УДК 342
DOI https://doi.org/10.24144/2788-6018.2025.06.2.43

ВІДКРИТА РОЗВІДКА (OSINT) У ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВІЙНАМ: АНАЛІТИЧНІ ІНСТРУМЕНТИ ТА ПРАВОВІ МЕЖІ

Думчиков М.О,
доктор юридичних наук, доцент,
доцент кафедри кримінально правових дисциплін
та судочинства
Навчально-наукового інституту права СумДУ
ORCID: 0000-0002-4244-2419

Думчиков М.О. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі.

Стаття присвячена комплексному дослідженню відкритої розвідки Open Source Intelligence – OSINT як одного з ключових інструментів протидії інформаційним війнам, дезінформаційним кампаніям та гібридним загрозам у сучасному цифровому середовищі. Актуальність дослідження зумовлена зростанням масштабів інформаційних впливів, використанням соціальних медіа для маніпуляції суспільною думкою та посиленням ролі цифрових технологій у воєнно-політичних конфліктах. Зважаючи на виклики, продиктовані повномасштабною збройною агресією Російської Федерації проти України, особливу увагу приділено аналізу аналітичного потенціалу застосування OSINT у контексті виявлення, документування та спростування фейкових наративів, збору доказів воєнних злочинів і зміцнення стратегічних комунікацій держави.

У роботі здійснено класифікацію основних напрямів OSINT, зокрема геопросторова розвідка, соціальна медіа-розвідка, технічна розвідка та окремих елементів HUMINT, що в сукупності формують багаторівневу систему збору, перевірки й верифікації даних з відкритих джерел. Розкрито методологічні підходи до аналізу інформації, алгоритми перевірки її достовірності, а також представлено сучасні інструменти автоматизації збору даних з використанням систем штучного інтелекту, зокрема AI-assisted OSINT, що істотно підвищують ефективність аналітичної діяльності.

Водночас, акцентовано на правових та етичних аспектах застосування відкритої розвідки, пов'язаних із захистом персональних даних, дотриманням принципів законності, пропорційності та мінімізації обробки інформації відповідно до вимог Загального регламенту ЄС із захисту даних. Проаналізовано національні та міжнародні підходи до врегулювання правомірності використання OSINT у правоохоронній і судовій практиці.

Наукова новизна дослідження полягає у поєднанні технологічного, правового та етичного вимірів використання OSINT як інструменту доказування та протидії інформаційним загрозам. У результаті, зроблено висновок про доцільність формування уніфікованих міжнародних стандартів збору та верифікації OSINT-даних, що забезпечать їх легітимність у кримінальному судочинстві, сприятимуть підвищенню рівня інформаційної безпеки держави та становленню культури відповідального й етичного використання відкритих джерел у демократичному суспільстві.

Ключові слова: відкрита розвідка, OSINT, інформаційна війна, дезінформація, штучний інтелект, кібербезпека, інформаційна безпека, цифрові докази, GDPR.

Dumchykov M.O. Open source intelligence (OSINT) in countering information wars: analytical tools and legal boundaries.

The article offers a comprehensive examination of Open Source Intelligence (OSINT) as one of the key instruments for countering information warfare, disinformation campaigns, and hybrid threats in the contemporary digital environment. The relevance of the research stems from the increasing scale of informational influence, the use of social media to manipulate public opinion, and the growing role of digital technologies in modern military-political conflicts. In light of the challenges triggered by the full-scale armed aggression of the Russian Federation against Ukraine, particular attention is devoted to analysing the analytical potential of OSINT in detecting, documenting, and refuting fake narratives, collecting evidence of war crimes, and strengthening the strategic communications of the state.

The study classifies the principal branches of OSINT, including geospatial intelligence (GeoINT), social media intelligence (SOCMINT), technical intelligence (TECHINT), and specific elements of human intelligence (HUMINT), which collectively form a multi-layered system of gathering, verifying, and validating data from open sources. The methodological approaches to information analysis and verification algorithms are elucidated, and contemporary tools for automating data collection using

artificial intelligence systems – particularly AI-assisted OSINT – are presented as means of significantly enhancing analytical efficiency.

At the same time, the article emphasises the legal and ethical dimensions of open-source intelligence, focusing on the protection of personal data and adherence to the principles of legality, proportionality, and data minimisation, in accordance with the requirements of the EU General Data Protection Regulation (GDPR). Both national and international approaches to the legal regulation of OSINT use in law-enforcement and judicial practice are analysed.

The scientific novelty of the study lies in the integration of technological, legal, and ethical dimensions of OSINT application as a tool for evidence gathering and countering informational threats. The paper concludes that the development of unified international standards for the collection and verification of OSINT data is essential to ensure their legitimacy in criminal proceedings, enhance state information security, and promote a culture of responsible and ethical use of open data within democratic societies.

Key words: open-source intelligence, OSINT, information war, disinformation, artificial intelligence, cybersecurity, information security, digital evidence, GDPR.

Постановка проблеми. Сучасні геополітичні конфлікти демонструють зсув парадигми війни, де маніпулювання інформацією та психологічні операції перетворилися на вирішальні елементи гібридних загроз. Варто акцентувати, що досвід російської агресії проти України яскраво ілюструє, як цілеспрямоване іноземне втручання та інформаційна маніпуляція можуть дестабілізувати суспільство та підірвати державні інституції [1].

Водночас, у відповідь на цю загрозу відкрита розвідка стала ключовим механізмом контррозвідувальної діяльності, що дозволяє як державним, так і недержавним акторам, зокрема, Bellingcat, InformNapalm, Molfar викривати фейки та встановлювати атрибуцію атак. Однак, незважаючи на значні успіхи, що закріпили легітимність OSINT як форми цифрового розслідування, зберігається критичний розрив між швидкістю поширення дезінформації та швидкістю її спростування [2].

На наше переконання, масове збирання, обробка та використання публічно доступних даних за для розслідувань неминуче вступає в конфлікт із традиційними правовими рамками. Тут, на нашу думку, нагальною проблемою є відсутність уніфікованих міжнародних та національних стандартів для верифікації OSINT-інформації, що ускладнює її трансформацію у належний доказ, особливо у кримінальному судочинстві, що стосується воєнних злочинів [3].

Це створює ситуацію, коли технологічний потенціал OSINT значно випереджає його правову інституціоналізацію. Таким чином, існує нагальна потреба у комплексному аналізі не лише технологічних можливостей, але й власне у критичному осмисленні правових імперативів та етичних обмежень, які забезпечать легітимність і стійкість застосування OSINT-даних у правовій площині.

Метою дослідження є комплексний аналіз сучасних аналітичних інструментів та методологій OSINT розвідки у контексті протидії інформаційним війнам, а також встановлення чітких правових та етичних меж, необхідних для легітимізації та використання OSINT-даних у правовій площині.

Стан опрацювання проблематики. Проблематика інформаційних війн та методів їх нейтралізації, зокрема засобами OSINT, активно досліджується як в Україні, так і за кордоном. Ми переконані, що значний внесок у аналіз дезінформаційних кампаній зробили міжнародні організації та структури безпеки. Так, наприклад, у 2015 році при ЄС створено East StratCom Task Force, яка веде проєкт EUvsDisinfo – базу даних ворожих фейків. Відтоді було накопичено величезний масив матеріалу, що становить понад 6000 випадків дезінформації, яку було задокументовано до 2019 року [4, с. 157]. Станом на 2024 рік тільки щодо війни в Україні зафіксовано понад 2800 окремих випадків дезінформації. Це свідчить про безпрецедентний розмах інформаційних атак [5].

Аналогічні висновки робить НАТО. Так, зокрема, за оцінкою Центру передового досвіду стратегічних комунікацій НАТО StratCom COE, російська дезінформація в ході останньої війни набула «небачених масштабів і зухвалості». Експерти StratCom наголошують, що успіх протидії агресії багато в чому залежить від посилення спроможностей у інформаційному просторі та ефективного використання OSINT для викриття ворожих впливів [6].

Варто наголосити, що активну роль у дослідженні та протидії дезінформації відіграють журналістські та громадські ініціативи. З 2014 року в Україні працює волонтерська спільнота StopFake, заснована на базі Могилянської школи журналістики, яка займається фактчекінгом пропаганди. Так, за перші чотири роки існування StopFake спростував понад тисячу фейкових новин про події в Україні [7].

На глобальному рівні відомою платформою розслідувальної OSINT-журналістики є колектив Bellingcat. Ця незалежна група дослідників прославилася розкриттям резонансних справ – від збиття рейсу MH17 на Донбасі до хімічних атак у Сирії. Варто наголосити, що в Україні виникають власні приватні OSINT-компанії, як-от Molfar, яка спочатку спеціалізувалася на бізнес-розвідці, проте з 2022 року її експерти активно залучилися до волонтерських розслідувань воєнної тематики.

Серед доктринальних досліджень застосування технологій OSINT варто виділити як вітчизняних науковців, так і зарубіжних дослідників. Зокрема, Серватнюк М.М. досліджував міжнародний, технологічний та юридичний аспекти OSINT, а також можливості їх імплементації у систему інформаційної безпеки під час розслідування кіберінцидентів. Серед зарубіжних дослідників варто відзначити Richard J. Aldrich та Brian D. Raymond, які досліджували застосування інструментів OSINT для виявлення та розслідування кіберзлочинів.

Таким чином, наукові й практичні напрацювання охоплюють широкий спектр – від аналітичних звітів StratCom COE до журналістських розслідувань Bellingcat і волонтерських кейсів StopFake та Molfar.

Виклад основного матеріалу. Сьогодні в рамках OSINT можна здобути розвідувальні відомості з усіх відкритих джерел санкціонованим способом. До них належать інтернет-ресурси, медіа, державні реєстри та бази даних, комерційні й наукові публікації. Варто зауважити, що 90% усієї розвідувальної інформації можна отримати саме з відкритих джерел.

Розвідка з відкритих джерел стала настільки ефективною та доступною, що її широко застосовують не лише спецслужби, а й журналісти-розслідувачі, громадські активісти та навіть звичайні громадяни. Так, зокрема, в Україні термін OSINT був відомий фахівцям давно, але на широку сцену вийшов із початком повномасштабної війни, коли, завдяки інструментам відкритої розвідки, журналісти почали відкрито допомагати ЗСУ виявляти ворожі позиції, знаходити докази воєнних злочинів та спростовувати пропагандистські міфи.

Ефективна протидія інформаційним війнам залежить від здатності OSINT-аналітиків використовувати широкий спектр інструментів, що охоплюють різні типи відкритих даних. Ми вважаємо, що класифікація цих інструментів допомагає структурувати розслідувальну діяльність. Так, зокрема, у таблиці № 1 представлено нашу класифікацію OSINT-інструментів.

Таблиця № 1. Класифікація інструментів OSINT

Тип OSINT-інструменту	Опис та приклади використання
GeoINT – Геопросторова розвідка [8].	Критично важливий інструмент, особливо в умовах збройного конфлікту. Використовує супутникові знімки, картографічні сервіси та відкриті GPS-трекери для верифікації місця та часу подій. Завдяки GeoINT стало можливим відстеження переміщення військ та документування пошкоджень інфраструктури під час повномасштабного вторгнення Росії в Україну.
SOCMINT – Розвідка соціальних медіа [9].	Фокусується на аналізі публікацій у соціальних мережах, таких як Facebook, X-Twitter, Telegram-канали та форуми. SOCMINT використовується для моніторингу розповсюдження ворожих наративів та ідентифікації ключових поширювачів.
TECHINT – Технічна розвідка [10].	Охоплює аналіз інфраструктурних слідів: перевірка доменних реєстрів WHOIS для атрибуції джерел дезінформації, аналіз метаданих зображень за допомогою таких інструментів, як Jeffrey's Image Metadata Viewer. Відрізняється від більш вузької COMINT.
Елементи HUMINT	Хоча OSINT формально оперує лише відкритими джерелами, аналіз довіри до джерел та пошук інформаторів серед відкритих публікацій вимагає елементів людської розвідки, що є частиною процесу верифікації.

Варто зауважити, що розслідування інформаційних атак ґрунтується на багатопрофільній роботі з відкритими даними. Так, зокрема, соціальні мережі та Telegram-канали, незважаючи на їхню корисність, створюють виклики через поєднання публічного доступу та високого рівня анонімності. Водночас для перевірки медіафайлів використовуються інструменти зворотного пошуку зображень, такі як TinEye або Berify, що дозволяють знайти оригінальне джерело або виявити змінені версії. Доменні реєстри допомагають виявити інфраструктуру, яка використовується для поширення дезінформації [10].

Сьогодні війна в Україні стала полігоном для передових OSINT-технік. Так, наприклад, агентство Bellingcat, особливо після розслідування MH17**,** встановило високі стандарти використання відкритих джерел для кримінальних розслідувань [11].

Під час повномасштабного вторгнення OSINT-методи були вирішальними для моніторингу та документування потенційних воєнних злочинів. Водночас оперативна публікація верифікованих доказів у режимі реального часу почала руйнувати російську агресивну кампанію дезінформації, яка

поширювала суперечливі версії подій. Українські спільноти, такі як InformNapalm, використовують ці методи для створення баз даних ворожих підрозділів, а Molfar застосовує OSINT для комерційної та контррозвідувальної аналітики [12].

Варто акцентувати, що для забезпечення достовірності та легітимності OSINT-результатів необхідно дотримуватися чіткого аналітичного алгоритму. Професійне OSINT-розслідування є послідовним процесом, який має відповідати криміналістичним стандартам.

По-перше, цей процес починається зі збору даних, де пасивні методи на етапі збору загальної інформації завжди передують активним методам, таким як збір конкретних даних про об'єкт. По-друге, це перевірка та верифікація отриманої інформації, що вимагає перехресної перевірки джерел, встановлення часу та місця події, а також аналізу метаданих. По-третє, відбувається синтез зібраних і верифікованих даних для виявлення TTPs або формування повного уявлення про подію.

Варто зауважити, що результати часто вимагають візуалізації, наприклад мапування розповсюдження наративів. Процес завершується створенням звіту, який трансформує інформацію в аналітичний продукт або, у правовому контексті, у потенційний судовий доказ [13].

Водночас, разом зі зростанням обсягів даних, автоматизація стала не просто бажаним кроком, а необхідністю. Використання API та Python-скриптів для веб-краулінгу сьогодні дозволяє значно прискорити збір інформації. В останні роки ключову роль відіграє OSINT, підтримуваний штучним інтелектом, який дозволяє ідентифікувати критичні сутності – такі, як люди, локації, організації – у великих масивах даних, автоматично проводити розпізнавання настроїв за допомогою обробки природної мови та моніторити джерела 24/7 [14].

Ми переконані, що штучний інтелект також вносить революційні зміни у процес верифікації. Зокрема, AI-assisted інструменти можуть виявляти незвичайні або підозрілі частини тексту чи фотографій, допомагаючи визначити, чи було медіа згенероване ШІ. Такий технологічний прогрес, на нашу думку, створює постійні «технологічні перегони» між творцями фейків та аналітиками.

Не можна оминути і проблеми точності, достовірності та верифікації даних у інформаційній війні. В умовах, коли ворог навмисно використовує стратегію поширення кількох, часто взаємовиключних, версій подій для створення плутанини, якість верифікації стає стратегічною вимогою.

Поширення технологій генеративного ШІ, які можуть створювати deepfake-відео, клонувати голоси та генерувати граматично точні, але фальшиві тексти, ставить під сумнів довіру до будь-якого цифрового сліду.

Таким чином, незважаючи на ефективність, яку надають технології, аналітики OSINT залишаються важливішими, ніж будь-коли, оскільки саме вони повинні верифікувати та валідувати інформацію. У цьому контексті варто розуміти, що процес верифікації перестає бути лише технічною процедурою – він стає стратегічним імперативом правової допустимості. Для забезпечення цілісності правосуддя, особливо у міжнародних кримінальних справах, процес збору, обробки та зберігання OSINT-даних повинен відповідати найвищим стандартам криміналістичної інформатики, щоб захистити докази від подальших маніпуляцій і підтвердити їхню автентичність.

Не менш важливим є питання правових та етичних меж застосування OSINT. Ми переконані, що використання OSINT у державних та громадських розслідуваннях нерозривно пов'язане з необхідністю дотримання правових та етичних обмежень, особливо у сфері захисту персональних даних.

Тут важливим є той факт, що OSINT оперує на стику фундаментальних прав, зокрема права кожного на вільне збирання, зберігання та використання інформації й права на приватність. В українському законодавстві вже існує прецедент, коли відсилання розпорядника інформації до загальнодоступних джерел у відповідь на запит про публічну інформацію вважається неправомірною відмовою. Це побічно вказує на те, що навіть якщо інформація є відкритою, її належна обробка, надання та, за аналогією, збір для подальшого використання мають відповідати встановленим процедурам [15].

Загальний регламент про захист даних (GDPR) встановлює найвищі глобальні стандарти для обробки персональних даних, наголошуючи на принципах прозорості та мінімізації даних.

З погляду GDPR, для OSINT-розслідувань слід з обережністю використовувати згоду суб'єкта як правову підставу для обробки, оскільки існує високий ризик її оскарження або відкликання. Водночас більш надійною підставою є законний інтерес, за умови, що інтерес розслідування переважає над правом особи на приватність [16].

Етичні аспекти застосування OSINT вимагають постійного балансування між публічним інтересом і правом на приватність. Неконтрольована, самоорганізована діяльність громадських активістів, спрямована на викриття або ідентифікацію осіб, може призвести до небезпеки «цифрового самосуду». Ми переконані, що професійні OSINT-розслідування, особливо ті, що проводяться журналістами та правозахисниками, повинні суворо дотримуватися етичних принципів, аналогічних стандартам IFCN та нормам GDPR, аби не допустити надмірного збору даних і забезпечити захист персональної інформації, яка не має прямого відношення до розслідування злочину [17].

Висновок. Відкрита розвідка стала незамінним та асиметричним інструментом у протидії іноземному інформаційному маніпулюванню та втручанню. Систематичне застосування GeoINT, SOCMINT та сучасних AI-assisted інструментів дозволяє незалежним і інституційним акторам оперативно виявляти, верифікувати та атрибутувати інформаційні атаки.

Успіхи у викритті фейків та документуванні воєнних злочинів в Україні підтвердили здатність OSINT впливати на кримінальне судочинство та стратегічну комунікацію.

Водночас, для забезпечення стійкості та легітимності OSINT у довгостроковій перспективі необхідно подолати два ключові виклики. По-перше – методологічна прозорість: в умовах зростання загрози deepfakes та маніпуляцій GenAI верифікація даних вимагає запровадження уніфікованих, прозорих і криміналістично сумісних стандартів. По-друге **–** правова легітимізація: OSINT-розслідування мають чітко відповідати вимогам захисту персональних даних, покладаючись на законний інтерес як правову підставу та мінімізуючи збір надлишкової інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). Website: EEAS. URL: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en (дата звернення 10.10.2025).
2. How OSINT shaped reporting on the war in Ukraine. URL: https://www.info-res.org/eyes-on-russia/articles/how-osint-shaped-reporting-on-the-war-in-ukraine (дата звернення 10.10.2025).
3. OSINT як доказ у розслідуванні воєнних злочинів: представники ВС взяли участь у тематичному семінарі. Вебсайт: Веровний суд України. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1883443 (дата звернення 10.10.2025).
4. Хакімова В.Т. ЄС в епоху постправди: діяльність East StratCom Task Force. *Актуальні проблеми політики*. 2021. № 67. С. 155–162. DOI https://doi.org/10.32837/app.v0i67.1166.
5. Ратушна Т. (2025). Фейки та дезінформація в соціальних мережах під час війни: ризики для українського суспільства. *Науково-теоретичний альманах Грані*, *28*(3), 84–91. URL: https://doi.org/10.15421/172573.
6. Russian information operations outside of the Western information environment (Revised version). Website: NATO SCCOE. URL: https://stratcomcoe.org/publications/russian-information-operations-outside-of-the-western-information-environment-revised-version/316 (дата звернення 10.10.2025).
7. Фейки, спростовані проектом StopFake в 2014– 2017 роках: наративи та джерела. Вебсайт: Spravdi. URL: https://spravdi.gov.ua/fejky-sprostovani-proektom-stopfake-v-2014-2017-rokah-naratyvy-ta-dzherela (дата звернення 10.10.2025).
8. SOCMINT, GEOINT, COMINT: three sub-disciplines of OSINT explained. URL: https://incyber.org/en/article/socmint-geoint-comint-three-sub-disciplines-of-osint-explained (дата звернення 10.10.2025).
9. Як викривати інформаційні маніпуляції за допомогою OSINT. URL: https://ms.detector.media/trendi/post/27076/2021-04-15-yak-vykryvaty-informatsiyni-manipulyatsii-za-dopomogoyu-osint (дата звернення 10.10.2025).
10. Fact-checking and Debunking. Website: NATO SCCOX. URL: https://stratcomcoe.org/publications/fact-checking-and-debunking/8 (дата звернення 10.10.2025).
11. How Bellingcat collects, verifies and archives digital evidence of war crimes in Ukraine. Website: Retures. URL: https://reutersinstitute.politics.ox.ac.uk/news/how-bellingcat-collects-verifies-and-archives-digital-evidence-war-crimes-ukraine (дата звернення 10.10.2025).
12. Davonte Hardway. Disinformation and war: How the Violent War in Ukraine Illustrates the Power of Disinformation 1. URL: https://democratic-erosion.org/2025/04/27/disinformation-ukraine-war (дата звернення 10.10.2025).
13. Як OSINT впливає на війну в Україні? URL: https://itedu.center/ua/blog/articles/osint (дата звернення 10.10.2025).
14. OSINT AI: How to Optimize Your Investigation in 2024. Website: Molfar. URL: https://molfar.com/en/blog/osint-ai-how-to-optimize-your-investigation (дата звернення 10.10.2025).
15. Про правомірність відсилання до відкритих джерел у відповідь на запит про надання інформації. URL: https://zaholovok.com.ua/pro-pravomirnist-vidsylannya-do-vidkrytykh-dzherel-u-vidpovid-na-zapyt-pro-nadannya-informatsiyi (дата звернення 10.10.2025).
16. GDPR essentials for OSINT research. URL: https://www.blockint.nl/methods/gdpr-essentials-for-osint-research (дата звернення 10.10.2025).
17. Julien Rossi, Université Paris 8 Jonathan Keller, CNRS PUBLISHED ON: 15 Sep 2025. DOI: 10.14763/2025.3.2034.