УДК 007:316.77:004.738.5]:355.01(477)

Марія Якубовська, канд. філол. наук, доцент
Національний університет «Одеська політехніка», м. Одеса

OSINT-КОМУНІКАЦІЯ ТА ЦИФРОВА МЕДІАРЕАЛЬНІСТЬ ВІЙНИ: ТРАНСФОРМАЦІЯ ІНФОРМАЦІЙНИХ ПРАКТИК В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОГО ПРОТИСТОЯННЯ

Анотація. Досліджено трансформацію інформаційних практик у цифровому медіапросторі України в умовах російсько-української війни крізь призму розвитку OSINT-комунікації. Проаналізовано роль відкритої розвідки у формуванні цифрової медіареальності, процесах інформаційної верифікації, протидії дезінформації та розвитку громадянської журналістики. Особливу увагу приділено феноменам цифрової риторики, алгоритмічної комунікації та мережевої взаємодії у соціальних медіа. Визначено, що OSINT стає важливим елементом сучасних соціальних комунікацій, забезпечуючи оперативність, достовірність і цифрову резильєнтність суспільства в умовах інформаційної війни.

Ключові слова: OSINT-комунікація, цифрова медіареальність, інформаційна верифікація, цифрова риторика, медіадискурс, алгоритмічна комунікація, соціальні медіа, цифрова резильєнтність, інформаційна війна, соціальні комунікації.

Сучасний етап розвитку інформаційного суспільства характеризується масштабною цифровізацією комунікативних процесів, трансформацією медіасередовища та посиленням ролі інформації як стратегічного ресурсу. В умовах російсько-української війни особливого значення набувають новітні форми цифрової взаємодії, пов’язані з використанням відкритих джерел інформації, мережевих платформ і технологій оперативної верифікації даних. Так, у сучасному інформаційному суспільстві соціальні мережі функціонують і як важливе джерело даних, і як середовище формування громадської думки, а зростання масивів відкритої інформації актуалізує проблеми збору, обробки та інтерпретації даних, про що пишуть зокрема Д. Могилевич, В. Могилевич та І. Кононова вивчаючи OSINT-інструменти при дослідженні соцмереж [3]. Автори зазначають, що інструменти Open Source Intelligence, забезпечують автоматизований моніторинг контенту, аналіз профілів, соціальних зв’язків, геолокацій та інформаційних потоків. Водночас різна функціональність і обмеження доступу до даних зумовлюють необхідність компаративного та системного аналізу даних «залежно від функціональних особливостей кожної соціальної мережі для досягнення максимальної ефективності та релевантності отриманої інформації» [3, с. 235].

У цьому контексті феномен OSINT постає не лише як технологічний інструмент аналітики, як про це зазначає у свою чергу М. О. Думчиков [2], а і як самостійний соціокомунікаційний механізм формування цифрової медіареальності.

Сучасний медіапростір війни функціонує в умовах високої інформаційної турбулентності, де швидкість поширення повідомлень часто перевищує можли-

вості їх перевірки. Соціальні медіа, месенджери та цифрові платформи трансформувалися в основні канали оперативної комунікації, що водночас створює ризики поширення дезінформації, маніпулятивних наративів та інформаційно-психологічних операцій [1]. У зв'язку з цим OSINT-комунікація набуває особливого значення як система збору, аналізу та верифікації інформації з відкритих джерел. Дослідники наголошують, що сучасна відкрита розвідка [5] стала одним із ключових інструментів протидії інформаційним війнам та дезінформаційним кампаніям у цифровому середовищі. Та й взагалі «ефективна протидія інформаційним війнам залежить від здатності OSINT-аналітиків використовувати широкий спектр інструментів, що охоплюють різні типи відкритих даних» [2, с. 275].

У межах соціальних комунікацій OSINT варто розглядати не лише як технологію інформаційного пошуку, а як окремий тип цифрової комунікації, що поєднує елементи громадянської журналістики, медіааналітики, фактчекінгу та мережевої взаємодії. Зараз в умовах війни користувачі соціальних платформ дедалі частіше стають активними учасниками інформаційного процесу, здійснюючи збір даних, пошук і визначення геолокації об'єктів, аналізуючи фото- та відеоконтент, а також перевіряючи інформаційні повідомлення, про що пише зокрема Максим Соклаков [8]. Цей фактор формує нову модель комунікативної поведінки аудиторії, засновану на принципах цифрової участі та колективної інформаційної верифікації.

Сучасні OSINT-засоби є незамінними для моніторингу та інтерпретації контенту у Facebook, X (Twitter) та Instagram. Проте стрімке збільшення обсягів даних вимагає критичного оцінювання інструментарію через такі особливості:

– офіційні API, які гарантують легальність, обмежують обсяг доступної інформації та потребують авторизації;

– спеціалізовані скрипти (на кшталт Twint чи OSINTgram) забезпечують глибший пошук, проте дуже залежать від технічних змін на платформах;

– комплексні платформи (Maltego тощо) ефективні для візуалізації зв'язків і синтезу даних, але є складними в опануванні та дороговартісними;

– сервіси архівування є важливими для фіксації цифрових доказів, що особливо актуально під час аналізу інформаційних протистоянь [3, с. 241].

Соціальні медіа-платформи перетворилися на дискурсивний простір інформаційного протистояння, у якому поєднуються офіційна комунікація, громадянський контент, візуальні наративи та алгоритмічне поширення інформації [1–8]. Дослідники зазначають, що цифрові платформи сьогодні є не лише каналами передачі інформації, а й середовищем конструювання суспільної реальності та формування колективних смислів [8].

У цьому контексті особливу роль відіграє цифрова риторика як система мовленнєвих і мультимедійних стратегій впливу у мережевому середовищі. Воєнний

медіадискурс характеризується високим рівнем емоційності, символізації та прагматичної спрямованості. Використання візуальних образів, меметичних конструкцій, коротких відеоформатів і мережевих наративів формує нові механізми інформаційного впливу та колективної мобілізації суспільства. Водночас алгоритмізація цифрових платформ створює ризики інформаційних маніпуляцій, поширення фейків та штучного підсилення окремих наративів [1; 2].

Дуже актуальною постає проблема використання штучного інтелекту у системі інформаційного протиборства, про що детально пишуть Олена Артеменкова, Валерія Василенко і Лілія Ковтун: «Центр стратегічних комунікацій та інформаційної безпеки вже активно використовує можливості штучного інтелекту для моніторингу медіа та виявлення ворожих інформаційних атак» [1, с. 5]. Новітні алгоритмічні технології дедалі активніше застосовуються для створення маніпулятивного контенту, deepfake-матеріалів, автоматизованих ботомереж, інформаційно-психологічних операцій та іншого специфічного контенту. Сучасні наукові дослідження підкреслюють, що штучний інтелект перетворюється на важливий інструмент ведення інформаційної війни у соціальних медіа, а алгоритми соцмереж не є нейтральними. У контексті сучасних інформаційних протиборств соціальні медіа трансформувалися у потужний інструмент маніпулятивного впливу. Це зумовлює критичну потребу в інтеграції технологічних рішень для ідентифікації штучно створеного контенту. Пріоритетними векторами захисту інформаційного простору є як підвищення рівня цифрової гігієни користувачів, так і впровадження алгоритмічних систем моніторингу, що здатні розпізнавати дезінформацію в режимі реального часу [1, с. 6].

Водночас український інформаційний простір демонструє високий рівень цифрової резильєнтності, що проявляється у здатності суспільства адаптуватися до інформаційних загроз, протидіяти дезінформації та підтримувати ефективну мережеву комунікацію, це є надважливим, оскільки російсько-українська війна є не лише військовим, а й наративним конфліктом, як на то доречно вказує Галина Петришин [7]. Значну роль у цьому процесі відіграють стратегічні комунікації держави, цифрові інформаційні кампанії, волонтерські OSINT-спільноти та незалежні фактчекінгові ініціативи, бо у сучасній війні надзвичайно важлива швидкість реакції, і, так, Україна під час війни створила нову модель цифрової стратегічної комунікації як вказує зокрема М. М. Науменко [4]. Саме синергія офіційної комунікації та громадянської цифрової активності формує нову модель інформаційної стійкості суспільства.

Отже, OSINT-комунікація в умовах російсько-української війни постає складним міждисциплінарним феноменом, що інтегрує технологічні, соціокомунікаційні та медіадискурсивні аспекти. Вона трансформує сучасні інформаційні практи-

ки, змінює моделі споживання й верифікації інформації та формує нові механізми цифрової взаємодії у суспільстві. Подальше дослідження OSINT-комунікації є перспективним напрямом розвитку соціокомунікаційної науки, медіалінгвістики та цифрової риторики в умовах сучасних інформаційних викликів.

Список використаних джерел

1. Артеменкова О., Василенко В., Ковтун Л. Використання штучного інтелекту в соціальних мережах як зброї інформаційної війни. *Вісник Книжкової палати.* 2025. № 8(349). С. 3–8. DOI: 10.36273/2076-9555.2025.8(349).

2. Думчиков М. О. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі. *Аналітично-порівняльне правознавство.* 2025. № 6. DOI: 10.24144/2788-6018.2025.06.2.43.

3. Могилевич Д., Могилевич В., Кононова І. Аналіз OSINT інструментів для дослідження соціальних мереж. *Herald of Khmelnytskyi National University. Technical Sciences.* 2025. № 359(6.1). С. 235–242. DOI: 10.31891/2307-5732-2025-359-33.

4. Науменко М. М. Стратегічна комунікація в інформаційній війні України. *Acta Securitatae Volynienses.* 2025. № 6. DOI: 10.32782/2786-9385/2025-6-22.

5. Онкович А. Соцмережа Фейсбук та інформаційно-психологічні операції. *Український інформаційний простір.* 2021. № 1(7). С. 98–107. DOI: 10.31866/2616-7948.1(7).2021.233974.

6. Петренко С., Назаренко Н. Практичні аспекти ведення інформаційної війни в онлайн просторі. *Інформаційні технології та суспільство.* 2024. № 1. DOI: 10.32689/maup.it.2024.1.12.

7. Петришин Г. Інформаційна війна Росії проти України: еволюція основних засобів, методів та динаміка наративів. *Наукові праці МАУП. Політичні науки та публічне управління.* 2025. № 1(77). DOI: 10.32689/2523-4625-2025-1(77)-17.

8. Соклаков М. Соціальні медіа-платформи як дискурсивне середовище в контексті російсько-української війни. *Українські культурологічні студії*. 2025. № 1(16). DOI: 10.17721/UCS.2025.1(16).04.