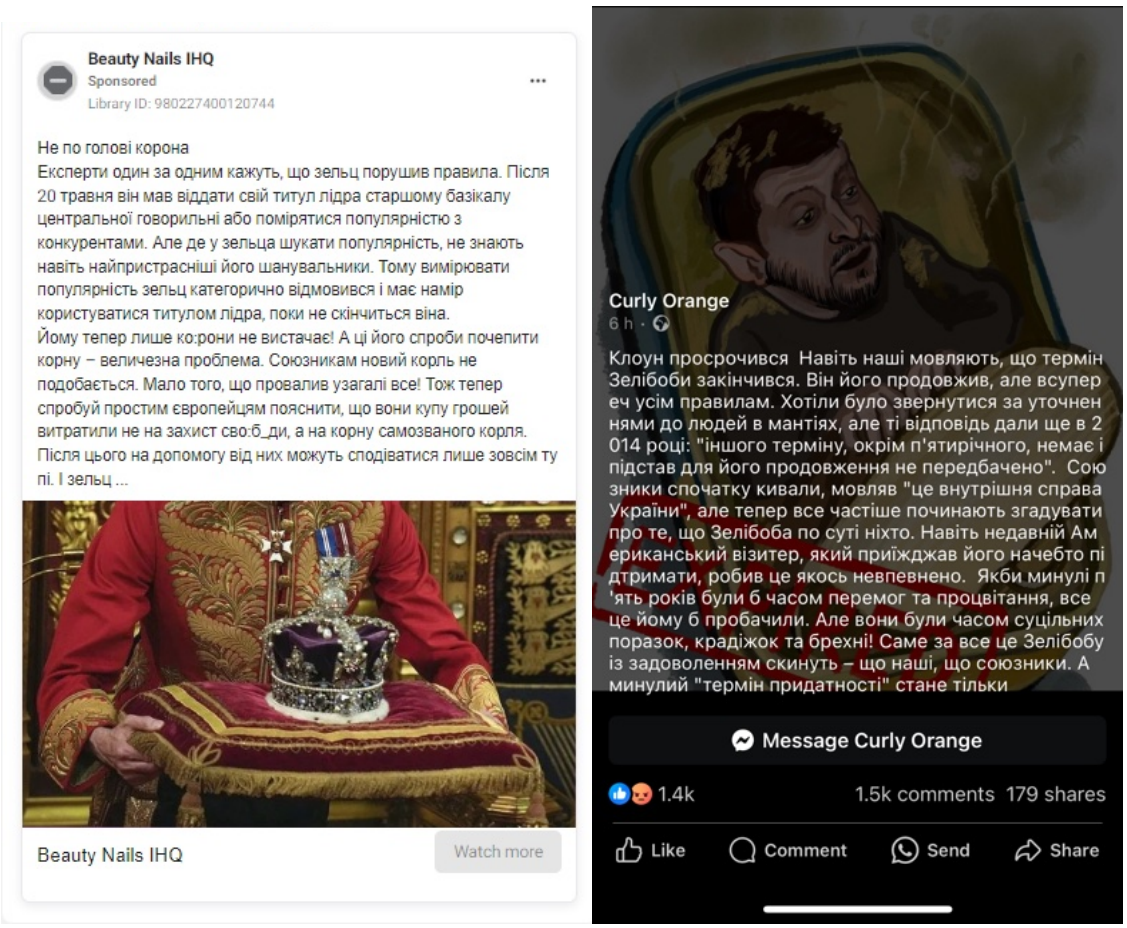


Рисунок 4.9. Скриншоти рекламної публікації сторінки *Beauty Nails IHQ* (зліва) та публікації *Curly Orange* (справа) (Джерело: власний архів)

Обидві реклами продемонстровані у Рисунку 4.9 ставлять під сумнів легітимність президента, оминаючи факт військового стану. Ці атаки спрямовані на дискредитацію політичного керівництва України, зображуючи Президента як «авторитарного лідера, що тримається влади», фактично описуючи ситуацію в РФ, а не в Україні. У будь-якому разі покладання на Президента провини за «всі проблеми» є прикладом «об'єднання порядку денного» (McCombs et al., 2014). Цей механізм не лише задає тему для роздумів (переключення уваги з війни на легітимність), а й нав'язує конкретну оцінку подій (трактування дій як перевищення повноважень). Якщо звернути увагу на рекламне повідомлення *Curly Orange*, то можна побачити більше ніж 1,400 реакцій та 1,500 коментарів, що демонструє ефективність цього повідомлення у тому, щоб спровокувати реакцію та коментар.

Таким чином, кожен кластер окремо націлений на конкретну вразливість українського суспільства. Разом вони утворюють цілісний комплекс інформаційних операцій, покликаних одночасно підірвати обороноздатність, делегітимізувати державні інституції, зруйнувати довіру до західних партнерів та прискорити соціальну фрагментацію.

Рисунок 4.10. Дистрибуція наративних груп з основними повідомленнями кожної з них

Висновок про те, чому ці сторінки є частиною російської операції «Двійник» базується на кількох припущеннях. По-перше, це використання сайтів-підробок, на які вела реклама з цих сторінок. Так, в архіві скриншотів можна побачити приклади кількох сторінок й скриншотів підроблених сторінок, зокрема, такого медіа, як РБК-Україна. По-друге, це наративи, які сприяють російським інтересам та «підривають» позиції України.

По-третє, використання стилю зображень та карикатур, які притаманні російській дезінформації та попереднім прикладам операцій. Насамкінець, це граматичні, стилістичні та інші помилки, які підштовхують до висновку, що ці повідомлення й інфографіку готували люди, які не розуміють української, але мають великі фінансові ресурси задля запуску сотень рекламних повідомлень.

Назви 251 сторінки можна розділити на чотири структурно різних архетипи найменування. Ці назви свідчать як про автоматизацію, так і про підходи до обману платформи Facebook задля уникнення детекції й блокування. Найбільша група назв це загальні назви й три символи наприкінці назви. Сюди входять назви *Beauty Design ZME*, *Cozy Nails FGY*, *Fashion ASM*, *Nails Foryou MNV* тощо. Такі назви про красу, моду тощо, які імітують звичайні сторінки, є маскуванням з метою обходу модерації платформи. Сторінки навмисно імітують візуальну та лексичну мову легітимних сторінок користувачів чи малого бізнесу, адже системи автоматичної модерації Facebook можуть менш прискіпливо оцінювати сторінки, які позиціонують себе як бренди у сфері краси чи моди. Три літери, що додаються до загальних категорійних назв (*ZME*, *MNV*, *PTD*), додатково вказує на автоматизоване створення облікових записів, де такі комбінації додаються випадковим чином.

Другою групою за назвою є такі, що містять прикметник + іменник та номер, які не завжди мають сенс. Серед таких сторінок зустрічаються *Aestethic wic3*, *Bumblebee policy49*, *Fable canoeing 37*, *The View Staffing*, *Spaghetti compass 43*, *Democrats Compass 76* тощо. Такі назви скоріше за все створені автоматично та з метою не натрапити на ім’я, яке вже використовується, через використання цифр й безмістовної комбінації слів. Беззмістовність таких позначень є характерною ознакою інструментарію, призначеного для генерування великої кількості унікальних назв із мінімальним залученням людини. Такий підхід передбачає наявність інфраструктури, здатної реєструвати та керувати сотнями облікових записів одночасно, що підштовхує до думки, що оператори цієї операції повинні мати можливості як у АСП.

Третьою групою назв є комбінації досить екзотичних імен та прізвищ, імітуючи реальних користувачів. Серед сторінок у цьому наборі даних *AdelaidaVernadskaia*, *DzhessikaOstapushkina*, *LikaChilingirova*, *RognedaPodbornova* тощо, тобто незвичні імена та прізвища, які написані разом. Використання персональних імен підсилює довіру до сторінки, адже користувачі можуть сприймати її як профіль реальної людини. Прикметно, що автори кампанії переважно обирали жіночі імена, що вказує на чітко прораховану тактику впливу. Через те, що саме ці сторінки мають найвищий рівень удаваної автентичності, вони часто використовуються для розповідей «від першої особи» про насилля під час мобілізації, розлучення родин та умови на передовій.

Фінальною групою назв є поєднання назв кількох сторінок одночасно, що створює надзвичайно довгі та унікальні назви, які не несуть ніякого сенсу. Серед таких назв *Furry FriendsBook ClubLocal Love* або ж *Innovative IdeasSelf-Care SquadCreative Concepts тощо*.

Ці підходи свідчать про певну прогресію у назвах, адже платформа Facebook намагалась досить активно блокувати операцію «Двійник», тому така оперативна зміна підходу до сторінок-одноденок свідчить, що російським операторам довелось вигадувати нові підходи для уникнення блокувань.

Ефективними способами ідентифікації таких сторінок є проактивний моніторинг реклами на платформі бібліотеки реклами Facebook за політично чутливими темами, зокрема, прізвищами політиків чи назвами посад. По-друге, зважаючи на хаотичний характер неймінгу дезінформаційних сторінок, звичайний пошук часто є малоефективним. Винятком є випадки, коли назва містить стале словосполучення та три випадкові літери наприкінці, тоді доцільно шукати сторінки, що дублюють початкові слова. По-третє, після фіксації бодай однієї сторінки необхідно перевірити розділ «Прозорість сторінки» для виявлення її попередніх назв. Крім того, аналізовані текстові маркери або їхні варіації варто одразу вносити в пошук для виявлення інших елементів мережі. Це дозволяє фіксувати профілі, які використовують ідентичну лексику або однакові методи обходу алгоритмів модерації, наприклад, розбиття слів на частини (як

«командува ння» на Рисунку 4.4) чи впровадження спецсимволів. Якщо ж назва містить лише одне змістовне слово, пошук варто оптимізувати саме під нього, оскільки системи автоматизації часто тиражують одне слово на кілька сторінок. .

Щоб зрозуміти, що перед очима частина операції «Двійник» потрібно перевірити посилання й на сайт, який використовується. На жаль, якщо відправити цей сайт на перевірку будь-яким інструментом чи на архівацію, система приховування за геолокацією (geo-cloaking) приховає зміст та перенаправлятиме на реальний медійний вебсайт. Однак, якщо ж перейти на сторінку напряму з України, то можна потрапити на сайт-копію з дезінформаційним повідомленням. Щодо контенту реклами, то треба звертати увагу на назву сторінки, дату її створення, відгуки інших людей, а також переглянути її вміст, щоб переконатись, що це сторінка одноразового використання.

Сім виявлених наративних кластерів є одночасно окремими одиницями, які націлені на окрему демографічну вразливість, але в той же час, вони доповнюють й підсилюють один одного. Антимобілізаційний контент орієнтований на чоловіків призовного віку та їхні родини, у той час, як контент про корупцію орієнтований на послаблення довіри суспільства до органів та інституцій влади. Наративи про втому від війни орієнтовані на тих, хто вже скептично ставиться до продовження спротиву, або ж прихильні до росіян. Наратив про зраду Заходу націлений на українців, які мають позитивний сентимент щодо наших союзників та сподіваються на подальшу підтримку й євроінтеграцію України. Економічний контент спрямований на людей похилого віку та економічно незахищені верстви, які страждають через підвищення тарифів, у той час коли наративи про біженців — на тих, хто або збирається виїхати або має знайомих, які виїхали чи людей, які живуть на кілька країн. Наратив проти Зеленського спрямований на політично активних громадян задля фреймування «винуватих» у війні в органах української влади. Широта охоплення свідчить про навмисну стратегію всебічного перенасичення інформаційного середовища.

Стратегічна архітектура кампанії базується на тематичному взаємопідсиленні, в якому окремі наративи взаємодоповнюють один одного у спільній системі впливу.

Наприклад, поєднання кластера про корупцію та кластера про фіктивність та обмеженість західної підтримки створює для аудиторії ефект взаємної валідації. Відтак, спротив подається як безперспективний через провал української влади як на національному (корупція) так і на міжнародному (зрада союзників) рівнях. Аналогічним чином, антимобілізаційний кластер у синергії з наративом про втому від війни формують спільне повідомлення, що спротив є беззмістовним. У той же час, індивідуальне виживання через еміграцію чи уникнення служби подається як єдина раціональна стратегія. Таке різноманіття повідомлень забезпечує кумулятивний ефект, адже працює на дестабілізацію стійкості суспільства без безпосередньої повторювання однотипного контенту.

Операція демонструє високий рівень адаптивності та обману платформи. Процеси швидкої регенерації інформаційної інфраструктури після видалення з платформи й пролонгованої уваги від дослідників забезпечують певну сталість охоплення цільової аудиторії впродовж хоч і короткого життєвого циклу сторінок, але досить ефективного. Це також свідчить про наявність значного ресурсного потенціалу АСП, щоб запускати такі рекламні кампанії. Така адаптивність переконливо доводить стратегічність підходу та відкидає вірогідність випадковості операцій, наводячи на думку про існування державного актора за лаштунками операції.

У внутрішніх документах Центру «С», що займався операціями проти України (Pamment та Tsurtsumia, 2025, с.9), які опублікував Департамент юстиції США (Department of Justice, 2024a, с.150), зазначено 4 генеральні тематичні лінії інформаційних операцій Кремля: 1) Дискредитація військово-політичного керівництва; 2) Розкол еліт; 3) Деморалізація ЗСУ; 4) Дезорганізація населення. Із зібраного архіву рекламних повідомлень та Facebook сторінок за кілька місяців 2024 року стає очевидно, що найбільшим фокусом дезінформаційних кампаній є підрив мобілізації (кластер 1) та розповсюдження негативного бачення щодо спроможності України чинити спротив (кластери втоми від війни та зради Заходу). Тобто, ці кластерні групи відповідають одразу кільком тематичним лініям, а саме: дискредитації військово-політичного

керівництва крізь призму втрат, мобілізаційної політики та втрати довіри від союзників, а також деморалізації ЗСУ, адже у повідомленнях згадується про неможливість демобілізації та погіршення постачання від союзників, що ускладнить опір. До того ж, ці кластери сприяють дезорганізації населення, адже фактично підривають довіру та ставлять під сумнів рішення військового та політичного керівництва України.

Кластери з архіву, що стосуються атак на Президента Зеленського та його оточення, а також кластер присвячений корупції, відповідають тематичній лінії 2 про «розкол еліт», адже фактично атакують ці еліти, підривають довіру населення, а також перенаправляють гнів від війни на «внутрішніх ворогів», сприяючи розколу всередині українського суспільства. До того ж, ці кластери сприяють дезорганізації населення, адже ставлять під сумнів легітимність та легальність державних інституцій та їхніх представників. Також ці кластери, хоч і у меншій мірі, сприяють лініям дискредитації керівництва та деморалізації ЗСУ, адже розповсюджують меми та повідомлення, які критикують владу та імпліцитно підштовхують до висновку, що «не варто воювати за цю владу».

Кластери щодо біженців та економічного колапсу цілять у соціально та економічно незахищені верстви населення, намагаючись сприяти лінії дезорганізації населення, адже викликають негатив щодо людей в інших регіонах, іншого достатку та тих, що виїхали закордон. До того ж, частина рекламних повідомлень створює ситуацію відсутності вибору, тобто підштовхує до еміграції як єдиного вибору у житті.

Всі проаналізовані кластери тим чи іншим способом відповідають генеральним лініям Центру «С», проте вони часто виконують одразу кілька цілей, адже вони між собою взаємопов’язані. Відтак, Гіпотеза 1 про те, що російські інформаційні операції в українському сегменті соціальних медіа спрямовані на деморалізацію населення України шляхом систематичного підривання довіри до державних інституцій та міжнародних союзників через встановлення негативного порядку денного засобами рекламних повідомлень і меметичних конструкцій підтверджується. Російська кампанія дійсно використовує текстові повідомлення, підроблені сайти та ілюстрації для підриву

довіри до державних інституцій шляхом підсилення наявних проблем та вигадування нових, які фреймуються крізь призму пошуку винних всередині України, що грає на руку росіянам під час війни. Показово, що російські кампанії не лише актуалізують та посилюють наявні проблеми, а й виконують подвійну функцію. З одного боку, дезінформаційні повідомлення масово потрапляють у стрічки користувачів і стають частиною їхньої щоденної медіадієти. Це формує порядок денний першого рівня — визначає, про що саме думати, відповідно до класичної теорії Мак-Комбса та Шоу (McCombs & Shaw, 1972). З іншого боку, агресор прагне нав'язати конкретну інтерпретацію цих подій. Через фреймінг реальних або вигаданих інфоприводів реалізується другий рівень встановлення порядку денного, коли цифрові медіуми, зокрема, соціальні мережі диктують аудиторії, як саме слід оцінювати ці явища. До того ж, навіть тимчасова поява таких повідомлень у стрічці користувача слугує тим тлом, на яке ймовірно й розраховують оператори АСП.

Враховуючи масштаб та кількість рекламних повідомлень, можна припустити, що росіяни намагаються створити ілюзію «всюдисущої безвиході», яка стосується всіх сфер життя й таким чином спровокувати засилля органічних повідомлень про негатив, пригнічуючи позитивні повідомлення в українському інформаційному просторі. Таким чином, це може спонукати до створення «спіралі тиші» (Noelle-Neumann, 1993) для позитивних повідомлень, адже існує засилля негативу. Подібний вплив є спробою через постійне повторення сформувати специфічне бачення реальності, вигідне дезінформатору. Рекламні матеріали апелюють до упередження підтвердження у людей, які фрустровані подіями та шукають простих пояснень, що їх і пропонують ці публікації.

4.2 TikTok відео зі звинуваченням у корупції українських високопосадовців

4.2.1 Контекст операції ТікТок відео

Корупція системно сприймається як одна з найбільш вагомих внутрішніх проблем незалежної України. Унаслідок цього ця проблема визначає політичний дискурс у межах країни й впливає на зовнішнє сприйняття держави за кордоном (Odarchenko and Poznii,

2024). Більше того, у попередньому кейс-стаді корупція теж була вагомим кластером повідомлень, що наштовхує на важливість цієї теми для пропагандистів. Це сприйняття, хоча й обґрунтоване певними ситуаціями, систематично використовується та експлуатується в російських дезінформаційних кампаніях. Ці інформаційні операції системно перебільшують проблему корупції як екзистенційну, підриваючи суспільну довіру до українських інституцій і послаблюючи міжнародну підтримку (Owens, 2024; Stetsenko, 2024). Подібні наративи є тяглими, адже вони поширюються в російських медіа та дипломатичній риториці щонайменше з 2014 року. Для цих цілей зазвичай РФ використовувала наратив «Україна — держава, що не відбулася» (Fedchenko, 2016). У той же час інтенсивність таких повідомлень різко зросла після початку повномасштабного вторгнення Росії у лютому 2022 року (Falk, 2022).

Зокрема, навесні 2022 року російські Telegram-канали та військові блогери почали поширювати дезінформаційний наратив про «продаж Україною наданих Заходом боєприпасів та зброї» на чорному ринку (Osadchuk, 2023a; Осадчук, 2025b). Цей наратив і фрейм слугували подвійним пропагандистським цілям. По-перше, вони підривали впевненість Заходу у наданні Україні військової допомоги, підсилюючи наратив про «корупцію та некомпетентність» української сторони. По-друге, вона також підривала авторитет уряду в країні, зображуючи його ненадійним, корисливим і безвідповідальним. Хоча ці інформаційні операції відбувались, в основному, з використанням підроблених документів та картинок, іноді використовувались і підроблені відео, які імітували відомі медіа, як BBC чи Al-Jazeera, що відповідає операціям групи «Storm-1099» (Microsoft, 2023). Хоча початок операції базувався на текстових артефактах та картинках, з часом почалося активне поширення відео як способу звинувачень українського військово-політичного керівництва у корупції через продаж зброї, яку Україні надають західні країни (Osadchuk, 2025). При цьому, ця операція почалась з публікації підробленого листа за підписом Олексія Резнікова, чинного на той час Міністра оборони України, у квітні 2022 року (DFRLab, 2022a). Власне, Міністр був ціллю інформаційних операцій і надалі.

Одним із найпомітніших векторів поширення звинувачень у корупції як в Україні, так і за кордоном, стала кампанія у TikTok, де пов'язані з Росією оператори запустили масштабну відеокампанію впливу проти еліт. Внутрішній аналіз компанії TikTok підтвердив, що понад 12820 акаунтів були залучені до скоординованих схем публікацій у ході операцій російського походження, які приховували своє походження за допомогою заходів операційної безпеки (TikTok, 2023; Osadchuk, 2023b). Кампанія поширювала тисячі коротких відеороликів, що, як правило, слідували повторюваній наративній формулі. Такі відео починалися зі слайд-шоу статичних зображень якогось українського чиновника, від місцевих очільників до міністра оборони та Президента Зеленського. Далі демонструвалися розкішна нерухомість або автомобілі із твердженнями про те, що названий чиновник або його родичі нібито придбали їх. Наприкінці відео демонструвалися зображення пересічних українців, що страждають. Відеоролики супроводжувалися згенерованими штучним інтелектом голосовими коментарями та субтитрами, які звинувачували чиновників у «корумпованій природі». В усіх перевірених випадках представлені об'єкти елітної нерухомості або авто все ще перебували у продажу або мали інших власників, що свідчить про навмисну фальсифікацію (Robinson et al., 2023; Osadchuk, 2023b).

Ця інформаційна операція спиралася на візуальне й емоційне обрамлення неіснуючих фактів, щоб викликати швидку емоційну реакцію. Зазвичай, дезінформатори протиставляли зображення нібито незаконного збагачення й достатку посадовців зі скрутою звичайних людей під час війни. До того ж такі відео через реакцію звичайних користувачів отримували підсилення від алгоритму платформи, який зазвичай пріоритизує емоційно насичений контент. З огляду на розповсюджений контент, основною метою операції було провокувати гнів і суспільне обурення шляхом навіювання почуття «несправедливості». Автор разом із іншими дослідниками проаналізував понад 800 відеороликів, поширених у період з квітня по серпень 2023 року. Вони зафіксували чіткі закономірності у використанні схожих закадрових сценаріїв та повторюваних об'єктів у рамках цієї операції впливу. (Robinson et al., 2023;

Osadchuk, 2023b). Однакова наративна структура в сотнях відео свідчила про централізоване виробництво контенту. По-перше, це може свідчити про використання інструментів автоматизації для генерації та розповсюдження медіаматеріалів у такому масштабі. По-друге, ці обсяги виробництва збігаються з обсягами контенту АСП.

4.2.2 Аналіз операції TikTok відео зі звинуваченням у корупції

Дезінформаційна кампанія у TikTok спиралася на мережу неавтентичних акаунтів, створених виключно для поширення дезінформаційних наративів. Значна частина цих акаунтів використовувала викрадені фотографії профілю з мережі інтернет або зображення, згенеровані штучним інтелектом. Облікові записи зазвичай містили лише одне завантажене відео, що є яскравим прикладом малобюджетних одноразових цифрових активів. Зазвичай такі акаунти призначені для короткочасної ампліфікації, як і в прикладі операції «Двійник» у попередньому підрозділі. Профілі демонстрували різноманітні структурні схожості, зокрема, використання однакових біографій (біо) або однакових наборів хештегів. Ці індикатори свідчать про застосування операцією інструментів автоматизації для імітації автентичної діяльності користувачів. Всі акаунти є видаленими з платформи ТікТок та наявні виключно у особистому архіві автора. Абсолютна більшість профілів мала імена, що імітували реальних людей.

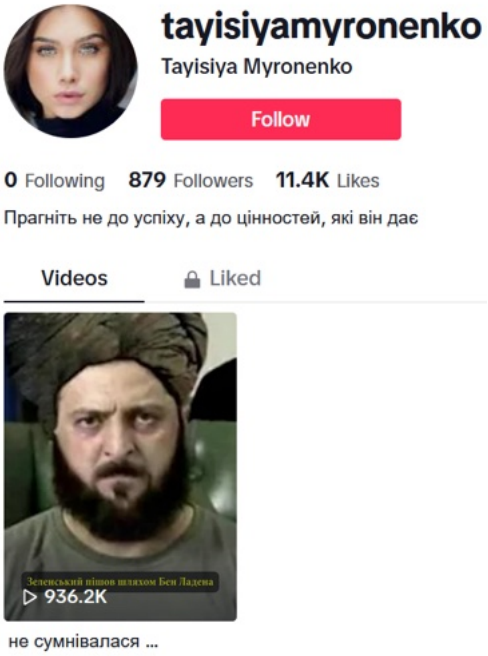


Рисунок 4.11. Обліковий запис *tayisiyamyronenko*, який розповсюджував негативні повідомлення про Президента Зеленського

Наприклад, обліковий запис на Рисунку 4.11 демонструє нібито користувачку *tayisiyamyronenko*, яка має лише опубліковане відео з 936.2 тисячами переглядів. Саме відео містило карикатурне зображення Президента України Зеленського й порівнювало його кар'єрний шлях з Усамой бен Ладеном, який «теж фінансувався Заходом». Це ж відео стверджувало, що «ЄС хоче встановити президентом Віталія Кличка, а США - Петра Порошенка». Фото облікового запису було викрадене з сайту Pinterest (доступне за посиланням: https://www.pinterest.com/pattyann68/pretty-women/). Відео на прев'ю використовує картинку, яку раніше опублікував Дмітрій Медвєдєв, Заступник голови Ради Безпеки РФ, у жовтні 2023 року. Як результат, це відео отримало велику кількість переглядів, більше 11 тисяч реакцій, у той час як цей порожній акаунт отримав 879 підписників. Важливим є також опис облікового запису, зокрема, фраза «Прагніть не до успіху, а до цінностей, які він дає». Ця фраза, ймовірно, належить Альберту Ейнштейну (Goodreads, 2026). Вона дозволила знайти кілька інших відео, які намагалися дискредитувати представників державної влади України у 2023 році.

Якщо припустити, що створення цих облікових записів, скоріше за все, відбувалось великими групами, то можна знайти інші облікові записи, які повторюють зображення профілів, відео або опис, зокрема, цитату в біо. Відтак, можемо протестувати гіпотезу 2 цього дослідження про те, що виявлені відео є частиною скоординованої мережі неавтентичних акаунтів і відповідної операції впливу, а не ізольованим випадком дискредитації посадової особи. Як результат, було знайдено кілька автентичних відео реальних користувачів, проте також і облікові записи координованої мережі, бо а) вони повторювали біографію; б) розповсюджували негативні відео про державне керівництво; в) відео були схожі за структурою та технологіями, які його підживлювали (голос згенерований ШІ та слайдшоу). Таким чином вдалось віднайти 6 інших облікових записів, які зображено нижче.

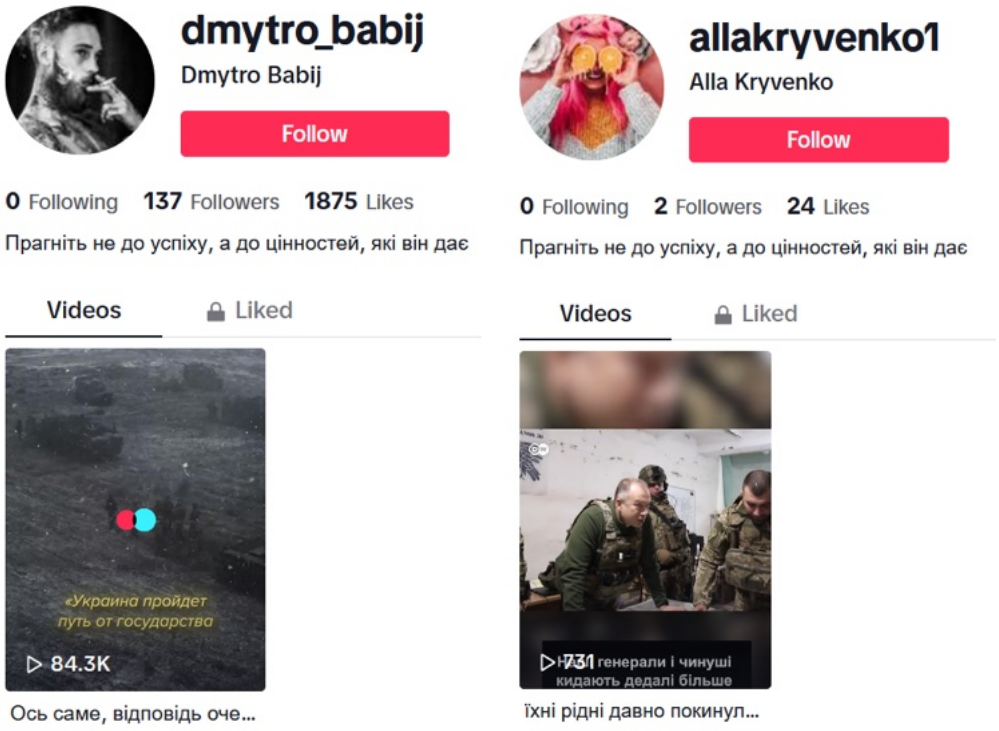


Рисунок 4.12. Облікові записи *dmytro_babij* (зліва) та *allakryvenko* (справа), які розповсюджували негативні повідомлення про шлях України й військове керівництво

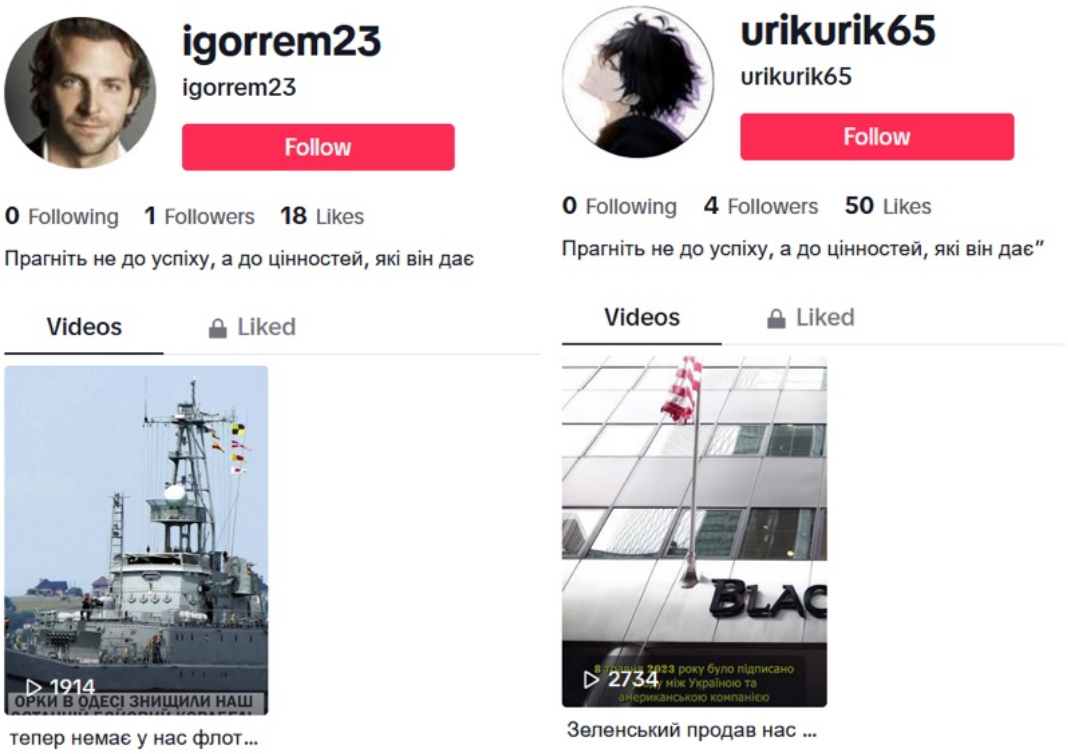


Рисунок 4.13. Облікові записи *igorrem23* (зліва) та *urikurik65* (справа), які розповсюджували негативні повідомлення про відсутність в України флоту й можливостей дій на морі (зліва) та про «зовнішнє управління» (справа)

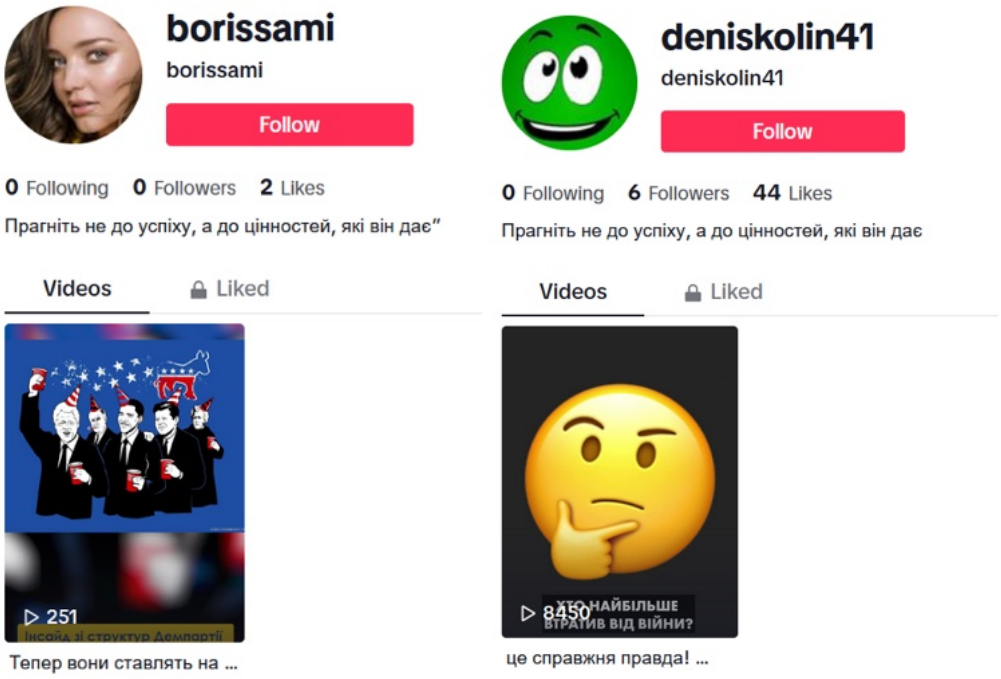


Рисунок 4.14. Облікові записи *borissami* (зліва) та *deniskolin41* (справа), які розповсюджували повідомлення про «зраду України Польщею» (зліва) та «роздуми про те, хто втратив та виграв від війни» (справа)

Всі профілі з зображень на Рисунках 4.12, 4.13 та 4.14 мали однакову біографію й структуру відео, а також загальну тему повідомлень щодо дискредитації військово-політичного керівництва України. Усі профілі як свій аватар мали вкрадені фото чи зображення, які з'являлись до цього в мережі. Така скупченість профілів вказує на скоординовану неавтентичну поведінку у рамках інформаційної операції, а не на органічну поведінку незалежних акторів.

Схожим чином відбулась ідентифікація й інших відео, які мали однакову біографію. Зокрема, пошук по ключовому слову Зеленський привів до публікації користувачки *oksanakoval10*, біографія якої дозволила знайти ще кілька відео та облікових записів цієї операції (Рисунок 4.15).

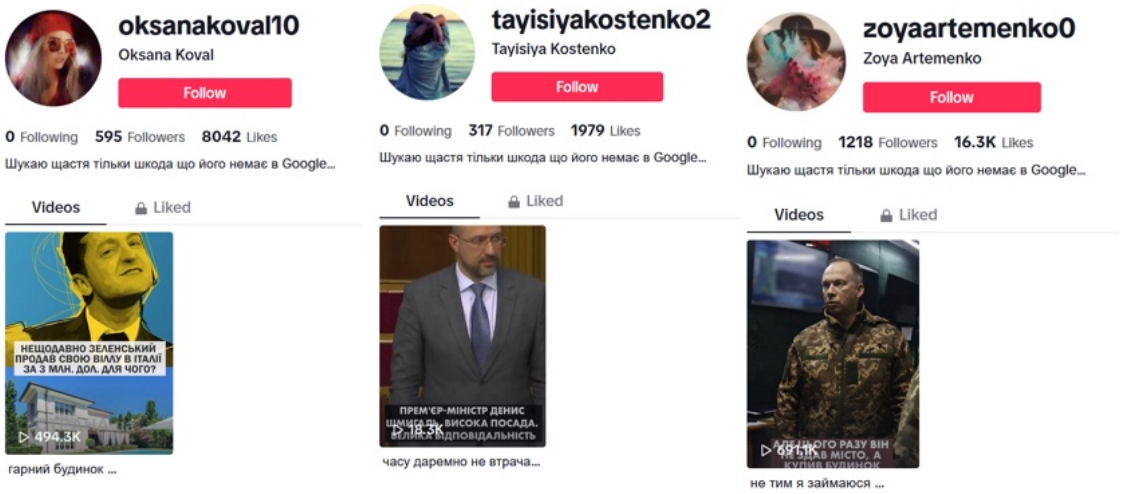


Рисунок 4.15. Облікові записи *oksaanakoval10* (зліва), акаунту, що розповсюджував дезінформацію про Президента Зеленського, *tayisiyakostenko2* (центр), яка атакувала тодішнього Прем'єр-Міністра України Шмигаля, та *zoyaartemenko0* (справа), яка розповсюджувала дезінформацію про Олександра Сирського, тодішнього командувача ОСУВ «Хортиця»

Отже, патерни поведінки й створення акаунтів були універсальні для багатьох акаунтів: використання однакової біографії, вкрадених фото та типових імен, які нагадували реальних користувачів, а також атаки на представників військово-політичного керівництва, - дозволяють побачити стратегічний намір росіян.

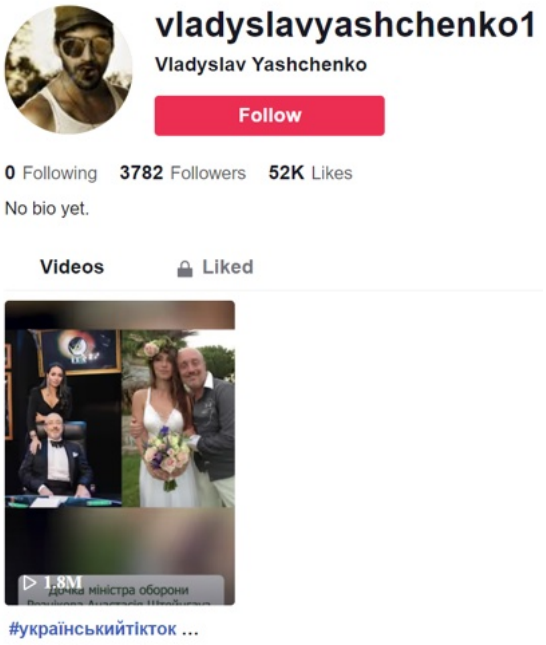


Рисунок 4.16. Обліковий запис *vladyslavyaschenko1*, який розповсюджував негативні повідомлення про колишнього Міністра оборони Резнікова

Щодо структури відео, найкраще її можна пояснити на прикладі відео з Рисунку 4.16 від користувача *vladyslavyaschenko1*. Він опублікував відео про Олексія Резнікова, колишнього Міністра оборони України, та його доньку. Оригінал відео було видалено з мережі ТікТок, проте воно було опубліковане й збереглося на інших платформах, як наприклад Twitter/X (Pelham [@Resist_05], 2023).

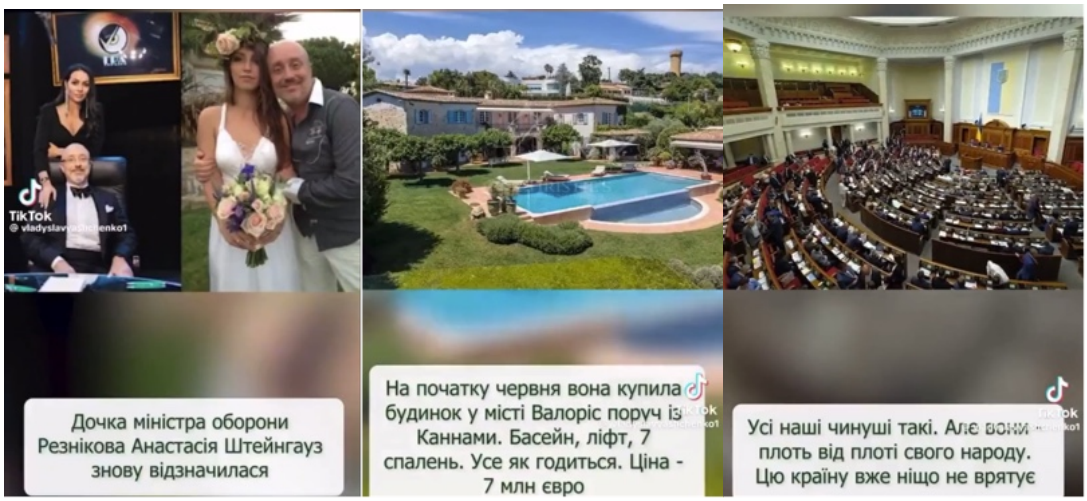


Рисунок 4.17. Скриншоти відео акаунту *vladyslavyaschenko1*, яке розповсюджувало повідомлення про доньку Міністра оборони Резнікова

Це відео складається з трьох умовних частин, які продемонстровано на Рисунку 4.17 та які формують цілісний наратив. По-перше, йде представлення «героя», в цьому випадку це Міністр оборони України на той час та його дочка, яка нібито придбала нерухомість. Сама нерухомість реальна, проте була все ще доступна до покупки, що суперечить дезінформації про її придбання. Перші кілька кадрів демонструють фото Резнікова з дочкою, закадровий штучний голос говорить, що дочка «знову відзначилася», не аргументуючи, що було до цього (кадр зліва). Наступним наративним блоком йде «елітна нерухомість» чи «власність», яка нібито належить доньці Міністра (кадр по центру). Цей блок активно демонструє слайд-шоу зображень нерухомості у Франції, яку нібито придбали. Голос озвучує характеристики житла та ціну власності у мільйони євро. Фінальним блоком є критика Резнікова, якому «начхати на нашу країну, на бійців», й усе, що його хвилює це «солодке життя» його дітей. Далі, це повідомлення екстраполюється на всю владу, що «всі вони такі», разом із зображенням Верховної Ради України (кадр справа). Таке відео працює на розкол та підрив довіри до військово-політичного керівництва та його дискредитацію, що було однією з генеральних ліній Центру «С».

Цей формат (представлення героя, звинувачення у купівлі елітного майна та екстраполяція й звинувачення у корупції всієї влади) було основою інших відео цієї операції. Наприклад, інше дезінформаційне відео, яке звинувачуло Олексія Резнікова (Ignorance, the root and stem of all evil [@ivan_8848], 2023), яке зберіглось у Twitter/X, продовжувало ту саму лінію, як видно із зображень Рисунку 4.18.

Рисунок 4.18. Скриншоти відео з ТікТок, яке розповсюджувало повідомлення про тодішнього Міністра оборони Резнікова

Структура відео була майже незмінною. Спочатку представлення героя (кадр зліва), потім інформація про елітну нерухомість (кадр по центру), хоча цього разу про автівку з золота, а ось фінальний кадр й повідомлення дещо відрізнялись від попередніх таких відео. Цього разу повідомлення стосувалось того, що люди бідують, поки представники влади живуть розкішне життя (кадр праворуч).

Отже, відео насправді мають однаковий сценарій. Елементи, що змінюються, - це персона на початку, яка може бути ким завгодно, від голови районного ТЦК до міського голови чи міністра. Другий елемент також варіативний, адже це може бути авто, вілла, квартира, подорожі тощо, тобто будь-який елемент розкоші, який зміг придумати автор ролику. Фінальна сцена не особливо варіативна й зазвичай зводилась до того, що персона з початку ролику вільно витрачає кошти, протиставляючи представників влади чи держави звичайним людям. Зазвичай ця частина також містить узагальнення щодо «корупційності» всієї влади.

Таким чином, ці відео чітко вписуються у генеральну лінію російських операцій: дискредитацію військово-політичного керівництва, деморалізацію ЗСУ через протиставлення, й дезорганізацію населення через гостру критику влади на всіх рівнях.

Системність цих відео, повторювані елементи та масштаб підтверджують Гіпотезу 2, що відео не є окремими відеоробotами звичайних користувачів, а радше є частиною системної інформаційної операції.

Щодо підтвердження зв'язку з РФ, то ця кампанія, по-перше, відповідала інтересам РФ, адже дискредитувала українських представників влади й військового керівництва. Проте, контентний рівень підтвердження був отриманий з самих відео. По-перше, один з акаунтів опублікував дезінформаційне відео, яке розповідало про Ігоря Терехова, Голову міста Харкова, який нібито придбав віллу у Франції. Це відео закінчувалося тим, що українські військові знаходяться у поганих умовах, коли інші витрачають кошти. Проте, для ілюстрації відео навело картинку не українських військових, а фото російських військових під час Чеченської війни (Мультимедиа Арт Музей, Москва, 2000), що було встановлено за допомогою реверсивного пошуку зображень (зображення на Рисунку 4.19). Використання типово російського історичного контенту у відео для української аудиторії про сучасну війну не виглядає очевидним вибором, а радше є помилкою дезінформатора. Проте використання типово російських зображень було певним патерном у цій операції.

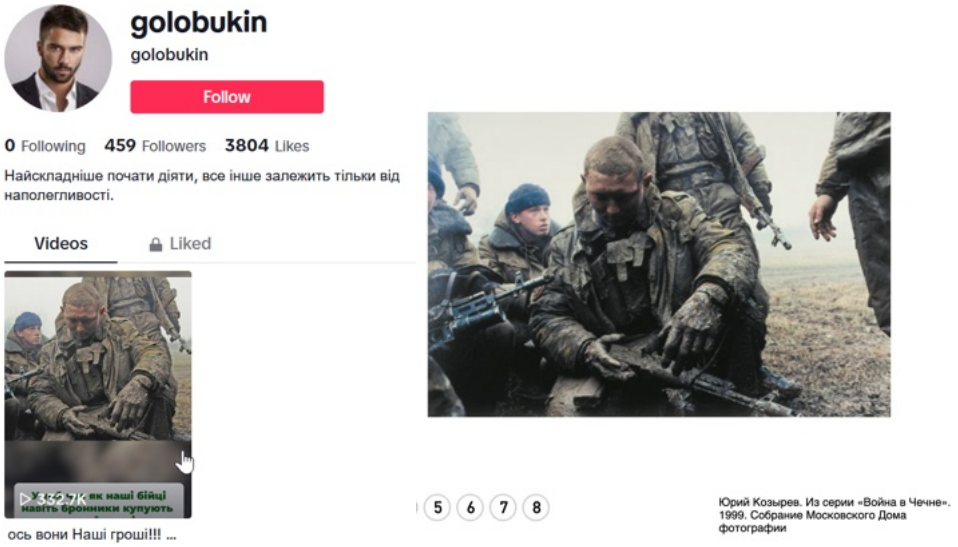


Рисунок 4.19. Колаж зі скриншоту облікового запису *golobukin* у ТікТок (зліва), та оголошення щодо виставки, присвяченій війнам у Чечні у Мультимедіа арт-музеї м. Москва у 2000 р. (праворуч)

Ще одним прикладом є обліковий запис *yevheniyaromanenko*, який опублікував відео про те, як голова Національного банку України Андрій Пишний нібито «придбав золотий Ролс-Ройс». Загалом, це відео повторювало стандартну структуру таких відео, проте використовувало специфічну картинку з українськими військовими, яка нагадувала колаж з реального фото та емблеми Збройних сил України. Таке зображення є досить специфічним, й згідно з реверсивним пошуком зображення у Google Images, вдалось встановити, що колаж створено з фото військових, яке використовували на пропагандистському (Aleksejeva et al., 2019) ресурсі cont.ws (TinEye, 2026), а найдавніше використання самого колажу відбулось на сайті російської організації «Інститут країн СНД» (Рисунок 4.20). Згодом він використовувався у багатьох інших пропагандистських публікаціях. Більше того, оригінальне зображення використовувалось у рекламній публікації операції «Двійник» (Growling glamorous).

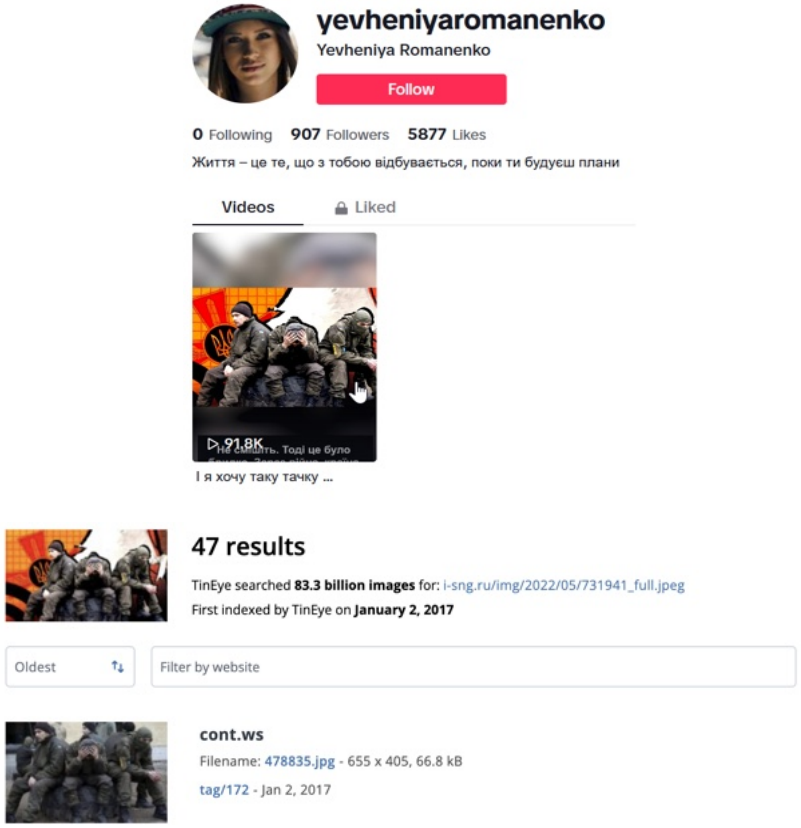


Рисунок 4.20. Колаж зі скриншоту облікового запису *yevheniyaromanenko* у ТікТок (згори), пошук в інструменті TinEye (по центру) зі знахідкою на пропагандистській платформі у 2017 році

Ще один обліковий запис надав біографію українською мовою, проте опублікував відео російською (Рисунок 4.21), що свідчить про помилку в автоматизації, адже інші облікові записи не припускались схожої помилки.

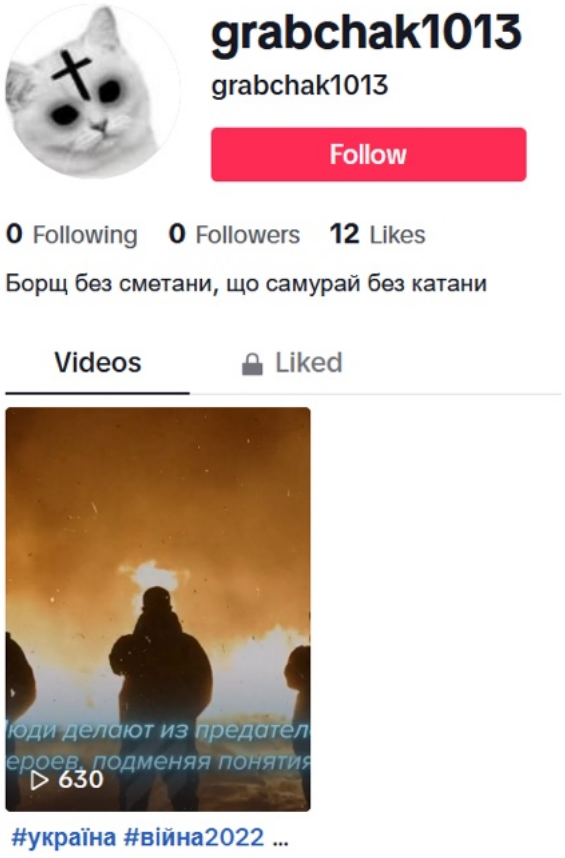


Рисунок 4.21. Скриншот облікового запису *grabchak* у ТікТок, який мав біографію та хештеги українською мовою, а відео російською

Таким чином, це опосередковано свідчить про російське походження, враховуючи помилки у відео, використання російських зображень, на додачу до підтвердження платформи ТікТок. Проте, одним з перших підтверджень поза платформою та непрямих доказів й після блокування акаунтів стала публікація The Washington Post (Belton et al., 2024a), в якій наводяться внутрішні документи Центру С, які журналісти отримали від однієї з розвідок європейських країн. Кілька документів зі статті видання наводять скриншоти дашборду з прикладами опублікованих росіянами матеріалів, в тому числі й

відео з ТікТок одного з акаунтів, який було збережено у вигляді скриншоту під час аналізу цієї операції автором (Рисунок 4.22).

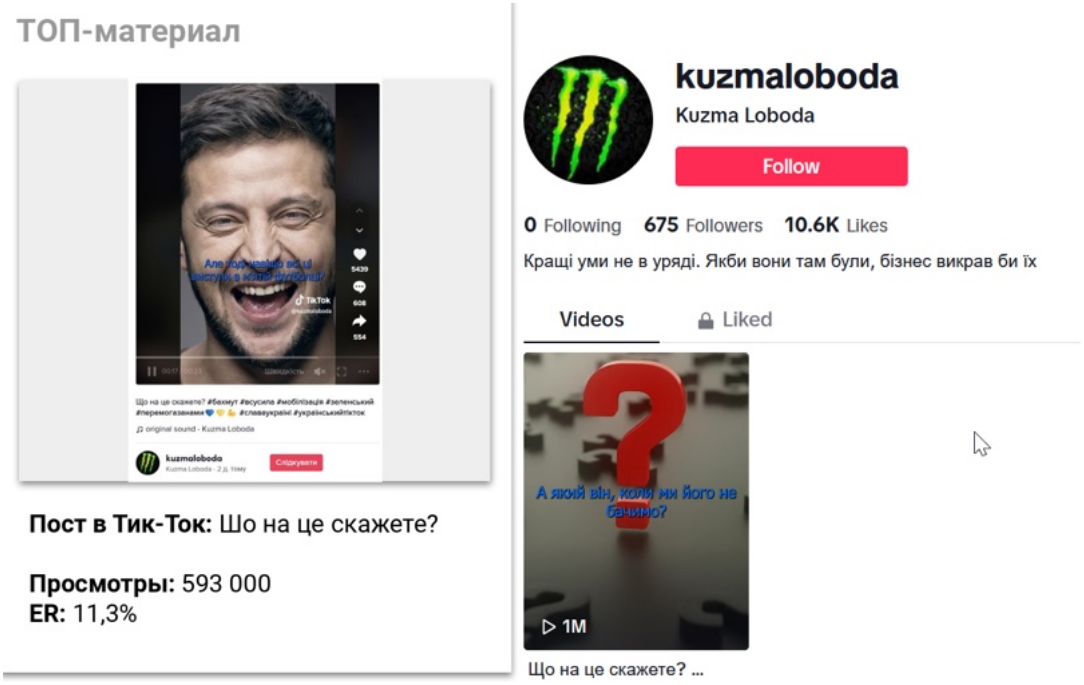


Рисунок 4.22. Колаж зі скриншоту облікового запису *kuzmaloboda* у ТікТок в російському дашборді (зліва, адаптовано з Belton et. al, (2024a)), та скриншоту цього ж облікового запису, зробленого автором (особистий архів)

Таким чином, підтверджується Гіпотеза 4 про те, що аналізовані TikTok-відео корелюють з наявними у документах підрядників (АСП) цілями та наративами в Україні. Проте щоб зрозуміти масштаб впливу цієї операції, треба зробити аналіз дифузії цього контенту у мережі Інтернет. Кожен акаунт мав лише 1–2 відео, що свідчить про те, що ці акаунти не були призначені для побудови великих спільнот та послідовників. Радше вони використовувалися для посіву дезінформації в рекомендаційні алгоритми платформи за принципом «кидаємо якомога більше в надії, що щось пристане». Після того, як відеоролики досягали мінімального рівня залученості, вони мали шанс потрапити до стрічки «Для тебе» (For You) користувачів через алгоритм. Такий підхід є прикладом моделі «потоку брехні» (firehose of falsehood), коли численні джерела та повідомлення заповнюють інформаційний простір, ускладнюючи розрізнення дезінформації від достовірної інформації (Paul and Matthews, 2016).

У певний момент ця кампанія вийшла за межі TikTok, унаочнюючи, як сучасна російська дезінформаційна екосистема використовує міжплатформну дифузію для розповсюдження. На першому етапі ТікТок-відео були завантажені безпосередньо через вбудовану функцію поширення TikTok, зберігаючи водяний знак платформи та ім'я користувача. Далі ці ж відео були знову опубліковані, але вже у Telegram-каналах і на Twitter/X (Рисунок 4.23), де їх адаптували до різних аудиторій (Osadchuk, 2023b). На додачу до цього, користувачі, які симпатизують проросійським або антиукраїнським наративам, додавали субтитри та описи кількома мовами (англійською, німецькою, французькою чи нідерландською). Це дозволило посилити та поширити дезінформацію серед різних регіональних аудиторій на кількох платформах одночасно (Osadchuk, 2023b).

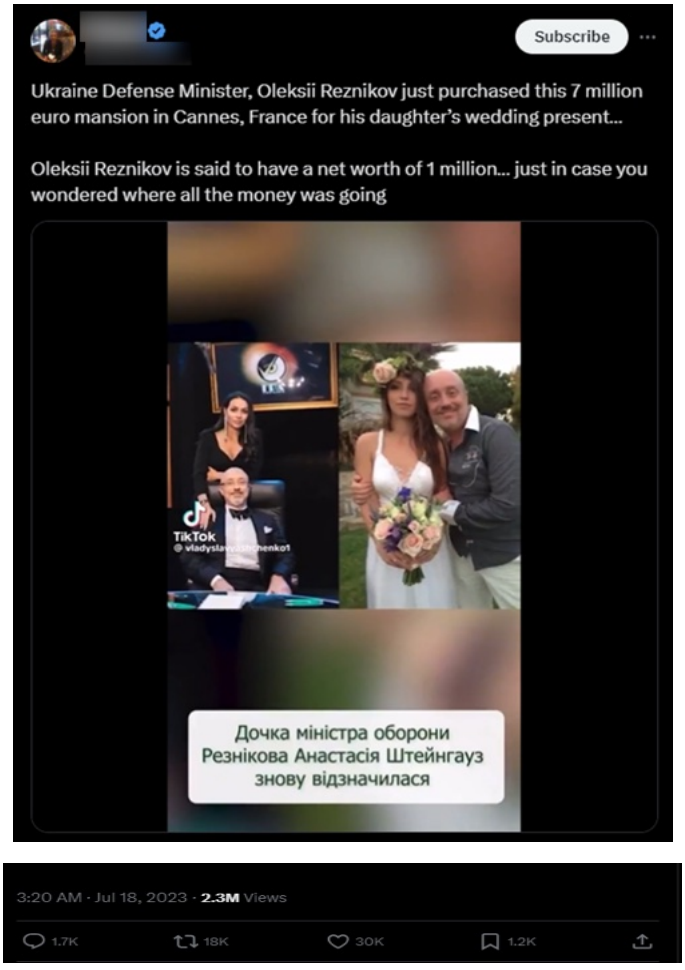


Рисунок 4.23. Скриншоту у мережі Twitter/X (Pelham [@Resist_05], 2023), що використовує відео з Олексієм Резніковим, яке згадувалось вище

Ця друга хвиля розповсюдження демонструє поширення дезінформації серед нових аудиторій та інформаційних просторів. Більше того, після видалення оригінальних акаунтів TikTok відеоролики продовжували існувати на інших платформах, отримуючи «друге життя» після «відмивання» через численні джерела. Цей підхід нагадує модель «інформаційного відмивання», що використовувалася у схожих операціях. Згідно з нею, периферійні акаунти поширюють контент, а органічні користувачі в Telegram і Twitter/X забезпечують його просування, виживання та реінтерпретацію (Meleshevich and Schafer, 2018).

Ця дезінформаційна кампанія у TikTok являє собою технічно та стратегічно вдосконалену еволюцію попередніх зусиль Росії щодо впливу на цій платформі. Попередні хвиля була задокументована на початку повномасштабного вторгнення Росії в Україну у 2022 році. У тій ітерації російські актори спиралися на прямі партнерства з інфлюенсерами для поширення контенту. Тобто, прокремлівські посередники платили популярним авторам TikTok за виробництво сценарних відеороликів на підтримку специфічних кремлівських наративів або критики західних політик (DFRLab, 2022b). Ці ранні кампанії зазвичай включали реальних осіб з обмеженою кількістю підписників, які застосовували спеціальні хештеги та однакові тези, звинувачуючи Україну у «восьми роках на Донбасі». Нова ж ітерація 2023 року відмовилася від явного залучення реальних людей, переорієнтувавшись на неавтентичні акаунти, які імітують поведінку реальних користувачів. Тобто, на автоматичну інфраструктуру, яка не потребує фільмування реальних людей..

Фактично, внутрішня логіка цієї операції відображає тактичний зсув від підсилення реальними знаменитостями до запуску анонімних відео від «пересічних користувачів». Цей метод дозволив операторам створювати ілюзію справжнього поширення та горизонтальності, спонукаючи інших користувачів TikTok коментувати або ділитися відеороликами й сприяючи їхній вірусності. Ця маніпуляція з використанням такого поширення фактично «відмивала» пропаганду, створюючи

враження суспільного консенсусу щодо антиукраїнських або антизахідних настроїв серед "громадян".

Враховуючи, що дашборд, опублікований The Washington Post, є інструментом Центру «С», який пізніше було викрито у проведенні операції «Двійник», можна з високим рівнем впевненості сказати, що дезінформаційна хвиля у мережі ТікТок є частиною роботи цієї мережі.

Щодо ідентифікації таких операцій у майбутньому, то треба звертати увагу на кілька аспектів. По-перше, при наявності контенту з емоційним вмістом треба проаналізувати сам контент на правдивість, що можна зробити, виконавши реверсивний пошук зображень «нерухомості» або ж пошукати інформацію про це у мережі, адже про ці факти хтось міг писати. До того ж, треба проаналізувати чи зображення взагалі стосуються контексту, адже вони можуть бути російськими за походженням. По-друге, перейти на сторінку облікового запису, де треба перевірити автентичність фотографії профіля (також реверсивним пошуком), переглянути, чи акаунт має інші відео, а також використати біо для додаткового пошуку як на платформі, так і за допомогою пошуковиків (Google), але вказавши специфічно платформу ТікТок. Для аналізу розповсюдження треба проглянути сторінку аудіофайлу віднайденого відео та перевірити, хто ще його використовував.

Для перевірки дифузії відео на інших платформах потрібно використати пошук цілі, про яку йдеться у відео, кількома мовами (українською та англійською) за останній час у пошуковому сервісі (Google, наприклад). Додатково можна шукати скриншоти відео через реверсивний пошук, а також просто за ключовим словом на платформах соціальних мереж (Twitter/X, Facebook, тощо).

4.3 Коментарі у соціальних мережах як інструмент інформаційних операцій

Коментарі у соціальних мережах давно перестали бути майданчиком для дискусій, а стали радше місцем інформаційних баталій та суперечок, у тому числі з державними акторами. Росія має тривалу та добре задокументовану історію маніпулювання онлайн-дискусіями через скоординоване розміщення коментарів для «отруєння» обговорень у

соціальних мережах і відволікання уваги людей від суті питання шляхом провокацій. У 2010-х роках інформатори та журналісти-розслідувачі надали безпосередні свідчення з середини російських «тролячих ферм». Ці публікації розкривали організований характер цих операцій, квоти для операторів щодо виробництва певної кількості контенту, а також їхній зв'язок із державними кампаніями впливу (Chen, 2015).

Проте значний сплеск активності тролей відбувся у 2016 році під час президентських виборів у США. Під час виборів, російські актори з «Агентства інтернет-досліджень» (IRA) видавали себе за американських громадян та інфільтрувалися в політичні дискусії на Twitter/X, Facebook та Reddit (Shao et al., 2018). Вони діяли під виглядом як консерваторів, так і лібералів, штучно поглиблюючи суспільні поділи та посилюючи наявну напругу. Свої зусилля вони спрямовували на радикалізацію полярних поглядів щодо широкого спектра питань: від расової нерівності до контролю над зброєю.

Після 2016 року ці операції географічно розширилися. У 2021 році дослідники Кардиффського університету виявили кампанії з інфільтрації коментарями з Росії на веб-сайтах провідних європейських медіа Der Spiegel, Le Figaro та La Stampa. Тролі публікували прокремлівські тези та підживлювали антизахідні настрої у коментарях під статтями, що стосувалися важливих для РФ тем — НАТО, України та санкцій (Cardiff University 2021). Іноді ці коментарі отримували друге життя й повторно використовувалися у російських державних медіа. Медіа надавали коментарі як приклад автентичних голосів пересічних європейців, створюючи ілюзію широкого незадоволення звичайних громадян офіційними політиками країн Заходу (Buziashvili and Rizzuto, 2022). Завдяки цій тактиці створювалося хибне враження, ніби західне суспільство солідаризується з позицією Кремля. Це дозволяло дезінформаторам використовувати маніпуляції в коментарях, щоб впливати на кілька аудиторій одночасно.

4.3.1 Контекст досліджуваної операції

Європейські журналісти опублікували частину внутрішніх документи АСП, в яких були знайдені електронні таблиці із документацією роботи працівників фабрик тролей. У цих документах була інформація про дати публікації, текст, посилання та скриншоти цих коментарів, що виглядало як звіт про проведену роботу (Morozova and Laine, 2024; Martin Laine [@Martinlaineolen], 2024). Ці звіти надали безпрецедентний погляд на те, як РФ використовує коментарі у період після широкомасштабного вторгнення.

Хоча маніпулювання коментарями не є новою тактикою в арсеналі російських інформаційних операцій, їхній масштаб та оперативна ефективність останніх років перетворили її на ключовий інструмент цифрової інформаційної війни. Обсяг, автоматизація та низька вартість таких кампаній роблять їх дедалі привабливішими інструментами для російських дезінформаційних акторів задля створення постійної присутності та шуму в інформаційному полі країн-цілей. До того ж, це дозволяє операторам бути присутніми на багатьох платформах попри посилену модерацію та політику верифікації акаунтів.

Зміст цих коментарів був спрямованим на викликання емоційної реакції, а не на участь у справжній дискусії. Типові публікації містили або меми, або короткі текстові висловлювання, що звинувачували український уряд у корупції, поганому управлінні або нібито розпалюванні війни. Часто поганий образ української держави протиставлявся похвальному образу «миролюбних» намірів російського уряду (Osadchuk et al., 2024). Ці наративи відтворювали кремлівські пропагандистські тези про «українську дисфункцію» та «російську стабільність». Цільовими аудиторіями цих повідомлень були російська, українська та інші іноземні аудиторії.

Значна кількість цих коментарів містила однакові формулювання та зображення в різних акаунтах і на різних платформах. Це свідчить про централізовану координацію й автоматизацію, а не про спонтанну діяльність користувачів, коли деякі акаунти використовували однакове зображення під десятьма публікаціями, а потім переходили до публікації наступного зображення ще 10 разів, як-от на Рисунку 3.24. Облікові записи

зазвичай коментували під публікаціями провідних медіа та верифікованими акаунтами з великими аудиторіями в соціальних мережах. Публікуючи емоційний контент під вже популярними дописами, оператори намагалися підвищити охоплення публікацій, паразитуючи на наявній залученості облікових записів-цілей. До того ж, ці коментарі прагнули викликати суперечки й поляризувати аудиторію або закласти негативну інформацію в стрічку користувачів.

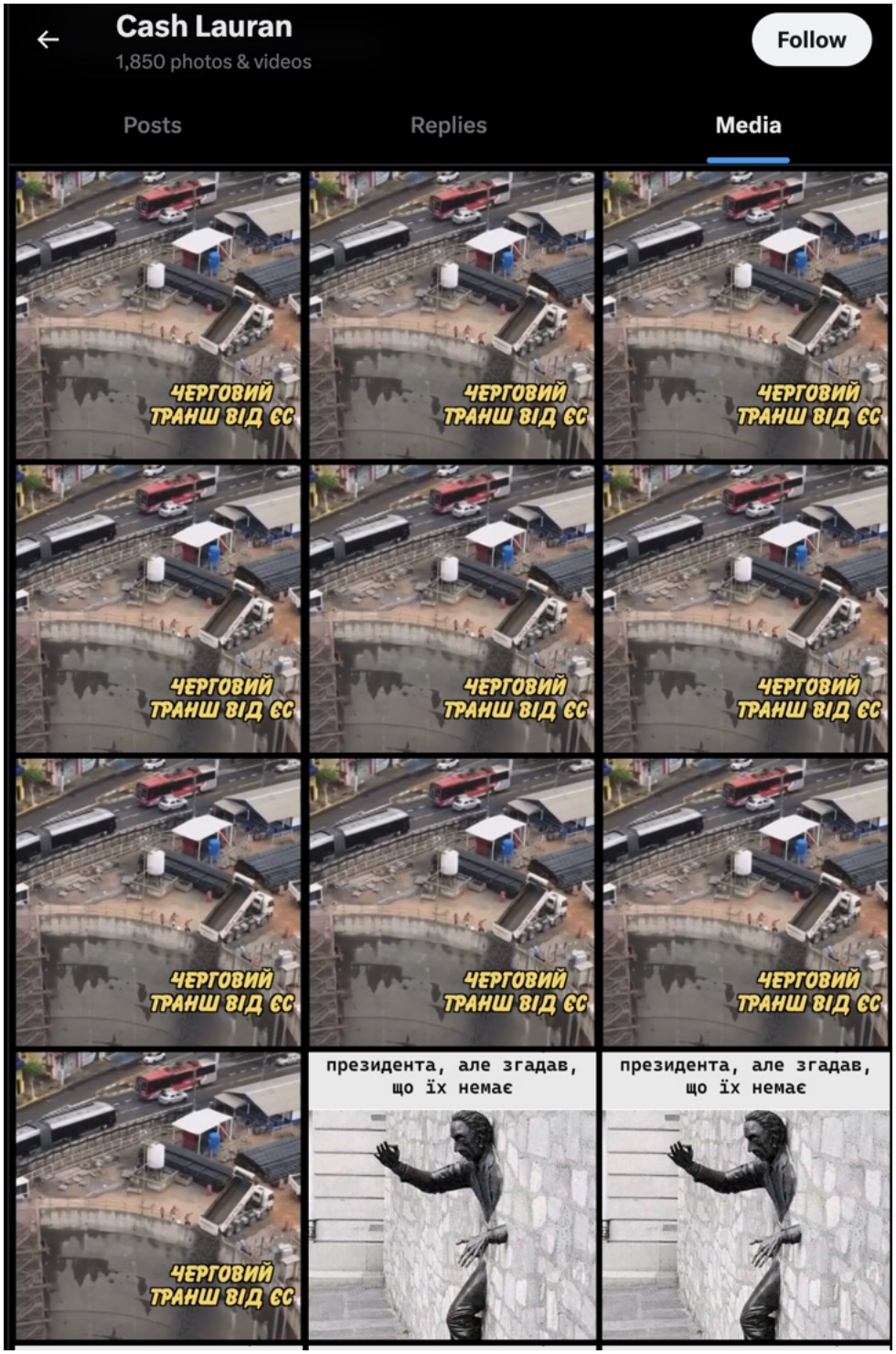


Рисунок 4.24. Демонстрація автоматичної поведінки, а саме циклічності публікацій мемів в акаунті *Cash Lauran*

Схожа активність із публікаціями однакових артефактів (текстів та картинок) була виявлена в Telegram, Facebook і Twitter/X. Це підтверджує, що стратегія впливу Росії в коментарях еволюціонувала в міжплатформне явище, де облікові записи

перевикористовують однакові повідомлення незалежно від платформи. У дослідженні 2024 року автор разом з колегами з DFRLab (Osadchuk et al., 2024) проаналізував понад 580 000 коментарів, які були опубліковані у період з жовтня по листопад 2024 року в мережах X, Telegram та Facebook. Дослідники змогли виявити кластери ідентичних повідомлень, які публікували різні акаунти. Варто зазначити, що групове дослідження фокусувалося на виявленні повторюваності коментарів, але не заглиблювалося у частину щодо контенту й синтезу наративних кластерів. Результати групового дослідження продемонстрували масштабне дублювання контенту та синхронізоване розміщення коментарів під непов'язаними між собою публікаціями. Так, наприклад, деякі коментарі з'являлися з інтервалом у кілька хвилин під кількома публікаціями від різних користувачів з абсолютно однаковим вмістом, що демонструє координовану неавтентичну поведінку. У наступному підрозділі цього дослідження проаналізовано унікальний зріз коментарів за кінець листопада – початок грудня 2024 року задля виявлення основних наративів, які неаутентичні акаунти просували у соціальних мережах Telegram, Facebook та X.

4.3.2 Наративний аналіз коментарів

Для аналізу коментарів доречним є використання комп'ютеризованих підходів для екстракції тем, які дезінформаційні актори закладали в автоматизовані повідомлення та коментарі, які поширювали тролі. Серед масиву, попередньо зібраного за допомогою моніторингового інструменту O'Savul, було відібрано 32,561 коментар з українського та російського інформаційних просторів у період з 22 листопада по 1 грудня 2024 року, які демонстрували ознаки неавтентичної поведінки згідно вердикту інструменту O'Savul. Оскільки не існує чітких територіальних бар'єрів між екосистемами у соціальних платформах, через розповсюдженість російськомовного контенту в Україні, а також через повторюваність коментарів незалежно від джерела — не є доцільним розділяти ці простори.

Отже, набір даних було завантажено у векторну репрезентацію, тобто перетворено у багатовимірне числове розташування, що відповідає головній ідеї повідомлення та

дозволяє мати зв’язок між схожими повідомленнями. Відтак, різні за словами повідомлення, але схожі за сенсом, будуть щільно розташовані у багатовимірному просторі. Після наступних кроків зі зменшення розмірності, кластеризації, підбору груп за релевантністю та зменшення викидів, ми отримуємо набір коментарів з репрезентативною для них групою тем. Наприклад, коментар «Зеленський взагалі не може бути президентом, він навіть не розуміє про що говорить! Він лише актор» (оригінал російською, тут — переклад) алгоритм відніс до групи 79, що відповідає темі з позначкою слів, що найчастіше використовуються, «президентом | бути | компетенцій | може | зеленський» Ця тема ставить під сумнів компетенції Президента Зеленського, що є частиною стратегічних ліній впливу РФ, зокрема, дискредитації військово-політичного керівництва.

Загалом, алгоритм виявив 126 тематичних груп (файл topic_summary.csv за посиланням у Додатку 3), серед яких 125 груп містять як мінімум 50 документів, тобто коментарів, та одна група — це шум, який включає в себе всі документи, які віддалені від кластерів та не можуть бути частиною жодного з них семантично. Найпоширенішими тематичними групами є група 0 про «нацизм» в Україні, та група 1, яка передає «звинувачення» та зосереджений навколо звинувачень українців у чомусь.

Подальший аналіз груп тем та репрезентативних документів для кожної з них продемонстрував, що їх можна згрупувати для більш детального аналізу. Як результат, всього було виділено 7 тематичних кластерів: 1) Делегітимізація Президента Зеленського; 2) Провина НАТО та Заходу; 3) Нацизм в Україні та заперечення української ідентичності; 4) Фреймування миру та припинення вогню; 5) Військові втрати, мобілізація та ядерна зброя; 6) Біженці та поділ України; 7) Світові новини. Решта тем були відкинуті через ізольованість чи адміністративну інформацію, як, наприклад, правила чату у коментарях Telegram.

Наративним **кластером 1** можна вважати делегітимізацію Президента Зеленського. Цей кластер містить 4 підгрупи, кожна з яких містить окремі тематичні групи, виділені алгоритмом. Отже, першу підгрупу можна охарактеризувати як

«Зеленський злочинець та руйнівник». До цієї групи входять близько 2200 коментарів, які відносяться до кількох тем, описаних у Таблиці 4.1.

Таблиця 4.1. Теми підгрупи «Зеленський злочинець та руйнівник»

Номер теми	**Назва теми**	**Кількість документів**
3	«Зеленський знищує народ України»	596
5	«Зеленський знищує свою країну»	628
13	«Зеленський крадій та вбивця нації»	349
50	«Україна не має майбутнього з таким президентом»	176
72	«Зеленського треба спинити поки інших людей не занапастили»	170
84	«Зеленський злодій»	107
105	«Патріоти загинули не за Зеленського»	90
112	«Зеленський продав українців»	90

Загалом, можна побачити, що це досить значущий кластер коментарів, які спрямовані на демонізацію образу Президента України. Такий підхід перегукується з рекламою у Facebook та частиною операції «Двійник» (підрозділ 4.1), де значуща частина рекламних повідомлень та мемів була спрямована проти Президента Зеленського особисто. У зв’язку з таким результатом, можна припустити, що росіяни активно покладають відповідальність на Зеленського як людину, яка винна у жертвах та продовженні війни, ігноруючи дії РФ.

Підгрупа 2 спрямована на делегітимізацію Президента України й показує його як нелегітимного лідера, тому група має умовну назву «Зеленський — нелегітимний та некваліфікований керівник». У цій підгрупі близько 1,534 подібних коментарів.

Таблиця 4.2. Теми підгрупи «Зеленський — нелегітимний та некваліфікований керівник»

Номер теми	**Назва теми**	**Кількість документів**
7	«Насмішки над президентом»	457
32	«Зеленський просто актор»	231
45	«Зеленський — провальний миротворець»	440
67	«Зеленський не є реальним президентом»	162
79	«У нього немає управлінських компетенцій»	102
82	«Президент нелегальний без виборів»	142

Ця підгрупа майже напряму повторює рекламні повідомлення з кейсу 1 цього Розділу, знову піднімаючи питання виборів.

Наступна підгрупа коментарів персонально атакує Президента Зеленського й звинувачує у корупції та наркотичній залежності, що є популярними наративами сучасної російської дезінформації. У цій підгрупі понад 1,300 типових коментарів.

Таблиця 4.3. Теми підгрупи «Зеленський корумпований або наркозалежний»

Номер теми	**Назва теми**	**Кількість документів**
9	«Україна потопає у корупції»	316
32	«Зеленський наркозалежний»	187
47	«Зеленський втрачає довіру»	149
63	«Зеленського хвилюють лише гроші»	160
69	«Він продовжує війну задля свого персонального збагачення»	213
85	«Свідчення про вживання наркотичних речовин»	95
94	«Режим зеленського збагачується на війні»	101
109	«Війна продовжується, щоб Київ продовжив отримувати Західні гроші»	95

Інша підгрупа також сфокусована на дискредитації, а також перекладенні провини за війну на Президента України, що відповідає підходу до дискредитації військово-політичного керівництва у внутрішніх документах АСП. У цій підгрупі 1,547 коментарів.

Таблиця 4.4. Теми підгрупи «Зеленський блокує мир»

Номер теми	Назва теми	Кількість документів
15	«Зеленський заборонив переговори»	400
51	«Він навмисно продовжує насилля»	176
75	«Йому все одно на людей»	251
81	«Режим Зеленського відмовляється від переговорів через гроші»	184
92	«Українці помирають за Зеленського, щоб він заробив»	118
113	«Перемир'я - єдиний вихід, а він його блокує»	317
115	«Він готовий знищити України, аби не домовлятись»	101

Загалом блок атаки на Президента Зеленського демонструє її спектр: від персональних атак до звинувачень у продовжені війни, відмови від миру та загалом дискредитації законності влади Президента України. Цей кластер тем демонструє, що Зеленський є однією з найголовніших цілей інформаційних атак росіян, адже левова частка коментарів спрямована саме на нього.

Наступним великим **кластером 2** є те, що можна охарактеризувати як «Провина Заходу», тобто фактичне звинувачення країн та організацій Заходу, включно з НАТО, ЄС та США, у війні та агресії проти РФ, а також у зовнішньому контролі над Україною, який «призвів» до вторгнення РФ в Україну. У цьому кластері простежується дві підгрупи тем. Разом вони складають масив у понад 4,000 коментарів.

Таблиця 4.5. Теми підгрупи «США та Захід навмисно затягують війну»

Номер теми	Назва теми	Кількість документів
6	«США навмисно продовжують війну через озброєння України»	446
35	«Поставки зброї від Заходу лише погіршують війну»	259
36	«США намагаються послабити РФ за допомогою України»	254
55	«США та союзники використовують Україну у власних інтересах»	168
64	«Війна не закінчиться поки Захід постачатиме зброю»	170
74	«США озброюють Україну й забороняють Зеленському вести переговори»	99
93	«Захід боїться ескалації та надсилає тільки застарілу зброю»	86
100	«Підтримка війни означає підтримку Заходу як ініціатора війни»	114

Як можна побачити з цієї підгрупи, коментарі та коментатори намагаються фреймувати війну та вторгнення РФ як щось, що було спричинене зовнішніми акторами,

намагаючись встановити інтерпретацію подій як великої змови Заходу, який веде проксі-війну з Російською Федерацією, та є фактично причиною її продовження.

Таблиця 4.6. Теми підгрупи «Україна - маріонетка Заходу»

Номер теми	**Назва теми**	**Кількість документів**
8	«5 мільярдів доларів було витрачено, щоб встановити маріонетковий режим»	575
12	«Україна є розмінною монетою для Заходу»	415
28	«Незалежність України це брехня, вона управляється кураторами»	344
59	«НАТО використовує Україну як зброю проти РФ»	209
71	«Захід планував зробити з Зеленського анти-Путіна, але він став терористом»	240

Ця підгрупа коментарів (Таблиця 4.6) фокусується на позбавленні агентності України як країни, яка має право на самозахист. Вона також підживлює тезу щодо нелегітимності Уряду України (що трохи перегукується з критикою Президента України), а також формує із Заходу образ ворога, який, до того ж, є головним винуватцем війни.

Варто відзначити, що коментарі з цього кластеру є часто повторюваними, тобто відповідають патернам автоматичного розповсюдження, а також були присвячені реальним подіям. Наприклад, тема «Незалежність України це брехня» сформована у

тому числі з 4 ідентичних коментарів, які формують порядок денний сприйняттям реального візиту Єврокомісарів до України 1 грудня 2024 року (EU Commission, 2024) як «десанту єврокомісарів з наказами для Зеленського» (переклад авторський). Тобто, ми спостерігаємо неавтентичне поширення однакових коментарів, які відповідають реальним подіям, таким чином підтверджуючи, що російські оператори дезінформаційних кампаній відслідковують події й коригують контент операцій відповідно до них.

Інша підгрупа у рамках цього кластеру фокусується на негативному зображенні перспектив України вступити до НАТО, що перегукується із кейсом реклам у Facebook, які було проаналізовано вище у рамках операції «Двійник».

Таблиця 4.7. Теми підгрупи «Україна не вступить до НАТО»

Номер теми	**Назва теми**	**Кількість документів**
19	«НАТО не хоче вступу України до альянсу, лише використовує її»	559
83	«Україна ніколи не стане частиною НАТО»	109

Наступним **кластером 3**, проаналізованим у рамках цього кейсу, є масив коментарів, які фреймують українців та українську ідентичність як «нацистську ідеологію». Це вкорінена теза російської дезінформації, яку факт-чекери постійно «розбивають» з 2014 року, відколи російські медіа почали зображати Революцію Гідності як «переворот», а Україну як «нацистську державу» (Romaniuk, 2024). У рамках цього кластеру проаналізовано близько 2,917 документів. Як видно з коментарів, російські актори продовжують фокусуватись на цій темі як виправданні вторгнення й політики РФ в цілому.

Таблиця 4.8. Теми підгрупи «Українці — нацисти»

Номер теми	Назва теми	Кількість документів
0	«Гасло ‘Слава Україні!’ є нацистським»	994
37	«Український націоналізм тотожний нацистській ідеології»	216
40	«Бандера — фашистський герой в Україні»	284
49	«Україна має відмовитись від націоналізму, щоб мати нормальне життя»	180

Таким чином ця група коментарів намагається покласти провину за війну та «ненормальне життя» на «націоналізм» українців, який до цього призвів, встановлюючи альтернативне пояснення вторгненню РФ та підштовхуючи до виправдання її дій.

Таблиця 4.9. Теми підгрупи «Заперечення української ідентичності»

Номер теми	Назва теми	Кількість документів
11	«Україні потрібен реальний українець на посту президента» (антисемітизм)	318
17	«Київська Русь належить РФ»	432
24	«Всі нації рівні, Україна не має бути	255

	над іншими»	
80	«Російська мова зазнає притискань в Україні»	238

Загалом цю групу можна охарактеризувати як спробу дезінформаційних акторів переписати історію та сформувати образ України та її влади як абсолютного зла через порівняння з нацизмом, при цьому використовуючи антисемітизм та експансіонізм. До того ж, тут є повторення тези про «русофобію» через притискання російської мови, що є класичним наративом з 2014 року.

Наступним **кластером 4**, який виявлено в рамках дослідження, є фреймування миру та припинення вогню. Він формує образ РФ як миротворця, що хоче миру, на відміну від України, що дещо перегукується з попередніми підгрупами, у яких критикували військово-політичне керівництво України та Захід. До того ж, він містить згадки про Мінські угоди як спосіб «виграти час». У цьому кластері зібрано 1,729 коментарів.

Таблиця 4.10. Теми підгрупи «Мир та вимоги щодо припинення вогню»

Номер теми	**Назва теми**	**Кількість документів**
2	«Припинення вогню та переговори потрібні вже зараз»	726
20	«Біженці могли б повернутись, якби Зеленський уклав угоду»	259
26	«Тільки русофоби хочуть продовження війни»	256
43	«Росія готова до переговорів, Київ	261

	не погоджується»	
21	«Захід використав Мінські угоди, щоб виграти час для України»	227

Ця підгрупа формує порядок денний того, що Росія готова до припинення вогню, але керівництво України не погоджується.

Кластером 5, зібраним для аналізу, є «Військові втрати, мобілізація та ядерна зброя», який об'єднує теми щодо обстрілів РФ території України, а також точкові повідомлення про втрати України та коментарі навколо висловів Президента Зеленського щодо ядерного арсеналу. Кластер складається з 2 підгруп, в яких понад 1,200 коментарів.

Таблиця 4.11. Теми підгрупи «Втрати та мобілізація»

Номер теми	**Назва теми**	**Кількість документів**
41	«Статистика загиблих занижена в Україні»	391
48	«Зеленський зрадив армію та зниження мобілізаційного віку до 18 років»	154
96	«ЗСУ чекає колапс й провал»	205
103	«Співробітники ТЦК жаліються на малу зарплату» в рамках «підвищення податків»	141

Ця підгрупа містить як оціночні судження й неправдиву статистику, так й іронію щодо ТЦК, зокрема у темі 103, яка містить 3 ідентичні коментарі з іронічною заявою про найбільший вклад ТЦК у перемогу й потребу більшої зарплати. Фінальна

підгрупа цього кластеру формує образ України як нестабільної країни, яка після отримання ядерної зброї (ЯЗ) знищить світ.

Таблиця 4.12. Теми підгрупи «Ядерні загрози та стримування»

Номер теми	Назва теми	Кількість документів
25	«Україна не має мати ядерної зброї»	258
88	«Якби Україна мала ЯЗ, Зеленський би її використав»	90

Фінальний **кластер 6** включає обговорення біженців та поділ України через включення до сусідніх країн. Перша підгрупа наративів стосується депопуляції України та налічує 1161 коментар.

Таблиця 4.13. Теми кластеру «Біженці та поділ України»

Номер теми	Назва теми	Кількість документів
31	«Захід сприяє депопуляції України»	371
54	«Україна має здатись, щоб спинити потік біженців з країни»	226
60	«Українські території будуть розділені»	564

Цей фінальний кластер спрямовує провину за «депопуляцію» України через втрати на війні та кількість біженців, які змушені покинути країну, на Захід та безпосередньо Україну, яка має погодитись на всі умови країни-агресорки, щоб зупинити війну та відтік громадян.

У цілому, аналіз тематичних підгруп наративів у рамках зібраних кластерів дозволяє побачити, що неавтентичні акаунти у соціальних мережах, які залишали

коментарі наприкінці листопада — на початку грудня 2024 року, дійсно активно перекладали провину за війну в Україні на кого завгодно, крім РФ. Головними винуватцями виступають країни Заходу, Президент Зеленський особисто, український націоналізм, неправильна історія тощо. Відтак, Гіпотеза 3 про те, що скоординована діяльність у коментарях у досліджуваному корпусі переважно реалізує стратегію перенесення відповідальності за війну з Російської Федерації на Україну та країни Заходу підтверджується. Зібраний масив коментарів тематично співвідноситься із задекларованими цілями операції впливу, про які ми знаємо з внутрішніх документів російських підрядників. Її метою є підмінити «порядок денний», наситити інформаційний простір суперечливими повідомленнями та сформувати альтернативне бачення подій для російських та українських користувачів соціальних мереж. Ці теми формують бачення світу через повторюваність, яка є однією із запорук довіри до інформації, незалежно від її джерела (Pennycook та Rand, 2021).

Щодо дискредитації військово-політичного керівництва, то проаналізований масив даних містить критику Зеленського та його «режиму», фіксуючи весь негатив на ньому, що є певним відходом від кампанії в ТікТок (Підрозділ 4.2), де під критику потрапляли всі рівні державної влади та адміністрацій, та від реклам операції «Двійник» (Підрозділ 4.1), де критикували військове керівництво й місцеву владу в цілому. На когнітивному рівні, таке повторення та постійне введення негативної інформації до порядку денного користувачів, навіть у вигляді шуму, впливає на користувачів та їх бачення світу. Це у свою чергу може призводити до зміни поведінки.

Ці скоординовані кампанії в коментарях охоплюють широку цільову аудиторію, яка чітко сегментована за географічною ознакою. В Україні коментарі насамперед спрямовані на підрив довіри до керівництва держави, підсилення внутрішніх розколів та поширення деморалізуючого контенту, що зображує опір РФ як марний. Ці публікації нерідко включають наративи про нібито корупцію, нецільове використання допомоги або сфабриковані дані про втрати на полі бою, експлуатуючи наявні суспільні дискусії для підриву морального духу та солідарності. Значна кількість коментарів також

цілеспрямовано розпалює ворожнечу між українцями. Наприклад, покладається провина за проблеми країни на самих українців, Президента Зеленського чи Захід, живлячи ширшу кремлівську стратегію психологічної дестабілізації на когнітивному рівні.

З іншого боку, в російському інформаційному просторі аналогічні тактики у коментарях слугують утверджувальним пропагандистським функціям. Публікації, як правило, схвалюють рішення російського уряду, легітимізують воєнний наратив через риторику «миротворчості» або «денацифікації» та демонізують Україну та її союзників як агресорів. Такі коментарі зміцнюють ідеологічний конформізм та відтворюють наративи державних медіа в партисипаторній формі, дозволяючи громадянам стикатися з урядовими тезами у нібито спонтанних, «породжених однолітками» обговореннях. Це дозволяє формувати картину світу, що відповідає інтересам Кремлівської верхівки, фактично ігноруючи реальність.

На технічному рівні такі операції проводяться за допомогою автоматизованого програмного забезпечення задля реєстрації облікових записів та публікації коментарів. Пошук та виявлення неавтентичних коментарів є складним завданням, особливо з розвитком моделей штучного інтелекту, які спростять процес переписування коментарів у майбутньому. Проте, на цей момент велика кількість коментарів є повторюваними, тобто віднайшовши підозрілий коментар потрібно проаналізувати обліковий запис, який його залишив та прослідкувати, чи залишав він схожі коментарі під публікаціями цього ж видання або сторінки. Найпростіше це зробити у мережі Twitter/X, зайшовши на сторінку профіля й проаналізувавши публікації та відповіді акаунта, які можуть бути як картинками, так й текстовими повідомленнями. В Telegram цей пошук можна зробити вручну, проаналізувавши коментарі на каналі, або ж зібравши масив даних, включно з коментарями, за допомогою спеціальних інструментів. Безпосередній пошук однакових коментарів варто виконувати через пошукову систему, наприклад Google, використовуючи підхід точної фрази, яка має бути в лапках, та зазначивши сайт платформи, на якій потрібно шукати. Таким чином можна віднайти публікації, під якими залишили однакові коментарі.

Щодо пошуку картинок, то це ускладнено закритістю платформ (Telegram та Facebook), але цілком можливо знайти реверсивним пошуком зображень однакові картинки на платформі Twitter/X.

4.4 Зв’язок між кампаніями та рекомендації з протидії

4.4.1 Зв’язок між трьома проаналізованими кейсами та атрибуція до стратегії РФ та документів АСП

Операція «Двійник» (Facebook): висока впевненість

Атрибуція виявлених рекламних повідомлень безпосередньо до операції «Двійник» (Doppelganger) та внутрішніх документів АСП і стратегії РФ спирається на кілька незалежних доказів. По-перше, це використання підозрілих посилань, які фільтрують трафік через систему Keitaro за IP-адресою. Тобто, ці посилання підміняють зовнішній вигляд сторінки, якщо запит надходить з IP-адреси поза країною-ціллю (Châtelet and Osadchuk, 2024; Qurium Media Foundation, 2022; скриншот *Sights of Sintra_5* з власного архіву). По-друге, специфічні патерни назв сторінок-одноденок, які були реконструйовані у Підрозділі 4.1, відповідають попереднім ітераціям операції та дослідженням цієї теми (Alaphilippe et al., 2022; Nimmo and Torrey, 2022). По-третє, це використання клонів реальних українських новинних видань (наприклад, РБК-Україна) для розповсюдження негативного контенту. По-четверте, це виявлений автором збіг меметичного матеріалу між рекламним каналом операції «Двійник» та координованою кампанією у коментарях, яку вела АСП, задокументованою у внутрішніх документах Центру «С» (Рисунок 3.25; Department of Justice, 2024a; Martin Laine [@Martinlaineolen], 2024). Додатково про це описано далі у цьому підрозділі. Сукупність цих чотирьох ознак надає атрибуції високий рівень впевненості у зв’язку з АСП та, як наслідок, зі стратегією інформаційних операцій РФ..

Кросплатформна TikTok-операція: середньо-висока впевненість

Атрибуція TikTok-кампанії до операторів АСП/Структури спирається на три типи доказів. По-перше, поява одного з документованих автором у цій кампанії відеосюжетів

безпосередньо на дашборді Центру «С», опублікованому у зливі документів (Belton et al., 2024a). Цей доказ є фактично найґрунтовнішим і виводить атрибуцію до АСП за межі низької впевненості. По-друге, це використання типових наративних ліній у відео, які повторюються з усталеними кремлівськими тропами щодо «корупції українського військово-політичного керівництва», задокументованими у внутрішніх документах АСП. По-третє, це використання зображень російського походження, які є нетиповими для використання поза РФ. Водночас цей кейс не має технічних артефактів, як операція «Двійник», що зумовлює помірне зниження впевненості до рівня середньо-високої.

Координовані кампанії у коментарях (Telegram, X, Facebook): змішана атрибуція

Цей кейс вимагає окремого розрізнення між атрибуцією координованої неавтентичної поведінки та атрибуцією прямої інституційної належності конкретних облікових записів до АСП/Структури. Щодо координованого характеру виявленої активності у коментарях, то у цьому дослідженні фіксуються типові ознаки такої поведінки, зокрема, повторюваність текстів, часова синхронність публікацій, патерни циклічного розміщення меметичного контенту тощо. Сукупність цих ознак та їхня тематична узгодженість із цілями, зафіксованими в афідевіті Міністерства юстиції США (Department of Justice, 2024a, Додаток 6A, с.150), забезпечують середній рівень впевненості у тому, що це координована кампанія впливу російського походження.

Щодо інституційної належності всіх та кожного облікового запису, який було проаналізовано, саме до АСП, то наявних доказів недостатньо для високого рівня впевненості. Відсутність артефактів не дає змоги ідентифікувати операторів конкретних мереж із впевненістю. Альтернативні пояснення, як-от наявність інших російських проксі-акторів або локальних проросійських активістів, що добровільно реплікують меметичний матеріал, не можуть бути виключені у межах цієї роботи. Відповідно, пряма атрибуція коментарів саме до АСП оцінюється на рівні низької впевненості.

Попри це, зв’язок між операцією «Двійник» та координованою кампанією у коментарях через спільний меметичний актив фіксується з високою впевненістю, адже це пряма контентна ланка. Зв’язок між документами АСП та TikTok-кампанією через

присутність одного з відеосюжетів на дашборді Центру «С» фіксується з високою впевненістю. Спільне інституційне керівництво всіма трьома кампаніями з боку єдиного консорціуму АСП–Структура оцінюється з середньою впевненістю, адже воно є найбільш узгодженим поясненням всієї сукупності виявлених фактів й відповідає проаналізованій документації та структурі роботи АСП. Однак, часткові альтернативи на рівні окремих компонентів (зокрема, для кейсу коментарів) не можуть бути остаточно відкинуті в межах цього дослідження.

Зазвичай зв'язок між різними частинами однієї операції треба будувати через поведінку й спільні тактики, техніки та процедури. Атрибуція цих трьох, на перший погляд, різних операцій до російських організацій, пов'язаних з Кремлем, як «Агентство соціального проєктування» (АСП) та Група компаній «Структура», була встановлена за допомогою кількох незалежних джерел на різних рівнях впевненості. Внутрішні документи АСП були включені до афідевіту Міністерства юстиції США, в рамках чого оприлюднені плани РФ щодо систематичного розміщення коментарів у соціальних мережах, конкретизуючи цілі, теми повідомлень і показники ефективності (Justice Department, 2024a). Додаткові розслідування журналістів (Morozova and Laine, 2024) опублікували витяги з внутрішніх електронних таблиць АСП, що розкривають шаблони виробництва коментарів та інструкції з координації для персоналу, а публікації The Washington Post (Belton et al., 2024a) продемонстрували дашборд, в якому росіяни вимірюють успіх дезінформаційних кампаній в кількох вимірах. Ці матеріали в сукупності підтверджують, що маніпулювання інформаційним простором України та інших країн становило невід'ємну частину ширшої стратегії дезінформаційного впливу РФ.

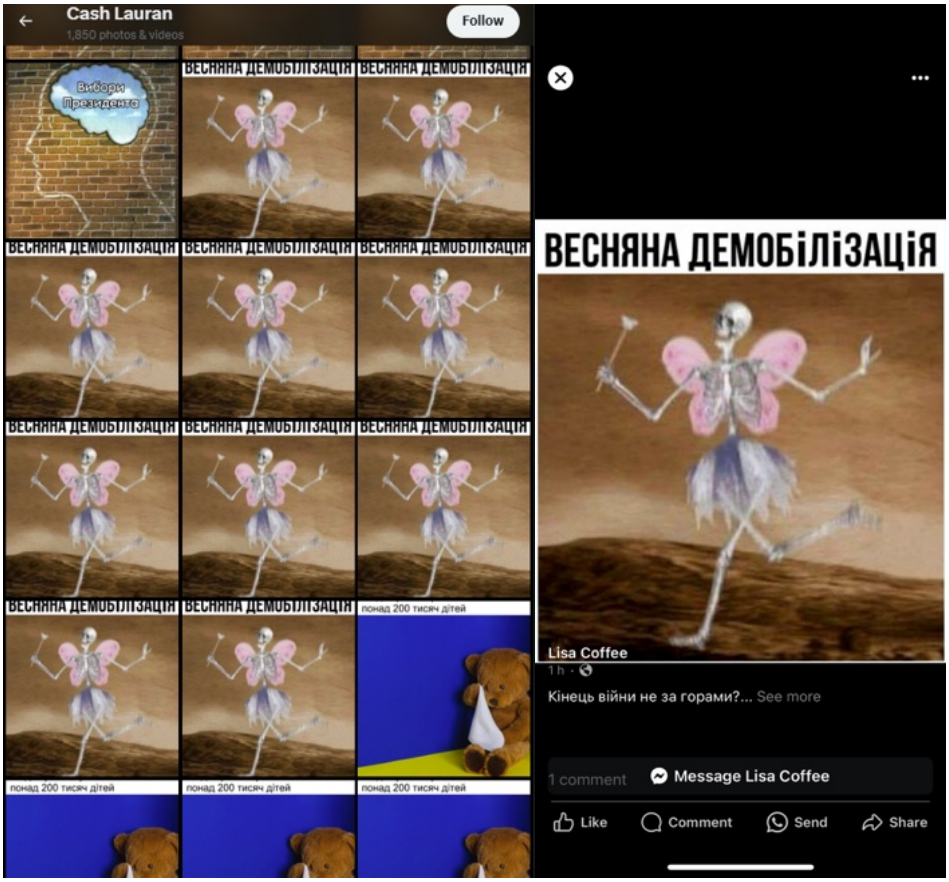
Разом з цим, усі три кампанії демонструють різні техніки та тактики впливу на суспільну думку іноземної аудиторії, вірогідно з боку російських структур АСП і Структура. Ці приклади є репрезентацією частини сучасних інформаційних операцій, але не можуть охопити весь простір й масштаб всіх таких операцій. Ці кампанії, попри зовнішні відмінності, мають спільні цілі: «послабити українське суспільство», «сіяти

напруженість» та «зменшити обсяг допомоги Україні» тощо. Ці цілі є наскрізною темою і підґрунтям кампаній, що виражено у Додатку 6А афідевіту (Department of Justice, 2024a, с.150), який містить список таких задекларованих цілей росіян, як «дискредитація військово-політичного керівництва», «розкол еліт», «деморалізація ЗСУ» та «дезорганізація населення». Було встановлено, що у трьох проаналізованих у цьому дослідженні прикладів основними пріоритетами операцій були всі зазначені вище цілі, окрім «розколу еліт», яка була менш виражена або ж була доповненням до цілі «дискредитації керівництва». Тобто, між трьома проаналізованими кампаніями є, як мінімум, тематичний зв'язок.

Варто зазначити, що проведений аналіз встановив зв'язок операцій з російськими операторами не тільки через спільні цілі та інтереси, а й підтвердження й перетин з опублікованими документами. Найтісніший зв'язок було встановлено щодо операції на платформі ТікТок, де один із задокументованих кейсів фактично з'явився на дашборді Центру «С». Щодо інших операцій, то належність рекламних повідомлень у Facebook до публікацій операції «Двійник» доведено використанням тих самих інфраструктурних підходів, тобто сторінок-одноденок, які мають чіткі патерни імен, схожий візуальний стиль, та, найголовніше, переводили своїх користувачів на сайти, які використовували підроблені версії реальних медіа (РБК Україна) або на інші сторінки у разі детекції іноземної IP-адреси користувача (geofencing).

Однак, коментарі є найскладнішою ланкою доведення через свою складність пошуку по платформах та відсутність інформації про облікові записи, які можуть створюватись сотнями й так само легко видалятись. Проте, повторюваність коментарів та відкрита декларація того, що коментарі є основним інструментом розповсюдження контенту (мемів та текстів) у внутрішніх документах Центру «С», а також масштаб зібраних через платформу O'Savul коментарів неавтентичних користувачів, їхня повторюваність та тематична схожість принаймні частково дозволяють ці операції пов'язати між собою.

Більше того, автору вдалось віднайти додатковий зв’язок між кампаніями через контент. Так, обліковий запис одного з коментаторів, який був у внутрішніх документах, які опублікував естонський журналіст (Martin Laine [@Martinlaineolen], 2024), використовував меми для коментування під публікаціями відомих українських медіа та публічних персон. Більше того, як продемонстровано на прикладі нижче, автор знайшов використання одного й того самого мему у операції «Двійник» та у коментарях цього профілю, що доводить зв’язки між операторами, або, принаймні, вказує на типову базу контенту для розповсюдження. Об’єднання різних типів контенту та операцій, як всередині РФ, так і в Україні та країнах Заходу, було пізніше підтверджене розкритими документами, у яких згадувалась спільна робота кількох організацій як єдиного цілого, попри різну реєстрацію (Pamment and Tsurtsumia, 2025, с.20).



Зображення 4.25. Колаж з публікації у Twitter/X від неавтичного акаунту, який був вказаний у документах Центру «С» (зліва) та публікація рекламного повідомлення Операції «Двійник» (справа) (з особистого архіву)

4.4.2 Контрзаходи на технічному (інфраструктурному) рівні

Виявлені у підрозділах 4.1–4.3 характеристики трьох сучасних російських інформаційних операцій формують емпіричну основу для формулювання рекомендацій з протидії, які спираються на конкретний матеріал виявлених кейсів. Ці рекомендації упорядковано в рамках трирівневої аналітичної рамки дослідження.

Технологічний рівень представлений кількома аспектами проаналізованих операцій. По-перше, систематичним використанням фільтрації трафіку згідно з локацією користувача через систему Keitaro у кейсі «Двійник». По-друге, залучення специфічних патернів іменування ефемерних сторінок-одноденок для розповсюдження контенту. По-третє, систематична мімікрія російських акторів під домени українських новинних видань. Насамкінець, задокументована у TikTok-кейсі та коментарях кросплатформна дифузія. Ці елементи технічного підходу до розповсюдження та введення в оману дозволяють сформулювати контрзаходи на цьому рівні для технологічних платформ і державних регуляторів.

Для технологічних платформ

Виявлене використання фільтрування по геолокації та клоакінгу, тобто приховування контенту від документації, вказує на потребу у впровадженні автоматизованого виявлення цього методу обходу алгоритму як критерію автоматичної модерації реклами. Така технічна інфраструктура для виявлення подібних розбіжностей вже існує у продуктах самих платформ і зазвичай використовується для боротьби з рекламним шахрайством та зловмисним програмним забезпеченням. Її розширення на детекцію клоакінгу політичної реклами є переважно питанням пріоритету. До того ж, більш ефективний алгоритм виявлення політичної реклами, коли вона прихована, був би допоміжним сигналом для реагування.

На рівні бібліотеки реклами потрібна обов’язкова публікація інформації про геотаргетинг та обсяги витрат у розрізі країн, що вже відбувається в країнах ЄС й відповідає логіці Регламенту Європейського Союзу про цифрові послуги (Digital Services Act). Цей підхід має розширитися на всі країни. До того, варто запровадити

зберігання реклами, яка часто видаляється безслідно. Без цього зрізу даних дослідницькі команди змушені відтворювати таргетинг емпірично, методом покрокового огляду стрічки, як це й робилося у цій дисертації. Такий підхід хоча й має результати, проте є несистематичним й менш повним, ніж пряме розкриття даних платформою.

Важливим кроком є API-доступ для дослідників, що уможливить незалежний моніторинг рекламних бібліотек і стрічок без необхідності ручного збирання та скриншотування. Виявлений у TikTok-кейсі патерн міжплатформної дифузії може отримати протидію у вигляді проактивного обміну індикаторами операцій між різними платформами. На зразок того, який існує в сфері кібербезпеки щодо класичних кіберзагроз. У сучасних інформаційних операціях, коли контент розповсюджується крос-платформно, жодна платформа не бачить повної картини, а обмін індикаторами є необхідним для системного реагування.

Для державних інституцій

Важливим кроком є впровадження постійного моніторингу рекламних бібліотек у межах аналітичних підрозділів із виявленням операцій іноземного впливу. Наразі такий моніторинг проводиться неурядовими організаціями в Україні й частково реалізується в межах діяльності Центру протидії дезінформації при РНБО. Проте, між цими акторами немає повноцінної співпраці та стандартизованого обміну інформацією (Kalenský and Osadchuk, 2024). До того ж, необхідним є розвиток українського аналога DSA чи інтеграції до документу ЄС, що сприятиме підвищенню прозорості рекламних бібліотек і дослідницького доступу. Розширення режиму санкцій проти юридичних і фізичних осіб, пов’язаних з виявленими операціями, є необхідним заходом протидії для зменшення впливу шкідливих акторів. Технічні артефакти, як-от доменна інфраструктура чи фінансові транзакції рекламодавців, є доказовою базою для розширення санкційних рішень України та її союзників. Санкції як інструмент є четвертою лінією оборони у концепції Каленського і Ганхіярві (Kalenský and Hanhijärvi, 2025), яка орієнтована на підвищення витрат для шкідливих акторів у проведенні такої діяльності.

Для дослідницької спільноти

Допоміжним інструментом може стати стандартизація методології документування ефемерного контенту як стандартної процедури роботи з рекламою та іншими операціями. Узгодження формату архівації виявлених кампаній може забезпечити накопичення зусиль різних дослідницьких команд і їхню комплементарність. Агрегація таких даних може бути допоміжною для подальших санкцій чи удосконалення методів детекції інфраструктури інформаційних операцій.

4.4.3 Контрзаходи на наративному (контентному) рівні

Сім наративних кластерів, індуктивно виявлених у комп'ютеризованому аналізі координованих коментарів (Підрозділ 4.3) у поєднанні з наративною структурою рекламних повідомлень операції «Двійник» (мобілізаційний, корупційний, антизахідний кластери) формують емпіричну основу для формулювання можливих наративних контрзаходів. Принциповий підхід полягає в тому, що ефективна протидія на цьому рівні має фокусуватися саме на цих ідентифікованих структурних кластерах, а не на реактивному реагуванні на окремі дезінформаційні твердження. Важливо зазначити, що протидія не може спиратись виключно на контртвердженнях чи пре-банкінг,у а має включати реальні дії та політичні рішення, які не можливо виконати виключно комунікацією.

Для аналітичних центрів і факт-чекінгових організацій

Ці організації мають здійснювати систематичний моніторинг визначених кластерів у документах АСП та цій роботі, публікуючи регулярні аналітичні звіти. Важливим є те, що ці звіти мають вийти за межі виключно аналітичних організацій й бути підхоплені медіа для широкого розповсюдження. Ці звіти мають демонструвати системність і структурність наративів, які використовує РФ як частину своєї стратегії. Українські факт-чекінгові та неурядові організації (IREX, 2024; Romanuk and Fedchenko, 2025) вже мають інституційну спроможність для проведення глибинного аналізу інформаційного простору та впровадження цих досліджень у програми з медійної

грамотності. Методологічним внеском цієї дисертації є апробація та презентація відтворюваного інструменту (BERTopic-підходу з векторами кількома мовами). Цей інструмент уможливлює продовження виявлення нових кластерів у міру їхньої появи у інформаційному просторі без необхідності попередньої таксономії. Організації з дослідження дезінформації та інформаційних операцій мають впровадити використання DISARM-таксономії (Terp and Breuer, 2022). Включення цієї рамки в публікації українських організацій дозволить агрегувати їхні спостереження в спільну аналітичну базу разом з європейськими партнерами та організаціями.

Обмеження факт-чекінгу як окремої стратегії задокументовані та визначають, що верифікація потребує більше ресурсів, ніж створення дезінформації; те, що аудиторія факт-чекінгу систематично відрізняється від аудиторії дезінформації (Guess et al., 2020); а також, що професійна перевірка фактів має меншу аудиторію та, по суті, є реактивною (Westlund, 2024). Проте в українському контексті фактчекінгові організації функціонують не лише як інструмент верифікації та спростування неправдивої інформації. Вони фактично є інституційними стовпами журналістських стандартів та системи освіти журналістики (Romanuk and Fedchenko, 2025), які готують нове покоління журналістів, що протидіятимуть російським інформаційним операціям. Це робить такі організації важливими для стратегічної стійкості України.

Для державних інституцій стратегічних комунікацій

Необхідним Державні інституції мають розробити проактивні кампанії з пребанкінгу, орієнтовані на споживачів ідентифікованих кластерів реклами та тематичних цілей впливу РФ. Експериментальні дослідження інокуляційного підходу свідчать, що попереджувальне ознайомлення аудиторії з типовими маніпулятивними техніками є ефективним методом протидії. Особливо якщо це порівняти з виключно реактивним спростуванням (van der Linden et al., 2017; Roozenbeek and van der Linden, 2022). Виявлені у роботі наративні кластери є темами для сценаріїв пребанкінгових інтервенцій у стратегічних комунікаціях державних органів. Враховуючи, що нам відомо заздалегідь, які саме фрейми будуть експлуатуватися російськими акторами

(наприклад, фрейм «провини Заходу за продовження війни», який неминуче активується у періоди мирних переговорів), це дає можливість підготувати когнітивне щеплення.

Незважаючи на переваги пребанкінгу, дослідження останніх років переглянули висновки щодо зворотного ефекту реактивного спростування (Wood and Porter, 2019; Ecker et al., 2022). Вони зафіксували, що ефект бумеранга, тобто поглиблення довіри до неправдивої інформації через факт-чекінг, за допомогою якого дискредитували факт-чекінг як метод, не є стабільним явищем за нормальних умов. Таким чином, дебанкінг має використовуватись як невід'ємна, хоча й недостатня сама по собі, частина наративної протидії. Державні інституції зі стратегічних комунікацій мають поєднувати дебанкінг з проактивним пребанкінгом за моделлю кількох ліній захисту, описаною Каленським та Ганхіярві (Kalenský and Hanhijärvi, 2025).

Для медіа та платформ

Платформи мають ширше інтегрувати факт-чекінгові результати у стрічку новин користувачів задля превенції поширення неправдивої інформації. Це може бути зроблено шляхом масштабного впровадження системи попереджувальних міток, що корелюють зі структурою кластерів з цієї роботи. Експериментальне дослідження Pennycook та ін. свідчить, що мінімальне когнітивне втручання, а саме пропозиція оцінити точність матеріалу перед поширенням, суттєво зменшує вірогідність розповсюдження неправдивого контенту. Цей ефект не залежить від політичних уподобань аудиторії (Pennycook et al., 2021). Системне розширення таких міток, яке вже існує в рамках роботи StopFake в Україні, у соціальних медіа є відносно простим та масштабованим контрзаходом.

Водночас слід враховувати ризик ефекту «імпліцитного консенсусу», за якого відсутність маркування контенту підвищує довіру до неперевіреного матеріалу (Clayton et al., 2020). Тобто, за таких умов, якщо якийсь матеріал не опрацьовано, він може сприйматись як правдивий через відсутність маркування. Це передбачає те, що повнота охоплення системи маркування є не менш важливою, ніж точність окремих міток.

Для системи освіти та ГО

Для освітніх інституцій важливим є включення актуальних прикладів інформаційних операцій до програм із підвищення медійної грамотності. Приклади, проаналізовані в цій дисертації, можуть поповнити ці програми для вивчення структурних рис російських наративів. Загалом інтеграція факт-чекінгової діяльності в систему вищої освіти є важливим аспектом підвищення інформаційної грамотності. В Україні діє проєкт StopFake у Національному університеті «Києво-Могилянська академія», який інтегрує факт-чекінг у систему підготовки журналістів (Romanuk and Fedchenko, 2025). Це дозволяє, на додачу до класичної академічної підготовки журналістів, додавати практичний досвід. Такий підхід виходить за межі тимчасового впливу окремих інтервенцій і вбудовує медіаграмотність в інституційну складову професії журналіста. Схожі підходи можна впроваджувати на факультетах психології задля побудови систем пребанкінгу. В цілому курси з медійної та інформаційної грамотності, а також розуміння системних інформаційних загроз з боку державних акторів (РФ та інших) можуть стати в пригоді студентам усіх спеціальностей.

4.4.4 Контрзаходи на когнітивному (психологічному) рівні

Усі три кейси продемонстрували такі характеристики, як емоційна насиченість контенту, створення образу ворога всередині країни через логіку «ми проти них». До того ж, всі три операції повторювали ключові повідомлення через множинні канали та намагалися вдавати вигляд автентичних джерел і голосів. Ці тактики є досить ефективними та використовують відомі психологічні вразливості людського мислення, що було описано у психологічній літературі (Lewandowsky et al., 2012; Pennycook and Rand, 2021; Ecker et al., 2022). Проаналізовані операції та внутрішні документи АСП підтверджують експлуатацію когнітивних механізмів операторами дезінформаційних операцій. Вони використовують повторення, затоплюють інформаційний простір суперечливими повідомленнями й створюють альтернативний порядок денний (Department of Justice, 2024a; Pamment and Tsurtsumia, 2025).

Як зазначено в обмеженнях дослідження (Підрозділ 2.3), пряме емпіричне вимірювання когнітивного ефекту описаних російських операцій впливу на українську аудиторію виходить за межі цієї дисертації. Відповідно, рекомендації на цьому рівні спираються на (а) релевантну психологічну літературу, (б) виявлену у трьох кейсах структуру повідомлень, (в) реконструкцію інтенцій операторів на основі документів та виявлених повідомлень. Безпосереднє експериментальне підтвердження ефективності цих рекомендацій є самостійним напрямком подальших академічних досліджень.

Інокуляційна інфраструктура

Для побудови системної стійкості українського суспільства потрібно масштабне розгортання інфраструктури інокуляції. Це може бути створенням серії коротких відеоматеріалів, інтерактивних веб-додатків та шкільних модулів, які були б побудовані за протоколами «теорії щеплення» (McGuire, 1964; van der Linden et al., 2017). Важливим елементом цього була б адаптація вже існуючих іноземних програм для української аудиторії з урахуванням проаналізованих російських операцій. Наприклад, гра «Bad News», яка була емпірично валідована в міжнародних дослідженнях, може бути корисною для українського досвіду (Roozenbeek and van der Linden, 2022). Українська адаптація має орієнтуватися на конкретні маніпулятивні техніки, виявлені українськими дослідниками в операціях стратегії РФ, а також ті, які були виявлені у дисертації. А саме, на фальшиву атрибуцію дій та цитат українським урядовцям (ТікТок-кейс та операція «Двійник»), мімікрія під автентичні новинні видання (операція «Двійник»), спекулятивна корупційна звинувачувальна риторика без фактологічної основи (TikTok-кейс), повторення емоційно зарядженого матеріалу через мережу неавтентичних акаунтів (мережа коментарів).

Принципове обмеження когнітивних інтервенцій

Варто зважати на те, що в ідеологічно поляризованих сегментах аудиторії такі когнітивні інтервенції можуть стикатися з ефектами вмотивованого мислення (Walter et al., 2020). Це означає, що для частини цільової аудиторії ці рекомендації та інструменти не дадуть бажаного ефекту. Його можна досягти виключно через комбінацію втручань

на технічному та наративному рівнях, на додачу до когнітивного. Таким чином, когнітивний рівень контрзаходів є необхідним, але недостатнім. Найкраще він працює у синергії з іншими рівнями, а не як ізольований інструмент втручання для протидії.

4.4.5 Координаційно-інституційна архітектура протидії

Виявлений у трьох кейсах факт ймовірно спільного інституційного походження емпірично відмінних кампаній доводить необхідність координації між акторами, які займаються протидією. Жоден ізольований суб'єкт (державні органи, окрема платформа, аналітичний центр чи факт-чекінгова організація тощо) не бачить повної картини інформаційних операцій. Це наштовхує на думку, що розподілена координація є необхідною для ефективної протидії.

Внутрішньонаціональна координація

Для зміцнення когнітивної безпеки країни доцільним є запровадження координації між Центром протидії дезінформації при РНБО, Центром стратегічних комунікацій та провідними приватними та неурядовими організаціями (StopFake, VoxCheck, Детектор Медіа та ін.). Ця координація може включати регулярний обмін знахідками та індикаторами проаналізованих операцій. У 2023 році Kalenský та Osadchuk (2024) провели інтерв'ю з 22 фахівцями з державного, приватного та неурядового секторів України для того, щоб виділити основні уроки української протидії російським інформаційним операціям. Головним висновком дослідників стала думка, що моніторинг інформаційного простору, пребанкінг, спростування й викриття дезінформації мають здійснюватися спільно як необхідний мінімум. Це має передбачати залучення громадянського суспільства та приватного сектора як рівноправних партнерів у протидії російським інформаційним операціям. Запропонована трирівнева аналітична рамка може використовуватися як концептуальна сполука, що об'єднує журналістські, безпекові, академічні та платформні традиції в межах спільного аналітичного словника.

Транснаціональна кооперація

Для підвищення ефективності протидії інформаційним операціям РФ наріжним є обмін даними досліджень між українськими інституціями та союзними структурами моніторингу й протидії. Серед потенційних організацій-партнерів є Центр стратегічних комунікацій НАТО (StratCom CoE) та Європейська служба зовнішніх дій (EEAS). Причому це має бути співпраця між рівними, де б українські організації виступали донорами експертизи, з огляду на унікальну українську інституційну спадщину протидії російським операціям, накопичену з 2014 року. Український досвід є цінним публічним благом для євроатлантичного співтовариства, оскільки країни Заходу перебувають в умовах посилення гібридних та FIMI-операцій проти них з боку РФ та інших шкідливих акторів. ЄС вже має існуючу концепцію реагування на загрози FIMI-ISAC та впроваджує до використання рамку для документації інцидентів DISARM. Ці елементи закладають інституційну основу й технологію взаємодії між розрізненими акторами. Вони дозволять українським структурам бути рівноправними учасниками мережі обміну даними про інциденти за умови їх використання. (EEAS, 2023; EEAS, 2024; EEAS, 2025; EEAS, 2026).

Стандартизована аналітична мова

У той же час координація неможлива, поки організації не будуть використовувати спільну аналітичну мову, яка може об’єднати різні аналітичні традиції та підходи. Запропонована у дисертації трирівнева рамка може функціонувати як концептуальний підхід вищого рівня, доповненням якого на рівні інструментального документування є DISARM-таксономія (Terp and Breuer, 2022), що забезпечує операційне документування конкретних тактик, технік і процедур. Системне використання DISARM у звітності українських державних центрів, аналітичних інституцій та неурядових організацій уможливить агрегацію спостережень за моделлю FIMI-ISAC. Без цього переходу розрізнені звіти про окремі інциденти не перетворюються на системне знання про закономірності, що є великою проблемою координації для протидії (EEAS, 2026).

Виявлені у трьох проаналізованих кейсах характеристики сучасних російських інформаційних операцій хоч і демонструють різні техніки, але мають схожий

інтегрований інституційний характер, кросплатформну архітектуру та наративну структурованість довкола порівняно стійкого набору кластерів наративів. Для ефективної протидії таким операціям треба використовувати багаторівневу й скоординовану протидію, в якій технічні, наративні та когнітивні заходи доповнюють одне одного, а не конкурують між собою, працюючи в синергії. Жоден окремо взятий інструмент (спростування неправдивої інформації, інокуляція, модерація платформ, санкційні механізми чи освітні програми) не є самодостатнім для вирішення проблеми. Натомість побудова адаптивної екосистеми протидії передбачає узгоджене розгортання всіх вищезазначених рівнів разом з регулярним оновленням, у разі оновлення тактик, технік та процедур шкідливих акторів та інформаційних операцій.

Стійкість російських кампаній крізь декади підкреслює, що інформаційна війна є не епізодичною, а радше структурною та безперервною. Зважаючи на проаналізовані доктринальні документи, інформаційна війна з боку РФ, ймовірно, триватиме та еволюціонуватиме доти, доки інформаційні екосистеми залишатимуться відкритими. Саме тому довгострокові контрзаходи мають зосереджуватися на кількох рівнях і будувати систему гнучкої суспільної стійкості. Вона має бути системою, яка передбачатиме довгострокові цілі й адаптуватиметься до нових загроз. Такий підхід передбачає зміцнення цифрової грамотності, розвиток критичного мислення та впровадження медіаосвіти в публічних інституціях і навчальних програмах задля «щеплення» громадян від маніпуляцій РФ чи інших агресивних країн.

ВИСНОВКИ

Систематизовано **теоретико-методологічні підходи**, які засвідчили що сучасні студії інформаційних операцій розвиваються на перетині кількох підходів та шкіл. По-перше, теорії пропаганди (Lasswell, Ellul) та концепції стратегічних наративів (Miskimmon), які є основами для формування повідомлень. По-друге, теорії рефлексивного контролю (Thomas), доктрини активних заходів (Rid) та інформаційного протиборства демонструють розуміння інформаційного домену для боротьби військовими РФ. Насамкінець, моделі координованої неавтентичної поведінки (Nimmo, DiResta) демонструють способи масштабної доставки контенту до нових аудиторій через коментарі та рекламу у соціальних платформах. Встановлено, що домінуюча проблема цього поля — аналітична фрагментарність між таксономічними, історичними, емпіричними та когнітивними вимірами. Вона створює потребу в інтегрованому інструментарії, здатному охопити інформаційну операцію як цілісну систему зі сталою історією, доктринальною основою та структурною складністю підрядних та державних організацій. Цю потребу в дисертації було задоволено шляхом розробки та застосування трирівневої аналітичної рамки.

Наявний методологічний інструментарій дослідження російських інформаційних впливів засвідчив його структурну фрагментарність. Технічно орієнтовані рамки (DISARM, ABC) ефективно описують окремі операційні тактики, проте не охоплюють наративного та когнітивного вимірів. У той же час наративні підходи опрацьовують зміст повідомлень у відриві від інфраструктурного контексту їхньої доставки. У свою чергу, когнітивно-психологічні дослідження зосереджуються на ефектах, але рідко простежують їхній зв’язок із технічними та наративними рішеннями операторів. Цей розрив обґрунтовує потребу в *інтегрованій трирівневій аналітичній рамці*, що системно поєднує технічний (інфраструктура, механізми доставки), наративний (стратегічні наративи, фреймінг, інформаційне відмивання) та когнітивний (психологічні вразливості, рефлексивний контроль) рівні аналізу. Запропонована рамка інтегрує

наявні стандарти у спільному аналітичному просторі, де технічні події ABC/DISARM є виявом наративних стратегій і когнітивних цілей.

Обґрунтована в дисертації методологія дослідження поєднує якісне порівняння стратегічних документів (витоки АСП і Структура) з кейс-стаді трьох документально зафіксованих операцій як емпіричного прояву стратегії. Кожен кейс-стаді мав свій метод дослідження, включаючи методи розвідки відкритих даних, комп'ютеризованого кластерного аналізу масиву даних задля документації й порівняння різних інформаційних операцій. Кожен кейс було розглянуто крізь призму трирівневої аналітичної рамки як інструмент послідовного зчитування реалізації стратегії в технічному, наративному та когнітивному вимірах. Ця методологічна архітектура забезпечує валідацію, адже документальний рівень демонструє задум, а рівень кейсів — практичну реалізацію цієї стратегії в реальних умовах платформ соціальних мереж.

Історична реконструкція інституційних і доктринальних витоків сучасних російських інформаційних операцій засвідчила прямі лінії спадковості між інфраструктурою Служби «А» Першого головного управління КДБ СРСР, що відповідала за активні заходи в період Холодної війни, та сучасними операторами впливу — АСП, Структурою та іншими. У роботі простежено перехід від «активних заходів» до системи державного іноземного мовлення у вигляді RT та Sputnik, які, у свою чергу, застосовували метод «потоку брехні» для перенасичення інформаційного простору неправдивою інформацією й техніку інформаційного відмивання для поширення свого контенту в інших виданнях. Також зафіксовано необхідність переходу в онлайн для здійснення інформаційних операцій після блокування основних видань РФ у ЄС, що й призвело до активності сучасних підрядників ІО.

Виокремлення еволюції державної та недержавної протидії інформаційним операціям засвідчило формування багаторівневої екосистеми відповіді на загрозу. Було виділено 4 періоди розвитку протидії, від перших кроків то глибинної інституціоналізації відповіді. Ця відповідь відбувається одразу на державному, неурядовому та наднаціональному рівні. Наприклад, в Україні державу представляють

Центр протидії дезінформації при РНБО, Центр стратегічних комунікацій та інформаційної безпеки, а на неурядовому — StopFake, VoxCheck, ГО «Детектор медіа», тощо. Існує також важливий наднаціональний рівень, що існує навколо НАТО та ЄС. Перевагами наявної системи відповіді є динамічність розвитку, різносторонність учасників та міжнародна координація. Недоліком є те, що система відповіді є «молодшою» й структурно більш фрагментованою, ніж операції РФ, які спираються на довгу традицію розвитку. По-друге, спільна аналітична рамка та спільне бачення протидії лише формуються й намагаються інтегрувати різні традиції у єдине бачення. У той же час, було виокремлено системну еволюцію офіційного бачення інформаційного протиборства РФ на основі доктринальних документів інформаційної безпеки Російської Федерації. Виділено 5 періодів розвитку російських документів, від введення «інформаційної безпеки» як частини концепії оборони (1997 р.) до інституціоналізації інформаційного протиборства й інтеграції приватних підрядників для проведення інформаційних операцій. Це делегування не означає виключення координації та контролю з боку Адміністрації Президента РФ. До того ж, простежено системність підходу — від ситуативних інформаційно-психологічних операцій до інтегрованого комплексу контр-дій, тобто визначення будь-яких наступальних операцій як «захист суверенітету РФ та багатополярності світу».

Реконструкція стратегічного рівня російських інформаційних операцій проти України після 2022 року на основі внутрішньої документації АСП і Структури дозволила виокремити ключові цілі цього впливу. Серед цих цілей — *ослаблення суспільної згуртованості українців* і *підрив довіри населення до військово-політичного керівництва.* Інша ж мета полягає у *зменшенні військової і фінансової допомоги Україні з боку Заходу* через поширення втоми та дискредитації України у країнах-донорах. З російської документації випливає перехід до індустріального рівня планування операцій із квотами за типом контенту. Документи АСП демонструють індустріальний характер планування, в якому присутні цільові показники охоплення, цільові аудиторії тощо. До того ж, структура організацій побудована як повноцінна структура для проведення

інформаційних операцій, маючи 4 рівні: моніторинговий, аналітичний, виробничий та рівень розповсюдження. Внутрішня логіка стратегії побудована за принципом *комплексних контркампаній*, де окремі тактики (як-от «Двійник») є лише компонентами ширшої операційної архітектури.

Кейс операції «Двійник» (Doppelganger) у Facebook. Проведено структурування унікального авторського корпусу 649 скриншотів повідомлень операції в українському сегменті Facebook. Зібраний корпус зафіксував систематичну спрямованість операції на деморалізацію населення України. Вона відбувалася через поєднання кількох наративних кластерів, які можна узагальнити в логіку підриву довіри до державних інституцій і міжнародних союзників України. Було виявлено та описано інфраструктурні характеристики операції, а саме патерни назв сторінок-одноденок і систематичне використання клонів реальних українських новинних видань. Операція використовувала імітацію легітимних європейських та українських ЗМІ з використанням таких технічних рішень, як фільтрація трафіку. Когнітивний рівень операції спирається на механізми соціального доказу, імітуючи легітимні медіа, а також повторюваність повідомлень. Кейс підтверджує гіпотезу про повну простежуваність стратегічного задуму в операційному втіленні за наявності документальних джерел. Операцію надійно атрибутовано до інституційного консорціуму АСП–Структура з високим рівнем впевненості на основі сукупності чотирьох незалежних речових ознак, серед яких особливе значення має виявлений автором збіг ідентичного меметичного матеріалу між рекламним каналом «Двійника» та викритою координованою мережею коментарів АСП.

Кейс TikTok-операції зі звинуваченнями у корупції. Використавши мультимодальний метод детекції було проведено верифікації мультимедійних документів у мережі TikTok (Barve et al., 2023; Khan et al., 2025). Проведений аналіз відеосюжетів, які звинувачували посадових осіб України у корупції, підтвердив російське походження матеріалу. Цей матеріал є частиною координованої кампанії впливу, яка складалась з 12820 відео, й не може бути ізольованим прикладом

дискредитації чи критики через співпадіння на кількох рівнях. На технічному рівні ця кампанія реалізовувала стратегічний задум РФ за допомогою кількох взаємопов'язаних інструментів. По-перше, використовувалися мережі одноразових акаунтів з іменами, схожими на реальні. Ці облікові записи поширювали короткі відео зі стандартною структурою. ЇЇ можна схематично описати як фото чиновника + зображення розкішного майна + емоційний контраст. До того ж усі відео були озвучені штучним інтелектом, що свідчить про схожу інфраструктуру. По-друге, цей контент було перекладено на кілька мов і поширено через Telegram і Twitter/X, що наочно демонструє роботу моделі «потоку брехні» у її сучасній реалізації на соціальних платформах (Paul and Matthews, 2016). На наративному рівні ця операція експлуатувала тему корупції, що використала реальну вразливість для послаблення довіри до української влади. Когнітивний рівень цієї операції ґрунтується на створенні емоційного контрасту між образами «розкішного життя еліт» і «страждань простих громадян». Цей фрейм може активувати почуття несправедливості та обурення. Зв'язок між цією операцією та активністю АСП/Структури оцінюється на рівні середньо-високої впевненості. Ця оцінка посилена появою одного із задокументованих сюжетів на дашборді Центру «С» (Belton et al., 2024).

Кейс координованої активності у коментарях в Telegram, Twitter/X і Facebook. Проведено комп'ютеризований наративний синтез з корпусу з 32561 коментаря за період з 22 листопада по 1 грудня 2024 року з використанням підходу BERTopic. Він включає багатомовне векторне представлення документів, з подальшим зниженням розмірності UMAP, використанням HDBSCAN-кластеризації й c-TF-IDF-репрезентації. Цей процес індуктивно виявив 125 наративних тем, які за процедурою якісного об'єднання згруповано у сім макронаративних кластерів: делегітимізація військово-політичного керівництва України; провина Заходу та НАТО; фрейм «нацистської ідеології» в Україні; заперечення української національної ідентичності; дискурс мирних переговорів на російських умовах; військові втрати й мобілізація; ядерна загроза. На технічному рівні ця операція демонструє як російські актори

використовують інфраструктуру коментарів у соціальних мережах для реалізації своєї стратегії. Вони використовують мережі неавтентичних акаунтів, які поширюють шаблонний контент під дописами інших користувачів, причому часто ці відповіді з'являються майже синхронно. Наративним шаром тут є інтерпретація подій та їхнє пояснення через призму дискредитації влади, тобто злиття порядку денного (agenda-melding). Цей підхід фактично формує враження «суспільної думки» навколо матеріалу легітимного каналу. Когнітивний же рівень експлуатує ілюзію згоди більшості й механізми соціального доказу. Важливо, що ці коментарі будуть найбільш ефективними в разі, коли користувач сприйматиме коментарі як автентичну реакцію. Серед виявлених кластерів за обсягом охоплення домінує кластер делегітимізації української влади, що відповідає задокументованій у внутрішніх матеріалах АСП цілі дискредитації керівництва України. Атрибуція координованого характеру виявленої активності до російських операцій впливу оцінюється на рівні середньої впевненості. Водночас пряма інституційна належність окремих облікових записів безпосередньо до АСП — на рівні низької впевненості, з огляду на можливість альтернативних пояснень.

Зіставлення виявлених емпіричних закономірностей трьох операцій з оприлюдненими внутрішніми документами АСП і Структури дозволило встановити прямі координаційні зв'язки. По-перше, наративні установки з документів АСП виявляються центральними у всіх трьох кейсах. По-друге, окремі візуальні матеріали повторюються між операцією «Двійник» і коментарними кампаніями, що документально підтверджено в дослідженні. По-третє, зафіксовано перетин зібраного матеріалу з дашбордом внутрішніх документів АСП, що підтверджує перетин задокументованих автором операцій з підрядниками. Таким чином, три зафіксовані кейси не є окремими тактичними епізодами, а становлять реалізацію єдиної стратегічної доктрини. У ній тактична конфігурація варіює залежно від платформного середовища, зберігаючи стратегічну стабільність задуму.

Порівняння трьох кейсів дозволяє визначити ключову закономірність російських інформаційних операцій проти України під час повномасштабного вторгнення.

Російські інформаційні операції тактично адаптуються до нових умов, але водночас зберігають стратегічну стабільність. Визначені стратегічні установки з внутрішньої документації АСП та доктрин РФ залишаються незмінними в усіх трьох операціях. А саме — постійне протиборство та насичення інформаційного простору корисними для РФ наративами. Тактика змінюється залежно від цифрового середовища і може включати інфраструктуру клонування ЗМІ, використання просторів для коментарів і крос-платформне розповсюдження контенту. Тобто еволюція російських операцій впливу після 2022 року є радше технічною та тактичною адаптацією в межах сталої стратегічної логіки, що розроблялася роками. Це розуміння є важливим для розроблення контрзаходів, адже точкові реакції на окремі тактики (як-от клонування сайтів) є структурно недостатніми. Протидіяти треба теж стратегічно, із розумінням того, що інформаційні операції РФ — це система. Таким чином, потрібно працювати над протидією на стратегічному рівні.

Верифікація гіпотез дослідження

Зведена картина верифікації висунутих у Вступі чотирьох гіпотез представлена в таблиці.

Таблиця 3.14. Результати верифікації гіпотез дослідження

№	Формулювання гіпотези	Кейс / емпіричний матеріал	Результат верифікації
Г1	Російські інформаційні операції в українському сегменті соціальних медіа спрямовані на деморалізацію населення України через підрив довіри до державних інституцій та міжнародних союзників через встановлення негативного порядку денного засобами рекламних повідомлень і меметичних конструкцій.	Операція «Двійник» (Facebook); 649 скриншотів реклами	**Підтверджено.** Виявлено систематичну сукупність наративних кластерів (мобілізаційний, корупційний, антизахідний), що реалізують зазначену стратегію.
Г2	Виявлені відео є частиною координованої мережі неавтентичних акаунтів і відповідної операції впливу, а не ізольованим випадком дискредитації посадових осіб.	TikTok-кампанія; кросплатформна дифузія	**Підтверджено.** Задокументовано мережу акаунтів-розповсюджувачів і характерну кросплатформну дифузію.

№	Формулювання гіпотези	Кейс / емпіричний матеріал	Результат верифікації
Г3	Скоординована діяльність у коментарях у досліджуваному корпусі переважно реалізує стратегію перенесення відповідальності за війну з РФ на Україну та країни Заходу й дискредитацію військово-політичного керівництва.	Корпус коментарів; BERTopic	**Підтверджено.** У той час як наратив про відповідальність Заходу/НАТО присутній і виражений як окремий макрокластер, він не є кількісно домінантним. Проте, делегітимізаційним кластером військово-політичного керівництва був найбільшим.

№	Формулювання гіпотези	Кейс / емпіричний матеріал	Результат верифікації
Г4	Повідомлення, виявлені у трьох проаналізованих кейсах, корелюють із цілями, зафіксованими у внутрішніх документах російських дезінформаційних підрядників, що підтверджує їхню належність до спільної інституційної архітектури впливу.	Тріангуляція трьох кейсів з афідевітом Міністерства юстиції США та внутрішніми документами Центру «С»	**Підтверджено.** Середня впевненість. Зв'язки між «Двійником» і коментарями та «Двійником» і TikTok операцією — висока впевненість. Зафіксовано прямий збіг меметичного матеріалу та інфраструктурних патернів «Двійника» із задокументованими активами АСП. Російське походження операції в ТікТок верифіковано методами OSINT. Перетин коментарів з АСП — середня впевненість, співпадіння за наративами та цілями.

Таким чином, чотири висунуті гіпотези верифіковано повністю

Узагальнена характеристика сучасних російських операцій впливу

Сукупність отриманих емпіричних і концептуальних результатів дає змогу сформулювати декілька узагальнень щодо сучасного стану російських інформаційних операцій проти України та країн західних демократій.

По-перше, сучасні російські операції імплементуються, зокрема, через екосистему приватних підрядників (АСП, Структура), які номінально незалежні від уряду, але працюють у безпосередній координації з державним апаратом РФ. Вони реалізують інформаційні операції, спрямовані на різні цільові аудиторії, адаптуючись до різних мовних середовищ і платформ соціальних мереж. Підрядники використовують спільну операційну інфраструктуру та меметичний матеріал для масштабування своїх операцій. Ці ж структури є тими, хто реалізує стратегію державних інформаційних операцій, зафіксовану у доктринах та інших офіційних документах.

По-друге, інформаційні операції характеризуються представленням на кількох платформах одночасно, з міграцією контенту між ними. Одне й те саме повідомлення інформаційних операцій може мігрувати між Telegram, TikTok, Twitter/X, Facebook та іншими периферійними платформами у формі вторинних повідомлень. Вони можуть мати переклади кількома мовами та стилістичні модифікації при подальшому розповсюдженні. Ці операції реалізують логіку «потоку брехні» в її сучасному цифровому варіанті, що використовує соціальні платформи для розповсюдження й затоплення простору шумом.

По-третє, наративна архітектура операцій структурована довкола порівняно стійкого набору наративів, зокрема, делегітимізації українського керівництва, провини Заходу/НАТО у війні, фрейму «нацистської ідеології», заперечення української ідентичності, дискурсу мобілізаційно-військового виснаження та ядерної загрози. Ці наративи демонструють разючу схожість і спадкоємність з наративами попередніх історичних епох російської пропаганди.

По-четверте, технологічна еволюція російських операцій є очевидною. Інтеграція великих мовних моделей у виробництво синтетичного контенту та створення інфраструктури для його розповсюдження, використання підходів клоакінгу для обходу

модерації, масштабування потрібних повідомлень через коментарі та продукування великої кількості контенту тощо, випереджають темпи розвитку методологічного інструментарію їхнього дослідження й протидії. Це зумовлює потребу у постійному оновленні дослідницьких підходів, обміні інформацією та появі новітніх методів детекції та моніторингу таких загроз.

Практичні рекомендації щодо протидії

Сформульовані у роботі рекомендації структуровані за трьома рівнями запропонованої аналітичної рамки і адресовані різним суб'єктам системи протидії російським інформаційним операціям.

Технічний (інфраструктурний) рівень. Для технологічних платформ і регуляторів бажаним є розширення прозорості рекламних бібліотек. Вони мають публікувати інформацію про географію таргетування й обсяг витрат у розрізі країн із обов'язковим зберіганням реклам, які порушили правила. До того ж, позитивним кроком було б впровадження обов'язкового виявлення клоакінг-технік як критерію автоматичної модерації реклами, яку платформи демонструють користувачам. Стандартизація API-доступу для дослідників відповідно до моделі Digital Services Act ЄС уможливить незалежний моніторинг операцій впливу. Для державних інституцій у цьому розрізі важливою є інституціоналізація постійного моніторингу рекламних бібліотек та платформ з відкритим API за допомогою спеціалізованих аналітичних підрозділів, що фокусуються на зовнішніх операціях впливу (FIMI).

Наративний (контентний) рівень. Аналітичні центри й факт-чекінгові організації мають продовжувати активність щодо своєчасної ідентифікації макронаративів та фреймів, які активно експлуатуються в координованих кампаніях впливу. До того ж, матеріали таких досліджень мають бути опубліковані у форматі, який був би прийнятний для для журналістів та редакцій, щоб збільшити поширення цих досліджень. Система освіти може включати актуальні кейси у програми медіаграмотності з акцентом на ідентифікацію структурних рис російських наративів, а не лише на верифікацію конкретних фактів. Державні інституції в рамках стратегічних

комунікацій можуть підготувати проактивні інокуляційні кампанії за моделлю, яка була валідована у роботах Roozenbeek та van der Linden (2022), й орієнтовувати такі кампанії на протидію найбільш активно експлуатованим макронаративам.

Когнітивний (психологічний) рівень. Системи освіти й суспільної комунікації мають працювати над розвитком критичного мислення та обізнаності людей з типовими когнітивними упередженнями (підтверджувальне упередження, ефект ілюзорної правди, ефект соціального доказу тощо) як універсального захисного інструмента в рамках широких інформаційних кампаній. При адаптації відомих інструментів інокуляції для українського контексту варто спиратися на дослідження російських інформаційних операцій. У цьому випадку корисним буде використати наративні кластери та цілі, які актори РФ переслідують в Україні згідно внутрішньої документації АСП, для найкращого ефекту.

Міжінституційний рівень. Для ефективної взаємодії між різними акторами у сфері протидії мають бути встановлені стійкі координаційні механізми між державними органами, провідними неурядовими, приватними та академічними організаціями. Форматом такої співпраці можуть бути регулярний обмін індикаторами інформаційних операцій РФ (тактик, технік та процедур) та підготовка спільних аналітичних звітів. Запропонована трирівнева аналітична рамка може використовуватися як спільна аналітична мова верхнього рівня у міжінституційній взаємодії, що забезпечуватиме узгоджене розуміння природи виявлених операцій і релевантних заходів реагування.

Науковий та практичний внесок

Сукупний науковий внесок роботи полягає в інтеграції технічного, наративного й когнітивного рівнів аналізу російських інформаційних операцій у єдину рамку. По-друге, було введено в науковий обіг унікальний авторський корпус 649 скриншотів операції «Двійник» в Україні. По-третє, виявлено 7 макронаративних кластерів координованої коментарської активності у двомовному (українсько-російському) корпусі з 32561 коментаря. По-четверте, була здійснена емпірична фіксація прямих

речових ланок між трьома різними кейсами російських операцій як прикладів реалізації стратегії РФ.

Практичний внесок реалізується у 3 форматах. По-перше, у вигляді відтворюваного методологічного інструментарію, що складається з BERTopic-підходу для аналізу коментарів. По-друге, скриншотного аналізу неавтентичних сторінок та їхніх реклам задля збереження ефемерного контенту. Насамкінець, структурованого підходу до OSINT-верифікації відеоматеріалів, які використовують в інформаційних операціях. Цей інструментарій разом з рамкою досліджень придатний для оперативного застосування аналітичними підрозділами державних інституцій та неурядових організацій, що займаються протидією інформаційним операціям. По-друге, у вигляді конкретних рекомендацій щодо протидії, диференційованих за рівнями запропонованої рамки, що можуть стати в пригоді відповідним акторам протидії. По-третє, у вигляді освітніх ресурсів, які можуть бути інтегровані у курси з медіаграмотності, цифрової безпеки та аналізу інформаційних операцій для студентських й професійних аудиторій.

Обмеження дослідження та перспективи подальших академічних розвідок

Виконане дисертаційне дослідження має низку обмежень, які повністю задокументовано у Підрозділі 2.3. Серед головних обмежень цього дослідження можна виділити те, що вибірка рекламних повідомлень операції «Двійник» є вибіркою зручності одного дослідника. Це обмеження обумовлено алгоритмічною логікою Facebook і неможливістю зібрати масив в автоматичному режимі через відсутність доступу до даних платформи у конкретному національному та часовому контекстах. По-друге, обчислювальний алгоритм тематичного моделювання не мав формального аналізу чутливості. До того ж, не було проведено валідацію узагальнених наративних кластерів з іншими дослідниками. По-третє, у роботі відсутній контрольний корпус органічних коментарів, який дозволив би порівняти специфіку координованих неавтентичних акаунтів із автентичними повідомленнями в тому ж інформаційному просторі. Масив даних є досить специфічним щодо часового зрізу, а не випадковим у ширшому періоді. До того ж робота спирається на вердикт аналітичного інструменту

O’Savul щодо неавтентичної поведінки, що не є розкритим у публічному просторі. Операціоналізація когнітивного рівня запропонованої трирівневої рамки є обмеженою. У межах роботи цей рівень реалізовано через літературний синтез і реконструкцію задумів операторів, а не через прямий експериментальний вимір ефекту.

Окреслені обмеження визначають програму подальших досліджень за чотирма основними напрямами.

Методологічний напрям передбачає 1) формальний аналіз стабільності виявлених наративних кластерів у випадку варіювання параметрів BERTopic; 2) валідацію з другим незалежним кодувальником із обчисленням показників надійності між кодувальниками; 3) побудову контрольних корпусів органічних коментарів для статистично коректного виокремлення специфіки координованої активності.

Емпіричний напрям передбачає 1) часове відстеження еволюції операції «Двійник» та координованих коментарських мереж впродовж ширшого періоду з фіксацією реакції операторів на ключові події (вибори, мирні переговори, військові події); 2) порівняльне дослідження російських операцій впливу в інших європейських країнах-цілях (Польща, Балтійські країни, Молдова), а також у інших регіонах, як-от країнах Глобального Півдня. Ці дослідження можуть фокусуватись на виявленні того, як російська інфраструктура інформаційних операцій адаптується до характеристик країн; 3) розширення методологічних підходів для дослідження операцій на інших платформах (Threads, Bluesky тощо) та форматах контенту (клонування голосу, синтетичні відео).

Експериментальний напрям передбачає 1) лабораторне та польове вимірювання когнітивного впливу типових повідомлень досліджуваних операцій на українську аудиторію. Це вимірювання має враховувати та контролювати такі параметри як вік, регіон, рівень медіаграмотності та політичні погляди; 2) валідацію адаптованих інокуляційних стратегій до українського контексту в середовищі соціальних платформ; 3) дослідження ефективності різних форматів спростування до різних типів дезінформаційних повідомлень.

Інституційний напрям передбачає 1) порівняльне дослідження ефективності рекомендованих заходів протидії в умовах різних країн та можливостей взаємодії між державою, платформами та громадянським суспільством; 2) розробку формальних протоколів обміну індикаторами між аналітичними підрозділами державних та неурядових установ; 3) концептуалізацію стійких механізмів системи протидії дезінформації у післявоєнний період, адже, із врахуванням доктрин РФ, інформаційна війна не має закінчення. Таким чином, ця система має зберегти інституційні здобутки протидії воєнного періоду в умовах майбутнього мирного часу.

Сучасні російські інформаційні операції становлять комплексний і технологічно мінливий феномен, дослідження якого вимагає одночасної концептуальної інтеграції різних аналітичних традицій. Стратегія цих операцій має історичну спадковість з радянськими «активними заходами», методично організовану доктринальну основу, яка частково реалізується компаніями-підрядниками, які продукують операції у промислових масштабах у соціальних мережах. Основним науковим внеском дисертації є емпірично обґрунтоване положення про *адаптацію тактик за умови збереження стратегічної стабільності* як визначальної характеристики російських інформаційних операцій в період повномасштабного вторгнення. Це положення випливає зі концептуалізації стратегічного рівня інформаційних операцій, який було реконструйовано за матеріалами доктринальних документів РФ та внутрішньої документації Агенції соціального проєктування та Структури. Цю стратегію було зіставлено з трьома контрастними прикладами реалізації стратегії — операцією Doppelganger у системі клонованих ЗМІ, скоординованою експлуатацією коментарів та масштабною TikTok-операцією з дискредитації українського керівництва. Ці операції спростовують поширене уявлення про російські операції впливу як про хаотичну сукупність різних тактичних підходів. Дисертаційне дослідження демонструє, що за цими операціями стоїть зріла й формалізована стратегічна доктрина, яка зберігає внутрішню логіку незалежно від платформного середовища. Запропонована та апробована в дисертації трирівнева аналітична рамка (технічний, наративний,

когнітивний виміри) виступає продовженням цього теоретичного внеску. Вона дозволяє системно аналізувати реалізацію стратегії в усіх трьох вимірах одночасно та може бути перенесена на дослідження інформаційних операцій інших державних і недержавних акторів. Відтак дисертація заповнює суттєву аналітичну прогалину в українських комунікаційних студіях та студіях стратегічних комунікацій, водночас пропонуючи концептуальний інструментарій, що має безпосереднє прикладне значення для розбудови національної системи протидії інформаційним загрозам та формування довгострокової стратегії інформаційної стійкості України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alaphilippe, A., Machado, G., Miguel, R., & Poldi, F. (2022). *Doppelganger. Media clones serving Russian propaganda* (p. 26). https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf
2. Aleksejeva, N., Andriukaitis, L., Bandeira, L., Barojan, D., Brookie, G., Buziashvili, E., Carvin, A., Karan, Kanishk, Nimmo, B., Robertson, I., & Sheldon, M. (2019). *Operation "Secondary Infektion."* Digital Forensic Research Lab (DFRLab). https://www.atlanticcouncil.org/wp-content/uploads/2019/08/Operation-Secondary-Infektion_English.pdf
3. Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, *31*(2), 211–236. https://doi.org/10.1257/jep.31.2.211
4. Andrew, C. M., & Mitrokhin, V. N. (2000). *The Mitrokhin archive: The KGB in Europe and the West*. Penguin.
5. Arif, A., Stewart, L. G., & Starbird, K. (2018). Acting the Part: Examining Information Operations Within #BlackLivesMatter Discourse. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1–27. https://doi.org/10.1145/3274289
6. Atanasova, A., Lesplingart, A., Poldi, F., & Kuster, G. (2024). *Operation Overload* (p. 90). Check First, Reset Tech. https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf
7. Badawy, A., Ferrara, E., & Lerman, K. (2018). Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign. *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 258–265. https://doi.org/10.1109/ASONAM.2018.8508646
8. Bail, C. A., Guay, B., Maloney, E., Combs, A., Hillygus, D. S., Merhout, F., Freelon, D., & Volfovsky, A. (2020). Assessing the Russian Internet Research Agency's impact on the political attitudes and behaviors of American Twitter users in late 2017. *Proceedings of the National Academy of Sciences*, *117*(1), 243–250. https://doi.org/10.1073/pnas.1906420116

9. Barve, Y., Saini, J. R., Rathod, R., & Gaikwad, H. (2023). Multi-Modal Misinformation Detection: An Exhaustive Review. *2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, 1–5. https://doi.org/10.1109/ICCUBEA58933.2023.10392005

10. Belton, C. (2023, December 30). Russia is working to subvert French support for Ukraine, documents show. *The Washington Post*. https://www.washingtonpost.com/world/2023/12/30/france-russia-interference-far-right/

11. Belton, C., Horton, A., O'Grady, S., Burianova, T., Morgunov, S., & Karklis, L. (2024, February 16). Kremlin runs disinformation campaign to undermine Zelensky, documents show. *Washington Post*. https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/

12. Belton, C., Mekhennet, S., & Harris, S. (2023, April 21). Kremlin tries to build antiwar coalition in Germany, documents show. *The Washington Post*. https://www.washingtonpost.com/world/2023/04/21/germany-russia-interference-afd-wagenknecht/

13. Belton, C., & Menn, J. (2024, April 8). Russian trolls target U.S. support for Ukraine, Kremlin documents show. *The Washington Post*. https://www.washingtonpost.com/world/2024/04/08/russia-propaganda-us-ukraine/

14. Ben Nimmo. (2017, November 16). How A Russian Troll Fooled America. *DFRLab*. https://medium.com/dfrlab/how-a-russian-troll-fooled-america-80452a4806d1

15. Benkler, Y., Faris, R., & Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (1st ed.). Oxford University Press New York. https://doi.org/10.1093/oso/9780190923624.001.0001

16. Bergmann, M., Dolbaia, T., & Fenton, N. (2022). *Russia's Adaptation Game: Deciphering the Kremlin's "Humanitarian Policy."* https://www.csis.org/analysis/russias-adaptation-game-deciphering-kremlins-humanitarian-policy

17. Berzins, J. (2014). *Russia's new generation warfare in Ukraine: implications for Latvian defense policy* (No. 02). National Defense Academy of Latvia Center for Security and

Strategic Research. https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf

18. Bittman, L. (1985). *The KGB and Soviet disinformation: An insider's view*. Pergamon-Brassey's International Defense Publ.

19. Borysenko, I. (2023, December 20). *90% of Ukraine aid funds spent in US — Secretary Blinken*. NV. https://english.nv.ua/nation/90-of-ukraine-aid-funds-spent-in-us-secretary-blinken-50378187.html

20. Bradshaw, S., & Howard, P. N. (2018). *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*. Oxford Internet Institute. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2018/07/ct2018.pdf

21. Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., Quinn, S. C., & Dredze, M. (2018). Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate. *American Journal of Public Health*, *108*(10), 1378–1384. https://doi.org/10.2105/AJPH.2018.304567

22. Buziashvili, E., & Rizzuto, M. (2022, February 4). Kremlin outlets exploit suspicious user comments on German Navy chief's resignation. *DFRLab*. https://dfrlab.org/2022/02/04/kremlin-outlets-exploit-suspicious-user-comments-on-german-navy-chiefs-resignation/

23. Campello, R. J. G. B., Moulavi, D., & Sander, J. (2013). Density-Based Clustering Based on Hierarchical Density Estimates. In J. Pei, V. S. Tseng, L. Cao, H. Motoda, & G. Xu (Eds.), *Advances in Knowledge Discovery and Data Mining* (Vol. 7819, pp. 160–172). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-37456-2_14

24. Cardiff University. (2021). *How a Kremlin-Linked Influence Operation is Systematically Manipulating Western Media to Construct & Communicate Disinformation*. https://www.cardiff.ac.uk/__data/assets/pdf_file/0008/2560274/OSCAR-report-September-2021.pdf

25. Carey, J. W. (1989). A Cultural Approach to Communication. In *Communication as Culture: Essays on Media and Society*. (pp. 13–36). Retrieved https://web.mit.edu/21l.432/www/readings/Carey_CulturalApproachCommunication.pdf

26. Chadwick, A. (2013). *The Hybrid Media System: Politics and Power*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199759477.001.0001

27. Chadwick, A., & Stanyer, J. (2022). Deception as a Bridging Concept in the Study of Disinformation, Misinformation, and Misperceptions: Toward a Holistic Framework. *Communication Theory*, *32*(1), 1–24. https://doi.org/10.1093/ct/qtab019

28. Châtelet, V., & Osadchuk, R. (2024, March 12). *Doppelganger targets Ukrainian and French audiences via Facebook ads*. https://dfrlab.org/2024/03/12/doppelganger-operation-targets-ukraine/

29. CheckFirst, & DFRLab. (2026). *Pravda in numbers—Content and Network analysis*. Retrieved April 5, 2026, from https://portal-kombat.com/

30. Chen, A. (2015, June 2). The Agency. *The New York Times*. https://www.nytimes.com/2015/06/07/magazine/the-agency.html

31. Chenrose, A. (2024, November 4). Sockpuppet network impersonating Americans and Canadians amplifies pro-Israel narratives on X. *DFRLab*. https://dfrlab.org/2024/11/04/sockpuppet-network-impersonating-americans-and-canadians-amplifies-pro-israel-narratives-on-x/

32. Chong, D., & Druckman, J. N. (2007). Framing Theory. *Annual Review of Political Science*, *10*(1), 103–126. https://doi.org/10.1146/annurev.polisci.10.072805.103054

33. Clayton, K., Blair, S., Busam, J. A., Forstner, S., Glance, J., Green, G., Kawata, A., Kovvuri, A., Martin, J., Morgan, E., Sandhu, M., Sang, R., Scholz-Bright, R., Welch, A. T., Wolff, A. G., Zhou, A., & Nyhan, B. (2020). Real Solutions for Fake News? Measuring the Effectiveness of General Warnings and Fact-Check Tags in Reducing Belief in False Stories on Social Media. *Political Behavior*, *42*(4), 1073–1095. https://doi.org/10.1007/s11109-019-09533-0

34. Collins. (2017, November 2). Collins 2017 Word of the Year Shortlist. *Collins Dictionary Language Blog*. https://blog.collinsdictionary.com/language-lovers/collins-2017-word-of-the-year-shortlist/

35. Copeland, T. (2025, December 5). *BBC Verify Live: Russian trolls made fake video about Zelensky buying Bill Cosby's house, says expert*. BBC News. https://www.bbc.com/news/live/cy9503dw9nnt

36. Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4. ed). SAGE.

37. Darcy, O. (2022, March 3). *RT America ceases productions and lays off most of its staff | CNN Business*. CNN. https://www.cnn.com/2022/03/03/media/rt-america-layoffs

38. Debunk.org. (2023, May 4). *Kremlin spent 1.9 billion USD on propaganda last year, the budget exceeded by a quarter*. Debunk.Org. https://www.debunk.org/kremlin-spent-1-9-billion-usd-on-propaganda-last-year-the-budget-exceeded-by-a-quarter

39. Department of Justice. (2018, July 13). *Office of Public Affairs | Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election | United States Department of Justice*. https://www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

40. Department of Justice. (2024a, September 4). *Office of Public Affairs | 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

41. Department of Justice. (2024b, September 4). *Office of Public Affairs | Two RT Employees Indicted for Covertly Funding and Directing U.S. Company that Published Thousands of Videos in Furtherance of Russian Interests | United States Department of Justice*. https://www.justice.gov/archives/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands

42. Department of State. (1987). *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-87*. United States Department of State. https://archive.org/details/dos-report_s-12so-8-12/mode/2up

43. DFRLab. (2022a, March 2). Russian Hybrid War Report: Social platforms crack down on Kremlin media as Kremlin demands compliance. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-hybrid-war-report-social-platforms-crack-down-on-kremlin-media-as-kremlin-demands-compliance/

44. DFRLab. (2022b, April 22). Russian War Report: Forged document claims Ukraine is selling surplus weapons to African countries. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-forged-document-claims-ukraine-is-selling-surplus-weapons-to-african-countries/

45. DFRLab. (2022c, October 11). Russia-based Facebook operation targeted Europe with anti-Ukraine messaging. *DFRLab*. https://medium.com/dfrlab/russia-based-facebook-operation-targeted-europe-with-anti-ukraine-messaging-389e32324d4b

46. DFRLab. (2023a, February 22). Narrative warfare. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/

47. DFRLab. (2023b, February 22). Undermining Ukraine. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine/

48. DFRLab. (2024, February 29). In Latin America, Russia's ambassadors and state media tailor anti-Ukraine content to the local context. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/in-latin-america-russias-ambassadors-and-state-media-tailor-anti-ukraine-content-to-the-local-context/

49. Digital Forensic Research Lab. (2022a, April 8). Russian War Report: Russia makes false claims while blaming Ukraine for Kramatorsk railway station attack. *New Atlanticist*. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-russia-makes-false-claims-while-blaming-ukraine-for-kramatorsk-railway-station-attack/#kramatorsk

50. Digital Forensic Research Lab. (2022b, July 22). Russian War Report: Russia accuses Ukraine of creating 'monster' troops in biolabs. *Atlantic Council*.

https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-russia-accuses-ukraine-of-creating-monster-troops-in-biolabs/

51. DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J., & Johnson, B. (2019). *The Tactics & Tropes of the Internet Research Agency* (p. 101). New Knowledge. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1003&context=senatedocs

52. Duguay, S., & Gold-Apel, H. (2023). Stumbling Blocks and Alternative Paths: Reconsidering the Walkthrough Method for Analyzing Apps. *Social Media + Society*, *9*(1), 20563051231158822. https://doi.org/10.1177/20563051231158822

53. Ecker, U. K. H., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N., Kendeou, P., Vraga, E. K., & Amazeen, M. A. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology*, *1*(1), 13–29. https://doi.org/10.1038/s44159-021-00006-y

54. EEAS. (2015, June 22). Action plan on strategic communication. *Ares(2015)2608242*. https://web.archive.org/web/20151106182524/http://eap-csf.eu/assets/files/Action%20PLan.pdf

55. EEAS. (2023). *1st EEAS Report on Foreign Information Manipulation and Interference Threats* (p. 36). European External Action Service. https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

56. EEAS. (2024). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats* (p. 38). European External Action Service. https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

57. EEAS. (2025). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats* (p. 43). European External Action Service. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

58. EEAS. (2026). *4th EEAS Report on Foreign Information Manipulation and Interference Threats* (p. 40). European External Action Service. https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf

59. Egelhofer, J. L., & Lecheler, S. (2019). Fake news as a two-dimensional phenomenon: A framework and research agenda. *Annals of the International Communication Association*, *43*(2), 97–116. https://doi.org/10.1080/23808985.2019.1602782

60. Eggen, K.-A. (2025). A strategy for the weak: The role of information confrontation in Russia's grand strategy. *Defence Studies*, *26*(2), 211–235. https://doi.org/10.1080/14702436.2025.2561639

61. Ellul, J. (1973). Categories of propaganda. In *Propaganda: The formation of men's attitudes* (pp. 15–16). Vintage Books.

62. Entman, R. M. (1993). Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication*, *43*(4), 51–58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x

63. Etymonline. (2025). *Propaganda—Etymology, Origin & Meaning*. Etymonline. https://www.etymonline.com/word/propaganda

64. EU Commission. (2024). *Remarks of President António Costa at the joint press conference with President of Ukraine Volodymyr Zelenskyy in Kyiv*. Consilium. Retrieved April 25, 2026, from https://www.consilium.europa.eu/en/press/press-releases/2024/12/01/remarks-of-president-antonio-costa-at-the-joint-press-conference-with-president-of-ukraine-volodymyr-zelenskyy-in-kyiv/

65. European Commission. (2023, July 28). *Subject: Social Design Agency | EU sanctions tracker*. https://data.europa.eu/apps/eusanctionstracker/subjects/155817

66. European Council. (2022). *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*. Consilium. Retrieved March 1, 2026, from https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/

67. EUvsDisinfo. (2019, June 20). *Renewed Focus on MH17*. EUvsDisinfo. https://euvsdisinfo.eu/renewed-focus-on-mh-17/

68. EUvsDisinfo. (2024, July 16). *MH17: Ten years of Russian lying and denying*. EUvsDisinfo. https://euvsdisinfo.eu/mh17-ten-years-of-russian-lying-and-denying/

69. Fairclough, N. (2013). *Critical discourse analysis: The critical study of language* (2nd edition, reprint). Routledge.

70. Falk, T. O. (2022). *How much of a problem is corruption in Ukraine?* Al Jazeera. Retrieved October 31, 2025, from https://www.aljazeera.com/news/2022/6/15/how-problematic-is-corruption-in-ukraine

71. Fedchenko, Y. (2016). Kremlin propaganda: Soviet active measures by other means. *Sõjateadlane (Estonian Journal of Military Studies)*, *2*, 141–170.

72. Ferguson, R. J. (2024). *Octavian, Antony and Cleopatra: Propaganda and War*. ResearchGate. Retrieved September 14, 2025, from https://www.researchgate.net/publication/383565605_Octavian_Antony_and_Cleopatra_Propaganda_and_War

73. François, C. (2019). *Actors, Behaviors, Content: A Disinformation ABC* (p. 10). Graphika and Berkman Klein Center for Internet & Society at Harvard University. https://www.congress.gov/116/meeting/house/109980/witnesses/HHRG-116-SY21-Wstate-FrancoisC-20190926-SD001.pdf

74. Franklin, M., Torrey, M., Agranovich, D., & Dvilyanski, M. (2024). *Adversarial Threat Report. Second Quarter*. https://transparency.meta.com/sr/Q2-2024-Adversarial-threat-report/

75. Galeotti, M. (2018, March 5). I'm Sorry for Creating the 'Gerasimov Doctrine.' *Foreign Policy*. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

76. Garant. (2000). *Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 09.09.2000 N Пр-1895)*. Retrieved May 24, 2026, from https://base.garant.ru/182535/

77. Garant. (2013). *Концепция внешней политики Российской Федерации (12 февраля 2013 г.)*. https://www.garant.ru/products/ipo/prime/doc/70218094/

78. Garant. (2016). *Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации."* https://base.garant.ru/71556224/

79. GEC. (2020). *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem*. Global Engagement Center and the U.S. Department of State. https://2017-2021.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

80. Gerbner, G., Gross, L., Jackson-Beeck, M., Jeffries-Fox, S., & Signorielli, N. (1978). Cultural Indicators: Violence Profile No. 9. *Journal of Communication*, *28*(3), 176–207. https://doi.org/10.1111/j.1460-2466.1978.tb01646.x

81. Gigitashvili, G., & Osadchuk, R. (2022, February 18). How ten false flag narratives were promoted by pro-Kremlin media. *Digital Forensic Research Lab (DFRLab)*. https://medium.com/dfrlab/how-ten-false-flag-narratives-were-promoted-by-pro-kremlin-media-c67e786c6085

82. Giles, K. (2012). *Russia's Public Stance on Cyberspace Issues*. https://ccdcoe.org/uploads/2015/04/CyCon_2012_book_web_sisu.indd_.pdf

83. Giles, K. (2016a). *Handbook of Russian information warfare*. Research division NATO Defense College. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf

84. Giles, K. (2016b). *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power* (p. 73). Chatham House. https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf

85. Global Engagement Center. (2023, October 5). *About Us—Global Engagement Center—United States Department of State*.

https://web.archive.org/web/20231005025458/https://www.state.gov/about-us-global-engagement-center-2/

86. Goldstein, J. A., Sastry, G., Musser, M., DiResta, R., Gentzel, M., & Sedova, K. (2023). *Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2301.04246

87. Goldstein, J., & Carbonell, J. (1996). Summarization: (1) using MMR for diversity - based reranking and (2) evaluating summaries. *Proceedings of a Workshop on Held at Baltimore, Maryland October 13-15, 1998* -, 181. https://doi.org/10.3115/1119089.1119120

88. Golovchenko, Y., Buntain, C., Eady, G., Brown, M. A., & Tucker, J. A. (2020). Cross-Platform State Propaganda: Russian Trolls on Twitter and YouTube during the 2016 U.S. Presidential Election. *The International Journal of Press/Politics*, *25*(3), 357–389. https://doi.org/10.1177/1940161220912682

89. Goodreads. (2026). *Albert Einstein Quotes (Author of Relativity)*. Retrieved April 19, 2026, from https://www.goodreads.com/author/quotes/9810.Albert_Einstein

90. Gouliev, Z. (2025). *Propaganda and Information Dissemination in the Russo-Ukrainian War: Natural Language Processing of Russian and Western Twitter Narratives* (arXiv:2506.01807). arXiv. https://doi.org/10.48550/arXiv.2506.01807

91. Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Knopf Doubleday Publishing Group.

92. Griffin, E. (Director). (n.d.). *FULL INTERVIEW with Yuri Bezmenov: The Four Stages of Ideological Subversion* [Broadcast]. Retrieved https://www.youtube.com/watch?v=yErKTVdETpw&ab_channel=NicholasMarshall

93. Grinberg, N., Joseph, K., Friedland, L., Swire-Thompson, B., & Lazer, D. (2019). Fake news on Twitter during the 2016 U.S. presidential election. *Science*, *363*(6425), 374–378. https://doi.org/10.1126/science.aau2706

94. Grisé, M., Demus, A., Shokh, Y., Kepe, M., Welburn, J. W., & Golins'ka, C. (with Rand Corporation). (2022). *Rivalry in the information sphere: Russian conceptions of information confrontation*. RAND Corporation.

https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA198-8/RAND_RRA198-8.pdf

95. Grootendorst, M. (2022). *BERTopic: Neural topic modeling with a class-based TF-IDF procedure* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2203.05794

96. Guess, A. M. (2021). (Almost) Everything in Moderation: New Evidence on Americans' Online Media Diets. *American Journal of Political Science*, *65*(4), 1007–1022. https://doi.org/10.1111/ajps.12589

97. Guess, A. M., Nyhan, B., & Reifler, J. (2020). Exposure to untrustworthy websites in the 2016 US election. *Nature Human Behaviour*, *4*(5), 472–480. https://doi.org/10.1038/s41562-020-0833-x

98. Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, *5*(1), eaau4586. https://doi.org/10.1126/sciadv.aau4586

99. Guo, L. (2014). Toward the Third Level of Agenda-Setting Theory. In *Agenda Setting in a 2.0 world* (pp. 112–134). Taylor & Francis. https://www.researchgate.net/publication/283920453_Toward_the_third_level_of_agenda_setting_theory_A_Network_Agenda_Setting_Model

100. Halverson, J. R., Goodall, H. L., & Corman, S. R. (2011). *Master narratives of Islamist extremism*. Palgrave McMillan.

101. Hameleers, M. (2023). Disinformation as a context-bound phenomenon: Toward a conceptual clarification integrating actors, intentions and techniques of creation and dissemination. *Communication Theory*, *33*(1), 1–10. https://doi.org/10.1093/ct/qtac021

102. Hampton, K., Rainie, L., Lu, W., Dwyer, M., Shin, I., & Purcell, K. (2014, August 26). Social Media and the 'Spiral of Silence.' *Pew Research Center*. https://www.pewresearch.org/internet/2014/08/26/social-media-and-the-spiral-of-silence/

103. Haug, M., Maier, C., Gewald, H., & Weitzel, T. (2025). Supporting opinions to fit in: A spiral of silence-theoretic explanation for establishing echo chambers and filter bubbles on social media. *Internet Research*, *35*(7), 30–51. https://doi.org/10.1108/INTR-03-2024-0413

104. Hayden, L., Carah, N., Robards, B., & Dobson, A. (2024, February 11). SCREENSHOT METHODOLOGIES TO COLLECT AND ANALYSE SOCIAL MEDIA PLATFORM ADVERTISING. *Selected Papers of #AoIR2024*. The 25thAnnual Conference of the Association of Internet Researchers. https://spir.aoir.org/ojs/index.php/spir/article/view/13958/11844

105. Horbulin, V. (2016). THE "HYBRID WARFARE" ONTOLOGY. *Strategic Priorities*, *38*(1), 4–13.

106. Horbulin, V. (Ed.). (2017). *Svitova hibrydna vijna: Ukraïns'kyj front*. Folio.

107. House Committee Hearing. (2019, September 26). *Online Imposters and Disinformation* [Legislation]. US Congress. https://www.congress.gov/index.php/event/116th-congress/house-event/109980

108. Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., & François, C. (2019). *The IRA, Social Media and Political Polarization in the United States, 2012-2018* (p. 47). Oxford University. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf

109. Hugging Face. (2019, August 27). *Sentence-transformers/paraphrase-multilingual-mpnet-base-v2 · Hugging Face*. https://huggingface.co/sentence-transformers/paraphrase-multilingual-mpnet-base-v2

110. Hutchings, S. C., Tolz, V., Chatterje-Doody, P. N., Crilley, R., & Gillespie, M. (2024). *Russia, disinformation, and the liberal order: RT as populist pariah*. Northern Illinois University Press, an imprint of Cornell University Press.

111. Ignorance, the root and stem of all evil [@ivan_8848]. (2023, July 18). 💥🇺🇦🚗 *Here is the Ukrainian minister of defense Reznikov's new toy: A Mercedes Benz SLR MacLaren 999 Red made of solid gold. It has gilded tires and diamonds inlaid cabin. The price tag is $11 million. Https://t.co/nnrcpo7FwR* [Tweet]. Twitter. https://x.com/ivan_8848/status/1681297743933763584

112. Inwood, O., & Zappavigna, M. (2024). The legitimation of screenshots as visual evidence in social media: YouTube videos spreading misinformation and disinformation. *Visual Communication*, 14703572241255664. https://doi.org/10.1177/14703572241255664

113. IREX. (2024). *Learn to Discern*. https://www.irex.org/sites/default/files/node/resource/media-literacy-ukraine-one-page-handout.pdf

114. Jamieson, K. H., & Cappella, J. N. (Eds.). (2010). *Echo chamber: Rush Limbaugh and the conservative media establishment*. Oxford University Press.

115. Jingnan, H., Bond, S., & Allyn, B. (2025, January 7). Meta says it will end fact-checking as Silicon Valley prepares for Trump. *NPR*. https://www.npr.org/2025/01/07/nx-s1-5251151/meta-fact-checking-mark-zuckerberg-trump

116. Johnson, T. (2022, March 3). RT America To Halt Production And Lay Off Most Staff After Being Dropped By Major U.S. Distributors. *Deadline*. https://deadline.com/2022/03/rt-america-to-halt-production-and-lay-off-most-staff-after-being-dropped-by-major-u-s-distributors-1234970503/

117. Jowett, G., & O'Donnell, V. (2019). *Propaganda & persuasion* (Seventh edition). SAGE.

118. Kahan, D. M. (2013). Ideology, motivated reasoning, and cognitive reflection. *Judgment and Decision Making*, *8*(4), 407–424. https://doi.org/10.1017/S1930297500005271

119. Kahneman, D. (2013). *Thinking, fast and slow* (First paperback edition). Farrar, Straus and Giroux.

120. Kalenský, J., & Hanhijärvi, H. (2025). *Countering disinformation in the Euro-Atlantic: Strengths and gaps* [Hybrid CoE Research Report 15]. Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2025/10/Hybrid_CoE_Research_Report_15_Countering_disinformation_Euro_Atlantic.pdf

121. Kalenský, J., & Osadchuk, R. (January 24). *How Ukraine fights Russian disinformation: Beehive vs mammoth* [Hybrid CoE Research Report 11]. Hybrid CoE.

https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf

122. Kent, S. (1964). *Words of estimate probability*. CIA. https://www.cia.gov/readingroom/docs/CIA-RDP93T01132R000100020036-3.pdf

123. Khan, S. A., Dierickx, L., Furuly, J., Vold, H. B., Tahseen, R., Linden, C., & Dang-Nguyen, D. (2025). Debunking war information disorder: A case study in assessing the use of multimedia verification tools. *Journal of the Association for Information Science and Technology*, *76*(5), 752–769. https://doi.org/10.1002/asi.24970

124. Koronska, K., Benzoni, P., Lompe, M., Neverovskaja, L., Schafer, B., & Rogers, R. (2024, March 13). From Russia With Spin: How Content From Russian State Media is Laundered by Polish Blogs. *Alliance For Securing Democracy*. https://securingdemocracy.gmfus.org/from-russia-with-spin-how-content-from-russian-state-media-is-laundered-by-polish-blogs/

125. Krafft, P. M., & Donovan, J. (2020). Disinformation by Design: The Use of Evidence Collages and Platform Filtering in a Media Manipulation Campaign. *Political Communication*, *37*(2), 194–214. https://doi.org/10.1080/10584609.2019.1686094

126. Krippendorff, K. (2019). *Content Analysis: An Introduction to Its Methodology*. SAGE Publications, Inc. https://doi.org/10.4135/9781071878781

127. Kuvaldin, S. (2022, December 7). *Why Russia Keeps Insisting That Poland Is Preparing to Partition Ukraine*. Carnegie Endowment for International Peace. https://carnegieendowment.org/russia-eurasia/politika/2022/12/why-russia-keeps-insisting-that-poland-is-preparing-to-partition-ukraine

128. Lasswell, H. D. (1927). *Propaganda technique in World War*. Kegan Paul, Trench, Trubner & Co., Ltd.

129. Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018). The science of fake news. *Science*, *359*(6380), 1094–1096. https://doi.org/10.1126/science.aao2998

130. Lewandowsky, S., Ecker, U. K. H., Seifert, C. M., Schwarz, N., & Cook, J. (2012). Misinformation and Its Correction: Continued Influence and Successful Debiasing. *Psychological Science in the Public Interest*, *13*(3), 106–131. https://doi.org/10.1177/1529100612451018

131. Light, B., Burgess, J., & Duguay, S. (2018). The walkthrough method: An approach to the study of apps. *New Media & Society*, *20*(3), 881–900. https://doi.org/10.1177/1461444816675438

132. Lilly, B., & Cheravitch, J. (2020). *The Past, Present, and Future of Russia's Cyber Strategy and Forces*. 27. https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf

133. Linvill, D. L., & Warren, P. L. (2020). Troll Factories: Manufacturing Specialized Disinformation on Twitter. *Political Communication*, *37*(4), 447–467. https://doi.org/10.1080/10584609.2020.1718257

134. Linvill, D., & Warren, P. (2023). Infektion's Evolution: Digital Technologies and Narrative Laundering. *Media Forensics Hub Reports*. https://open.clemson.edu/mfh_reports/3

135. Liu, K., Geng, X., & Liu, X. (2022). The application of network agenda setting model during the COVID-19 pandemic based on latent dirichlet allocation topic modeling. *Frontiers in Psychology*, *13*, 954576. https://doi.org/10.3389/fpsyg.2022.954576

136. Martin Laine [@Martinlaineolen]. (2024, September 16). *Breaking news: Leaked docs from a Kremlin-controlled propaganda machine reveal a campaign backing far-right parties in EU elections and spreading disinformation to undermine Ukraine. Read further: Https://vsquare.org/leaked-files-putin-troll-factory-russia-european-elections-factory-of-fakes/ Let's dive into the #FactoryofFakes 1/15* [Tweet]. Twitter. https://x.com/Martinlaineolen/status/1835697494711304622

137. Mazza, M., Avvenuti, M., Cresci, S., & Tesconi, M. (2022). Investigating the difference between trolls, social bots, and humans on Twitter. *Computer Communications*, *196*, 23–36. https://doi.org/10.1016/j.comcom.2022.09.022

138. McCombs, M. E., & Shaw, D. L. (1972). The Agenda-Setting Function of Mass Media. *The Public Opinion Quarterly*, *36*(2), Article 2.

139. McCombs, M. E., Shaw, D. L., & Weaver, D. H. (2014). New Directions in Agenda-Setting Theory and Research. *Mass Communication and Society*, *17*(6), 781–802. https://doi.org/10.1080/15205436.2014.964871

140. McCombs, M., Llamas, J. P., Lopez-Escobar, E., & Rey, F. (1997). Candidate Images in Spanish Elections: Second-Level Agenda-Setting Effects. *Journalism & Mass Communication Quarterly*, *74*(4), 703–717. https://doi.org/10.1177/107769909707400404

141. McGuire, W. J. (1964). Some Contemporary Approaches. In *Advances in Experimental Social Psychology* (Vol. 1, pp. 191–229). Elsevier. https://doi.org/10.1016/S0065-2601(08)60052-0

142. McInnes, L., Healy, J., & Melville, J. (2018). *UMAP: Uniform Manifold Approximation and Projection for Dimension Reduction* (Version 3). arXiv. https://doi.org/10.48550/ARXIV.1802.03426

143. Meister, S. (2016). The "Lisa case": Germany as a target of Russian disinformation. *NATO Review*. https://web.archive.org/web/20161007075714/http://www.nato.int/docu/review/2016/also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm

144. Meleshevich, K., & Schafer, B. (2018, January 9). Online Information Laundering: The Role of Social Media. *Alliance For Securing Democracy*. https://securingdemocracy.gmfus.org/online-information-laundering-the-role-of-social-media/

145. Menn, J. (2024, June 2). News site editor's ties to Iran, Russia show misinformation's complexity. *The Washington Post*. https://www.washingtonpost.com/technology/2024/06/02/grayzone-russia-iran-support/

146. Meta. (2018). *Inauthentic Behavior | Transparency Center*. https://transparency.meta.com/policies/community-standards/inauthentic-behavior/

147. Microsoft. (2023, December 7). *Російські джерела загроз готуються скористатися втомою від війни*. https://www.microsoft.com/uk-ua/security/security-insider/intelligence-reports/russian-threat-actors-dig-in-prepare-to-seize-on-war-fatigue

148. Microsoft. (2024, April 17). Russian US election interference targets support for Ukraine after slow start. *Microsoft On the Issues*. https://blogs.microsoft.com/on-the-issues/2024/04/17/russia-us-election-interference-deepfakes-ai/

149. Miskimmon, A., O'Loughlin, B., & Roselle, L. (2013). *Strategic narratives: Communication power and the new world order*. Routledge.

150. Morozova, A., & Laine, M. (2024, September 16). Leaked Files from Putin's Troll Factory: How Russia Manipulated European Elections. *VSquare.Org*. https://vsquare.org/leaked-files-putin-troll-factory-russia-european-elections-factory-of-fakes/

151. Mueller, R. S. (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (p. 207). Department of Justice. https://www.justice.gov/storage/report_volume1.pdf

152. Myers, S. L. (2025, May 15). Trump Administration Cancels Scores of Grants to Study Online Misinformation. *The New York Times*. https://www.nytimes.com/2025/05/15/business/trump-online-misinformation-grants.html

153. NewsGuard. (2024, September 12). *A well-funded Moscow-based global 'news' network has infected Western artificial intelligence tools worldwide with Russian propaganda*. https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global

154. Nimmo, B. (2017, November 16). How A Russian Troll Fooled America. *DFRLab*. https://medium.com/dfrlab/how-a-russian-troll-fooled-america-80452a4806d1

155. Nimmo, B., & Torrey, M. (2022). *Taking down coordinated inauthentic behavior from Russia and China* (p. 51). Meta. https://about.fb.com/wp-content/uploads/2022/10/CIB-Report_-China-Russia_Sept-2022-1-1.pdf

156. Noelle-Neumann, E. (1993). *The spiral of silence: Public opinion, our social skin* (2nd ed). University of Chicago Press.

157. Nye, J. S. (2009). *Soft power: The means to success in world politics*. PublicAffairs.

158. Odarchenko, K., & Poznii, O. (2024, July 31). *Ukrainians See Corruption as a Key Issue Even During the War | Wilson Center*. https://www.wilsoncenter.org/blog-post/ukrainians-see-corruption-key-issue-even-during-war

159. Office of the Director of National Intelligence. (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* (p. 25). https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-filesations-ica-2017-01.pdf

160. Office of the Director of National Intelligence. (2023). *ICD 203 Analytic standards* [Intelligence Community Directive]. Office of the Director of National Intelligence. https://www.dni.gov/files/documents/ICD/ICD-203.pdf

161. O'Keefe, D. J. (2012). The Elaboration Likelihood Model. In J. Dillard & L. Shen, *The SAGE Handbook of Persuasion: Developments in Theory and Practice* (pp. 137–149). SAGE Publications, Inc. https://doi.org/10.4135/9781452218410.n9

162. OpenAI. (2024). *Influence and cyber operations: An update* (p. 54). OpenAI. https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf

163. Osadchuk, R. The model of Russian disinformation after the large-scale invasion of Ukraine: The case of 'Ukraine sells Western arms' narrative. *ECREA 2024, 10th European Communication Conference* (4–27 September 2024, Slovenia), Book of Abstracts, P. 99-100. https://flore.unifi.it/bitstream/2158/1392253/1/ECREA-2024-Abstract-Book.pdf

164. 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

165. Osadchuk, R. (2022, October 14). Pro-Kremlin influencers reignite Zelenskyy "green screen" theory. *DFRLab*. https://medium.com/dfrlab/pro-kremlin-influencers-reignite-zelenskyy-green-screen-theory-d827f761d17d

166. Osadchuk, R. (2023a, March 9). Seven steps to spread a conspiracy: How Russia promoted weapons trade allegations. *Digital Forensic Research Lab (DFRLab)*. https://medium.com/dfrlab/seven-steps-to-spread-a-conspiracy-how-russia-promoted-weapons-trade-allegations-a3e80ebedaf5

167. Osadchuk, R. (2023b, December 14). *Massive Russian influence operation targeted former Ukrainian defense minister on TikTok*. https://dfrlab.org/2023/12/14/massive-russian-influence-operation-targeted-former-ukrainian-defense-minister-on-tiktok/

168. Osadchuk, R., Adam, I., Gigitashvili, G., & Furbish, M. (2024, December 18). How inauthentic accounts exploit Telegram comments to spread anti-Ukrainian narratives. *DFRLab*. https://dfrlab.org/2024/12/18/inauthentic-telegram-accounts-ukraine/

169. Owens, R. (2024, May 7). *Corruption in Ukraine and EU Accession*. https://cddrl.fsi.stanford.edu/news/corruption-ukraine-and-eu-accession

170. Pacepa, I. M., & Rychlak, R. J. (2013). *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*.

171. Pamment, J. (2020). *The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework* (Future Threats, Future Solutions 2, p. 26). Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Pamment_-_Crafting_Disinformation_1.pdf

172. Pamment, J., & Tsurtsumia, D. (2025). *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency*. Psychological Defence Research Institute. https://mpf.se/psychological-defence-agency/publications/archive/2025-05-15-beyond-operation-doppelganger-a-capability-assessment-of-the-social-design-agency

173. Pariser, E. (2012). *The filter bubble: What the Internet is hiding from you*. Penguin books.

174. 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

175. Pelham [@Resist_05]. (2023, July 18). *Ukraine Defense Minister, Oleksii Reznikov just purchased this 7 million euro mansion in Cannes, France for his daughter's wedding present… Oleksii Reznikov is said to have a net worth of 1 million… just in case you wondered where all the money was going https://t.co/VQVTF86iCf* [Tweet]. Twitter. https://x.com/Resist_05/status/1681096634854436865

176. Pennycook, G., Epstein, Z., Mosleh, M., Arechar, A. A., Eckles, D., & Rand, D. G. (2021). Shifting attention to accuracy can reduce misinformation online. *Nature*, *592*(7855), 590–595. https://doi.org/10.1038/s41586-021-03344-2

177. 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

178. Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of Persuasion. In *Advances in Experimental Social Psychology* (Vol. 19, pp. 123–205). Elsevier. https://doi.org/10.1016/S0065-2601(08)60214-2

179. Pocheptsov, G. (2018). Cognitive Attacks in Russian Hybrid Warfare. *Information & Security: An International Journal*, *41*, 37–43. https://doi.org/10.11610/isij.4103

180. Porten-Cheé, P., & Eilders, C. (2015). Spiral of silence online: How online communication affects opinion climate perception and opinion expression regarding the climate change debate. *Studies in Communication Sciences*, *15*(1), 143–150. https://doi.org/10.1016/j.scoms.2015.03.002

181. Poynter. (2026). International Fact-Checking Network. *Poynter*. https://www.poynter.org/ifcn/

182. Pratkanis, A. R., & Aronson, E. (1992). *Age of propaganda: The everyday use and abuse of persuasion* (1st ed.). Freeman. https://www.scribd.com/document/216582785/Age-of-Propaganda-Anthony-R-Pratkanis-Elliot-Aronson

183. Qurium Media Foundation. (2022, September 27). *Under the hood of a Doppelgänger – Qurium Media Foundation*. https://www.qurium.org/alerts/under-the-hood-of-a-doppelganger/

184. Ramsay, G., & Robertshaw, S. (2019). *Weaponising news RT, Sputnik and targeted disinformation* (p. 140). King's College London Centre for the Study of Media, Communication & Power. https://www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf

185. RAND Corp. (2026). *Factcheck.org*. https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/factcheckorg.html

186. Recorded Future. (2024a). *Russia-Linked CopyCop Expands to Cover US Elections, Target Political Leaders*. Recorded Future. https://assets.recordedfuture.com/insikt-report-pdfs/2024/cta-ru-2024-0624.pdf

187. Recorded Future. (2024b). *Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale* (p. 23). Recorded Future. https://web.archive.org/web/20240514121830/https://go.recordedfuture.com/hubfs/reports/cta-2024-0509.pdf

188. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

189. Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

190. Robinson, O., Robinson, A., & Sardarizadeh, S. (2023, December 15). Ukraine war: How TikTok fakes pushed Russian lies to millions. *BBC*. https://www.bbc.com/news/world-europe-67687449

191. Romaniuk, V. (2024). Disinformation narratives of hate as a tool of escalating Russia's war against Ukraine (based on stopfake fact-checking project materials). *The Estonian Journal of Military Studies*, 143-157 Pages. https://doi.org/10.15157/ST.VI23.24202

192. Romaniuk, V. (2025). Transforming media education to counter disinformation: fact-checking, Stratcom, AI. *Obraz*, (2 (48)), 168–178. https://doi.org/10.21272/Obraz.2025.2(48)-168–178

193. Romanuk, V. S., & Fedchenko, Y. M. (2025). Media education as a tool of national security: the strategic function of stopfake in countering disinformation. *"Scientific Notes of*

V. I. Vernadsky Taurida National University", Series: "Philology. Journalism," 2(5), 299–305. https://doi.org/10.32782/2710-4656/2025.5.2/43

194. Romero, L. (2022, August 12). How 'War on Fakes' uses fact-checking to spread pro-Russia propaganda. *Poynter*. https://www.poynter.org/fact-checking/2022/how-war-on-fakes-uses-fact-checking-to-spread-pro-russia-propaganda/

195. Roozenbeek, J., & Van Der Linden, S. (2019). Fake news game confers psychological resistance against online misinformation. *Palgrave Communications*, *5*(1), 65. https://doi.org/10.1057/s41599-019-0279-9

196. Roozenbeek, J., & Van Der Linden, S. (2020). Breaking Harmony Square: A game that "inoculates" against political misinformation. *Harvard Kennedy School Misinformation Review*. https://doi.org/10.37016/mr-2020-47

197. Roozenbeek, J., Van Der Linden, S., Goldberg, B., Rathje, S., & Lewandowsky, S. (2022). Psychological inoculation improves resilience against misinformation on social media. *Science Advances*, *8*(34), eabo6254. https://doi.org/10.1126/sciadv.abo6254

198. RT. (2016, December 13). *'Putin did it': CIA mercilessly trolled with #RussianHack blame game*. RT International. https://www.rt.com/viral/370140-russian-hack-memes-cia/

199. Ruths, D., & Pfeffer, J. (2014). Social media for large studies of behavior. *Science*, *346*(6213), 1063–1064. https://doi.org/10.1126/science.346.6213.1063

200. Schafer, B., Benzoni, P., Koronska, K., Rogers, R., & Reyes, K. (2024). *The Russian Propaganda Nesting Doll*. GMF. https://www.gmfus.org/sites/default/files/2024-05/Laundromat%20Paper.pdf

201. Sciutto, J., Lister, T., & Ilyushina, M. (2017, October 17). *Putin's 'chef,' the man behind the troll factory | CNN Politics*. CNN. https://www.cnn.com/2017/10/17/politics/russian-oligarch-putin-chef-troll-factory

202. Shao, C., Ciampaglia, G. L., Varol, O., Yang, K.-C., Flammini, A., & Menczer, F. (2018). The spread of low-credibility content by social bots. *Nature Communications*, *9*(1), 4787. https://doi.org/10.1038/s41467-018-06930-7

203. Shifman, L. (2013a). Memes in a Digital World: Reconciling with a Conceptual Troublemaker. *Journal of Computer-Mediated Communication*, *18*(3), 362–377. https://doi.org/10.1111/jcc4.12013

204. Shifman, L. (2013b). *Memes in Digital Culture*. The MIT Press. https://doi.org/10.7551/mitpress/9429.001.0001

205. Snegovaya, M. (2015). *Putin's information warfare in ukraine*. https://www.files.ethz.ch/isn/193932/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf

206. Snopes. (2026). *About Us | Snopes.com*. Retrieved April 28, 2026, from https://www.snopes.com/about/

207. Spike, J. (2026, March 26). *Hungary's government files charges against prominent journalist for alleged espionage*. AP News. https://apnews.com/article/hungary-files-charges-journalist-espionage-d24d501efcbfa0240e905aa0cb22fbc4

208. Starbird, K., Arif, A., & Wilson, T. (2019). Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1–26. https://doi.org/10.1145/3359229

209. Starbird, Kate. (2018, October 21). *The Trolls Within: How Russian Information Operations Infiltrated Online Communities*. https://web.archive.org/web/20181021144612/https://medium.com/@katestarbird/the-trolls-within-how-russian-information-operations-infiltrated-online-communities-691fb969b9e4

210. Stetsenko, M. (2024, June 13). Corruption in Ukraine: Myths and Reality. *Just Security*. https://www.justsecurity.org/96190/ukraine-corruption-myths-reality/

211. Tandoc, E. C., Lim, Z. W., & Ling, R. (2018). Defining "Fake News": A typology of scholarly definitions. *Digital Journalism*, *6*(2), 137–153. https://doi.org/10.1080/21670811.2017.1360143

212. Taranenko, A. (2023). Critical discourse analysis for studying disinformation. *Politology Bulletin*, (90), 175–185. https://doi.org/10.17721/2415-881x.2023.90.175-185

213. Terp, S., & Breuer, P. (2022). DISARM: A Framework for Analysis of Disinformation Campaigns. *2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, 1–8. https://doi.org/10.1109/CogSIMA54611.2022.9830669

214. The Economist. (2024, May 1). The truth behind Olena Zelenska's $1.1m Cartier haul. *The Economist*. https://www.economist.com/interactive/science-and-technology/2024/05/01/the-truth-behind-olena-zelenskas-cartier-haul

215. Thomas, T. (2004). Russia's Reflexive Control Theory and the Military. *The Journal of Slavic Military Studies*, *17*(2), 237–256. https://doi.org/10.1080/13518040490450529

216. TikTok. (n.d.). *Community Guidelines Enforcement Report (Jul—Sep 2023)*. Retrieved June 14, 2025, from https://www.tiktok.com/transparency/en-us/community-guidelines-enforcement-2023-3/

217. TinEye. (2026). *Ukrainian soldiers*. TinEye. https://tineye.com/search/d163c7e9d172803e19fd6c7467db2ee628885317

218. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). *DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection* (arXiv:2001.00179). arXiv. https://doi.org/10.48550/arXiv.2001.00179

219. Turton, J., Smith, R. E., & Vinson, D. (2021). Deriving Contextualised Semantic Features from BERT (and Other Transformer Model) Embeddings. *Proceedings of the 6th Workshop on Representation Learning for NLP (RepL4NLP-2021)*, 248–262. https://doi.org/10.18653/v1/2021.repl4nlp-1.26

220. United States Department of State. (2023, November 7). *The Kremlin's Efforts to Covertly Spread Disinformation in Latin America—United States Department of State*. https://web.archive.org/web/20260327180654/https://2021-2025.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america/

221. United States Department of State. (2024, March 20). Imposing Sanctions on Actors Supporting Kremlin-Directed Disinformation Efforts. *United States Department of State*. https://2021-2025.state.gov/imposing-sanctions-on-actors-supporting-kremlin-directed-disinformation-efforts/

222. U.S. Department of the Treasury. (2022, February 22). *U.S. Treasury Imposes Immediate Economic Costs in Response to Actions in the Donetsk and Luhansk Regions*. U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/jy0602

223. US Joint Chief of Staff. (2012). *Joint Publication 3-13 Information Operations*. US Joint Chief of Staff. https://irp.fas.org/doddir/dod/jp3_13.pdf

224. Uscinski, J. E. (2017). The Study of Conspiracy Theories. *Argumenta*, *3*(2), 1–13. https://doi.org/10.23811/53.arg2017.usc

225. Van Der Linden, S., Leiserowitz, A., Rosenthal, S., & Maibach, E. (2017). Inoculating the Public against Misinformation about Climate Change. *Global Challenges*, *1*(2), 1600008. https://doi.org/10.1002/gch2.201600008

226. Van Dijk, T. A. (2008). *Discourse and Power*. Macmillan Education UK. https://doi.org/10.1007/978-1-137-07299-3

227. 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

228. Vatican. (2025). *Congregation for the Evangelization of Peoples Profile*. https://www.vatican.va/content/romancuria/en/congregazioni/congregazione-per-levangelizzazione-dei-popoli/profilo.html

229. Viginum. (2023). *RRN: A complex and persistent information manipulation campaign* [Technical report]. Viginum. https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf

230. Viginum. (2024a). *Portal Kombat: A structured and coordinated pro-Russian propaganda network*. https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

231. Viginum. (2024b). *Portal Kombat: A structured and coordinated pro-Russian propaganda network. Part 2* (p. 17).

https://www.sgdsn.gouv.fr/files/files/Publications/20240214_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_PART2_ENG_VF.pdf

232. Viginum. (2025). *Analysis of the Russian information manipulation set Storm-1516*. Viginum. https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf

233. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

234. Walter, N., Cohen, J., Holbert, R. L., & Morag, Y. (2020). Fact-Checking: A Meta-Analysis of What Works and for Whom. *Political Communication*, *37*(3), 350–375. https://doi.org/10.1080/10584609.2019.1668894

235. Wardle, C., & Derakhshan, H. (2017). *INFORMATION DISORDER: Toward an interdisciplinary framework for research and policy making*. Council of Europe. https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77

236. Warren, P., Linvill, D., Sheffield, S., Fecher, L., Gilbert, K., Greco, J., Gubanich, A., Gubanich, J., Hundley, P., Kea, E., Manson, C., May, E., Meadows, S., Pridnia, C., Rippy, M., Rockow, M., Ross, T., & Webb, P. (2024). Writers of the Storm: Who's Behind the Ongoing Production of Pro-Russian False Narratives. *Media Forensics Hub Creative Inquiry Reports*. https://open.clemson.edu/mfh_ci_reports/10

237. Warrick, J., & Troianovski, A. (n.d.). *How a powerful Russian propaganda machine chips away at Western notions of truth*. Washington Post. Retrieved February 11, 2026, from https://www.washingtonpost.com/graphics/2018/world/national-security/russian-propaganda-skripal-salisbury/

238. Welch, D. (2014). *Propaganda, power and persuasion: From World War I to Wikileaks*. I.B. Tauris.

239. Westlund, O., Belair-Gagnon, V., Graves, L., Larsen, R., & Steensen, S. (2024). What Is the Problem with Misinformation? Fact-checking as a Sociotechnical and Problem-Solving Practice. *Journalism Studies*, *25*(8), 898–918. https://doi.org/10.1080/1461670X.2024.2357316

240. Wood, T., & Porter, E. (2019). The Elusive Backfire Effect: Mass Attitudes' Steadfast Factual Adherence. *Political Behavior*, *41*(1), 135–163. https://doi.org/10.1007/s11109-018-9443-y

241. Woolley, S. C., & Howard, P. N. (Eds.). (2018). *Computational Propaganda* (Vol. 1). Oxford University Press. https://doi.org/10.1093/oso/9780190931407.001.0001

242. Yablokov, I. (2015). Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of *Russia Today* (*RT*). *Politics*, *35*(3–4), 301–315. https://doi.org/10.1111/1467-9256.12097

243. Zadrozny, B. (2024). *The disinformation pipeline: How Russian propaganda reaches and influences the U.S.* Retrieved April 4, 2026, from https://www.nbcnews.com/specials/russian-disinformation-2024-election-storm-1516/

244. Zakharchenko, A. (2025). Advantages of the connective strategic narrative during the Russian–Ukrainian war. *Frontiers in Political Science*, *7*, 1434240. https://doi.org/10.3389/fpos.2025.1434240

245. Zannettou, S., Caulfield, T., De Cristofaro, E., Sirivianos, M., Stringhini, G., & Blackburn, J. (2018). *Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web* (Version 2). arXiv. https://doi.org/10.48550/ARXIV.1801.09288

246. Біляївка.City. (2024, April 19). *Заступника голови Фонтанської сільради затримали в кабінеті: Отримав хабар за ухилення від служби*. Біляївка.City. https://bilyayivka.city/articles/355307/za-vinagorodu-zastupnik-golovi-fontanskoi-gromadi-dopomagav-cholovikam-uhilitisya-vid-mobilizacii

247. Богданьок, О. (2024, April 15). *Маляр вибачилася перед Совсун за суперечку в ефірі через демобілізацію яка довела до сліз—Суспільне Новини*. https://web.archive.org/web/20250101025627/https://suspilne.media/725025-malar-vibacilasa-pered-deputatkou-sovsun-aku-dovela-do-sliz-v-efiri-novogo-vidliku-na-suspilnomu/

248. Большая российская энциклопедия. (2023, January 12). *Информационная война*. Большая российская энциклопедия. https://bigenc.ru/c/informatsionnaia-voina-2b7815

249. Герасимов, В. (2013). *Ценность науки в предвидении*. https://www.abertzalekomunista.net/images/Liburu_PDF/Internacionales/Gerasimov_Valery/Cennost%20nauki%20v%20predvidenii%20-K.pdf

250. Звоздецька, О. (2022). Institutional Toolkit to Counter Fake News and Disinformation in the EU: Challenges and Achievements. *Mediaforum : Analytics, Forecasts, Information Management*, (10), 107–122. https://doi.org/10.31861/mediaforum.2022.10.107-122

251. Іваненко, М. (2026, January 5). *Плакат, що розколов країну: Хто і навіщо вигадав "три сорти" українців*. https://glavred.net/culture/plakat-raskolovshiy-stranu-kto-i-zachem-pridumal-tri-sorta-ukraincev-10729553.html

252. Квіт, С. (2008). *Масові коменікації: Підручник*. Видавничий дім «Києво-Могилянська академія».

253. Київська міська державна адміністрація. (2024, May 13). *«Київський метрополітен» оголошує тендер на продовження будівництва метро на Виноградар*. Офіційний портал КМДА - Головна. https://kyivcity.gov.ua/news/kivskiy_metropoliten_ogoloshuye_tender_na_prodovzhennya_budivnitstva_metro_na_vinogradar/

254. Министерство инностранных дел РФ. (2008). *Концепция внешней политики Российской Федерации—Министерство иностранных дел Российской Федерации*. https://www.mid.ru/ru/foreign_policy/news/1670707/

255. Министерство инностранных дел РФ. (2023, March 31). *Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В.В.Путиным 31 марта 2023 г.)—Министерство иностранных дел Российской Федерации*. https://www.mid.ru/ru/detail-material-page/1860586/

256. Министерство обороны РФ. (2011). Концептуальные взгляды на деятельность вооруженных сил российской федерации в информационном пространстве (p. 14). https://info.publicintelligence.net/RU-CyberStrategy.pdf

257. Мультимедиа Арт Музей, Москва. (2000). *Выставки: Чечня. 1994-1996. Чечня 1999-2000 (Мультимедиа Арт Музей, Москва)*. Мультимедиа Арт Музей, Москва. https://mamm-mdf.ru/exhibitions/chechnya-1994-1996-chechnya-1999-2000/

258. Осадчук, Р. Ю. (2023). Багатоступеневий підхід РФ у побудові і розповсюдженні дезінформації: приклад "продажу зброї". *Протидія дезінформації в умовах російської агресії проти України: виклики й перспективи: тези доповіді*. Учасників міжн. наук.-практ. конф. (Анн-Арбор - Харків, 12-13 груд. 2023 р.), с. 277-281. https://doi.org/10.32782/PPSS.2023.1.72

259. Осадчук Р.Ю. (2025a) Модель розповсюдження російської дезінформації. *Російська війна проти України: трансформації соціальних інституцій та практик: збірник тез науково-практичної конференції*. (24 лютого — 7 березня 2025 року, м. Київ). С. 28-32 https://ekmair.ukma.edu.ua/handle/123456789/36638

260. Осадчук, Р. Ю. (2025b). Російські дезінформаційні операції проти України під час широкомасштабного вторгнення: кейс-стаді. *Синопсис: текст, контекст, медіа*, 215. https://doi.org/10.28925/2311-259x.2025.3.10

261. Осадчук, Р.Ю. (2026). Теоретична рамка дослідження сучасних російських дезінформаційних операцій. *Обрії Друкарства*, (2026: Online first). https://doi.org/10.20535/2522-1078.2026.1(19).356053

262. РБК. (2017). *Шойгу рассказал о российских войсках информационных операций*. РБК. https://www.rbc.ru/politics/22/02/2017/58ad78cd9a794757f3c80ece

263. Родионов, М. (1998). К вопросу о формах ведения информационной борьбы. *Военная Мысль*, *2 (3-4)*. https://www.militaryarticle.vibrokatok.by/voennaya-mysl/1998-vm/8931-k-voprosu-o-formah-vedenija-informacionnoj-borby

264. Сайт президента России. (1997). *Указ Президента Российской Федерации от 17.12.1997 г. № 1300*. Президент России. http://kremlin.ru/acts/bank/11782

265. Сайт президента России. (2000). *Указ Президента Российской Федерации от 10.01.2000 г. № 24*. Президент России. http://kremlin.ru/acts/bank/14927

266. Сайт президента России. (2010). *Военная доктрина Российской Федерации*. Президент России. http://kremlin.ru/supplement/461

267. Сайт президента России. (2015, December 31). *Указ Президента Российской Федерации от 31.12.2015 г. № 683*. Президент России. http://kremlin.ru/acts/bank/40391

268. Сайт президента России. (2021, July 2). *Указ Президента Российской Федерации от 02.07.2021 г. № 400*. Президент России. http://kremlin.ru/acts/bank/47046

269. Сайт президента России. (2022, September 5). *Указ Президента Российской Федерации от 05.09.2022 г. № 611*. Президент России. http://kremlin.ru/acts/bank/48280

270. Совет Безопасности Российской Федерации. (2014, December 25). *Военная доктрина Российской Федерации*. Совет Безопасности Российской Федерации. http://www.scrf.gov.ru/security/military/document129/

271. Судово-юридична газета. (2024, January 5). *Київ закупив 30 скляних зупинок на понад 8 млн гривень—Sud.ua*. Судово-юридична газета. https://sud.ua/uk/news/ukraine/289852-kiev-zakupil-30-steklyannykh-ostanovok-na-bolee-8-mln-griven

272. Сунь-цзи. (2015). *Мистецтво війни*. Видавництво Старого Лева.

273. Яковлєв, М. (2023). *Теорії змов. Як (не) стати конспірологом*. Віхола.

ДОДАТОК А

ВИХІДНИЙ КОД ДЛЯ АНАЛІЗУ КОМЕНТАРІВ

```python
# Встановлення необхідних бібліотек
%pip install bertopic sentence-transformers umap-learn hdbscan plotly scikit-learn pandas openpyxl
```

```python
#імпорт необхідних бібліотек для BERTopic
import pandas as pd
import numpy as np
import re
import warnings
warnings.filterwarnings("ignore")
from sentence_transformers import SentenceTransformer
from umap import UMAP
from hdbscan import HDBSCAN
from sklearn.feature_extraction.text import CountVectorizer
from bertopic import BERTopic
from bertopic.representation import KeyBERTInspired, MaximalMarginalRelevance
import plotly.express as px
```

```
import plotly.io as pio
pio.renderers.default = "notebook"   # якщо запуск відбувається поза межами Jupyter - треба змінити на 'browser'
```

```python
# Конфігурація дослідження

CSV_PATH = "/doc1.csv" # Розташування CSV файлу, тобто набору даних
TEXT_COL = "text"                    # Назва стовпчика у таблиці, який містить текст коментарів
MIN_TEXT_LEN = 20                    # Параметр для ігнорування комірок з кількістю менше ніж 20

# Мультимовна модель ембедингів, яка сприймає контент багатьма мовами, включаючи українську та російську
EMBEDDING_MODEL = "paraphrase-multilingual-mpnet-base-v2"

# UMAP зменшення розмірності
```

```
UMAP_N_NEIGHBORS = 15            # Чим вищий показник, тим більш глобальна структура
UMAP_N_COMPONENTS = 5            # Розмірність HDBSCAN алгоритму (5 є стандартною опцією)
UMAP_MIN_DIST = 0.0              # мінімальна відстань = 0.0 працює для кластеризації

# HDBSCAN кластеризація
HDBSCAN_MIN_CLUSTER_SIZE = 50    # Мінімальна кількість документів для кластеру. Чим більший показник, тим менше тем, але вони широкі
HDBSCAN_MIN_SAMPLES = 10         # Контроль викідів; менше значення = менше винятків

# BERTopic словник
VECTORIZER_MIN_DF = 5            # Мінімальна частотність документів для термінів словника
VECTORIZER_NGRAM = (1, 2)

# Кількість топ ключових слів, які будуть відображені
TOP_N_WORDS = 10
```

Output files

OUTPUT_DOCS_CSV = "docs_with_topics.csv" # Назва документу, який демонструватиме всі документи разом з визначеними топіками

OUTPUT_TOPICS_CSV = "topic_summary.csv" # Назва документу з усіма визначеними темами

OUTPUT_MODEL_DIR = "bertopic_model" # Тека для збереження тренованої моделі

```

```python

#Завантаження набору даних й попередній перегляд

df = pd.read_csv(CSV_PATH)

print(f"Loaded {len(df):,} rows | Columns: {list(df.columns)}")

df.head(3)

```

```python

#Підчищення набору даних, прибирання зайвих пробілів, посилань, тощо

def preprocess_text(text: str) -> str:

```
    if not isinstance(text, str):
        return ""
    text = text.strip()
    # Collapse excessive whitespace
    text = re.sub(r"\s+", " ", text)
    # Remove URLs
    text = re.sub(r"https?://\S+", "", text)
    # Remove HTML entities
    text = re.sub(r"&[a-z]+;", " ", text)
    return text.strip()

df["text_clean"] = df[TEXT_COL].apply(preprocess_text)

# Ігнорування порожніх та коментарів, що містять менше 20 символів
before = len(df)
df = df[df["text_clean"].str.len() >= MIN_TEXT_LEN].reset_index(drop=True)
print(f"Dropped {before - len(df):,} short/empty rows. Remaining: {len(df):,}")
```

```python
#створення ембедингів коментарів
print(f"Loading embedding model: {EMBEDDING_MODEL}")
```

```
embedding_model = SentenceTransformer(EMBEDDING_MODEL)


docs = df["text_clean"].tolist()


print(f"Embedding {len(docs):,} documents...")
embeddings = embedding_model.encode(
    docs,
    show_progress_bar=True,
    batch_size=64,
    normalize_embeddings=True
)
print(f"Embeddings shape: {embeddings.shape}")
```

```python
#ініціалізація субмоделей для BERTopic
umap_model = UMAP(
    n_neighbors=UMAP_N_NEIGHBORS,
    n_components=UMAP_N_COMPONENTS,
    min_dist=UMAP_MIN_DIST,
    metric="cosine",
    random_state=42,
```

```
    low_memory=False
)

hdbscan_model = HDBSCAN(
    min_cluster_size=HDBSCAN_MIN_CLUSTER_SIZE,
    min_samples=HDBSCAN_MIN_SAMPLES,
    metric="euclidean",
    cluster_selection_method="eom",  # 'eom' дає більше кластерів
    prediction_data=True
)

# Векторизатор
vectorizer_model = CountVectorizer(
    ngram_range=VECTORIZER_NGRAM,
    min_df=VECTORIZER_MIN_DF,
    max_features=10_000
)

# Модель репрезентації тем
representation_model = MaximalMarginalRelevance(diversity=0.3)
```

```
print("Sub-models configured.")
```

```python
#налаштування моделі
topic_model = BERTopic(
    embedding_model=embedding_model,
    umap_model=umap_model,
    hdbscan_model=hdbscan_model,
    vectorizer_model=vectorizer_model,
    representation_model=representation_model,
    top_n_words=TOP_N_WORDS,
    language="multilingual",
    calculate_probabilities=False,   # Set True for soft assignments (slower)
    verbose=True
)

topics, _ = topic_model.fit_transform(docs, embeddings)

df["topic"] = topics
```

```
n_topics = len(set(topics)) - (1 if -1 in topics else 0)

n_outliers = topics.count(-1)

print(f"\n✓ Topics found: {n_topics}")

print(f"  Outlier docs (topic -1): {n_outliers:,} ({100*n_outliers/len(topics):.1f}%)")
```

```python
# верифікація результатів - кількість тем й перегляд перших 20 записів

topic_info = topic_model.get_topic_info()

print(f"Total topics (including -1 outlier): {len(topic_info)}")

topic_info.head(20)
```

```python
# Топ ключових слів для кожної теми

print("Top 10 topics by document count:\n")

for _, row in topic_info[topic_info.Topic != -1].head(10).iterrows():

    words = topic_model.get_topic(row.Topic)
```

```
    kw = ", ".join([w for w, _ in words[:8]])
    print(f"  Topic {row.Topic:3d}  ({row.Count:5,} docs)  → {kw}")
```

```python
# Додавання мітки теми (топ ключових слів) до кожного документу
def topic_label(t_id):
    if t_id == -1:
        return "outlier"
    words = topic_model.get_topic(t_id)
    return " | ".join([w for w, _ in words[:5]])

df["topic_label"] = df["topic"].apply(topic_label)
df[["id", "date", "platform", "source_name", "actor_name", "text_clean", "topic", "topic_label"]].head(10)
```

```python
# Перерозподіл документів-викидів до найближчої теми, на основі схожості ембедингу

new_topics = topic_model.reduce_outliers(docs, topics, strategy="embeddings", embeddings=embeddings, threshold=0.5)
```

```
topic_model.update_topics(docs, topics=new_topics)


df["topic"] = new_topics
df["topic_label"] = df["topic"].apply(topic_label)


n_outliers_after = list(new_topics).count(-1)
print(f"Outliers after reduction: {n_outliers_after:,}
({100*n_outliers_after/len(new_topics):.1f}%)")
```

```python
# Експортування документів
export_cols = ["id", "date", "url", "platform", "source_name", "source_url",
               "source_country", "source_verified", "actor_name", "actor_url",
               "text_clean", "topic", "topic_label"]


# Експортування стовпчиків, які дійсно існують
export_cols = [c for c in export_cols if c in df.columns]


df[export_cols].to_csv(OUTPUT_DOCS_CSV, index=False, encoding="utf-8-sig")
print(f"Saved document table → {OUTPUT_DOCS_CSV}")
```

```
    # Підсумкова таблиця тем
    topic_summary = topic_model.get_topic_info().copy()
    topic_summary["keywords"] = topic_summary["Topic"].apply(
        lambda t: ", ".join([w for w, _ in (topic_model.get_topic(t) or [])[:10]])
    )
    topic_summary.to_csv(OUTPUT_TOPICS_CSV, index=False, encoding="utf-8-sig")
    print(f"Saved topic summary  → {OUTPUT_TOPICS_CSV}")
```

ДОДАТОК Б

ПОСИЛАННЯ НА УПОРЯДКОВАНИЙ АРХІВ ОПЕРАЦІЇ «ДВІЙНИК»

https://drive.google.com/drive/folders/1rI2sKq-2upUw2sth1M6P47hfdFuqBgVM?usp=sharing

ДОДАТОК В

ПОСИЛАННЯ НА НАБІР ДАНИХ ТА РЕЗУЛЬТАТИ ТЕМАТИЧНОГО АНАЛІЗУ BERTOPIC

https://drive.google.com/drive/folders/1ckAmbY9-y44fXdJYB4JO_JUmVbV071NA?usp=sharing

Тека містить 3 файли:

1) Input dataset.csv — це вхідний набір даних з коментарями, які були проаналізовані
2) topic_summary.csv — таблиця зі всіма ідентифікованими алгоритмом тематичними кластерами
3) dataset_with_topics.csv — вхідний набір даних з коментарями, які асоційовані з визначеними темами.

ДОДАТОК Г

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. 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

2. Осадчук, Р. (2025). Російські дезінформаційні операції проти України під час широкомасштабного вторгнення: кейс-стаді. *Синопсис: текст, контекст, медіа*, 215. https://doi.org/10.28925/2311-259x.2025.3.10

3. Осадчук, Р. (2026). Теоретична рамка дослідження сучасних російських дезінформаційних операцій. *Обрії Друкарства*, (2026: Online first). https://doi.org/10.20535/2522-1078.2026.1(19).356053

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Osadchuk, R. (2024) The model of Russian disinformation after the large-scale invasion of Ukraine: The case of 'Ukraine sells Western arms' narrative. *ECREA 2024, 10th European Communication Conference Book of Abstracts*, p. 99-100. https://flore.unifi.it/bitstream/2158/1392253/1/ECREA-2024-Abstract-Book.pdf

2. Осадчук Р.Ю. (2025) Модель розповсюдження російської дезінформації. *Російська війна проти України: трансформації соціальних інституцій та практик: збірник тез науково-практичної конференції*, с. 28-32 https://ekmair.ukma.edu.ua/handle/123456789/36638

3. Осадчук, Р. Ю. (2023). Багатоступеневий підхід РФ у побудові і розповсюдженні дезінформації: приклад "продажу зброї". *Протидія дезінформації в умовах російської*

агресії проти України: виклики й перспективи: тези доповіді, с. 277-281. https://doi.org/10.32782/PPSS.2023.1.72

Публікації, які додатково відображають наукові результати дисертації

1. Kalenský, J., & Osadchuk, R. (2024). *How Ukraine fights Russian disinformation: Beehive vs mammoth* (p. 48) [Hybrid CoE Research Report 11]. Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf

Відомості про апробацію результатів дисертації

1. Osadchuk R. (2024, September 25) *The model of Russian disinformation after the large-scale invasion of Ukraine: The case of 'Ukraine sells Western arms' narrative* [Conference presentation]. 10th ECREA conference, Ljubljana, Slovenia.
2. Osadchuk R. (2025, September 25) *AI as a tool of disinfo weaponization* [Presentation]. Workshop of European Commission's Joint Research Center DISINFO Workshop, Brussels, Belgium
3. Osadchuk R. (2025, February 21-22) *Russian disinformation campaigns against Ukraine during the full-scale invasion*. International confrence «The Russo-Ukrainian War: Russia's information warfare strategies in comparative perspective». Ottawa, Canada. https://ruwconference.ca/
4. Osadchuk R. (2024, September 12) *Russia's hybrid war through different channels, tools, and continents* [Panel discussion]. Conference «Unveil the truth: Eastern Partnership fact-checking conference», Tbilisi, Georgia.
5. Osadchuk R. (2024, September 18) *Tip of the Spear: A report from the frontlines of the war on disinformation* [Panel discussion]. International conference «#Connexions 24. Extreme

in the Mainstream: Information Disorder, (Dis)engagement, & Digital (R)evolution», University of Texas, Austin, Texas, USA.

6. Osadchuk R. (2024, September 19) *Red Flags: Russia's & China's influence operations around the world* [Panel discussion]. International conference «#Connexions 24. Extreme in the Mainstream: Information Disorder, (Dis)engagement, & Digital (R)evolution», University of Texas, Austin, Texas, USA.

7. Osadchuk R., (2024, March 12-14) *Massive Russian influence operation targeted former Ukrainian defense minister on TikTok* [Conference presentation]. Department of Defense Global Information Conference «Forging The Future: from strategy to action». Washington, DC, USA.

8. Осадчук Р.Ю. (2023, 21 листопада) *Еволюція російської дезінформації та асиметрична відповідь України* [доповідь]. Наукова конференція «Революція Гідності: на шляху до історії» в Національному музеї Революції Гідності, м. Київ, Україна.

9. Осадчук Р.Ю. (2023, 30 листопада) *Багатоступеневий підхід російської дезінформації*. Науковий семінар Харківського національного університету Повітряних Сил імені Івана Кожедуба (ХНУПС) «Інформаційне протиборство в умовах російсько-української війни», м. Харків (онлайн), Україна.

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 07:54:46 25.06.2026

Назва файлу з підписом: Осадчук_дисертація.pdf.asice
Розмір файлу з підписом: 4.7 МБ

Перевірені файли:
Назва файлу без підпису: Осадчук_дисертація.pdf
Розмір файлу без підпису: 5.0 МБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: Осадчук Роман Юрійович
П.І.Б.: Осадчук Роман Юрійович
Країна: Україна
РНОКПП: 3366807230
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 07:54:42 25.06.2026
Сертифікат виданий: "Дія". Кваліфікований надавач електронних довірчих послуг
Серійний номер: 514B5C86A1E5DA1104000000A28C2A0010BBFC04
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними для перевірки (XAdES-B-LT)
Сертифікат: Кваліфікований

Версія від: 2026.05.15 13:00