https://doi.org/10.31891/2307-5732-2025-359-33
УДК 004.056.55

МОГИЛЕВИЧ ДМИТРО
КПІ ім. Ігоря Сікорського
https://orcid.org/0000-0002-4323-0709
e-mail: mogilev11@ukr.net
МОГИЛЕВИЧ ВАДИМ
КПІ ім. Ігоря Сікорського
https://orcid.org/0000-0003-2937-5327
e-mail: vadym.vadym63@gmail.com
КОНОНОВА ІРИНА
КПІ ім. Ігоря Сікорського
https://orcid.org/0009-0004-3736-4761
e-mail: viti21@ukr.net

АНАЛІЗ OSINT ІНСТРУМЕНТІВ ДЛЯ ДОСЛІДЖЕННЯ СОЦІАЛЬНИХ МЕРЕЖ

У статті розглянуто значення соціальних мереж як джерела розвідки та проаналізовано особливості використання спеціалізованих інструментів для отримання, обробки та аналізу даних із різних соціальних платформ. З урахуванням стрімкого зростання обсягів відкритих даних у Facebook, Twitter (X) та Instagram, здійснено класифікацію та оцінку сучасних OSINT-інструментів за функціональним призначенням, методами збору, аналітичними можливостями та візуалізації інформації. Проаналізовано переваги та обмеження як офіційних API (Graph API, Twitter API, Instagram Graph API), так і неофіційних рішень (Twint, OSINTgram, Maltego з розширеннями, інструменти архівації тощо). Констатовано, що ефективне застосування OSINT-інструментів залежить від технічних характеристик платформи, доступності даних, політики конфіденційності, а також стабільності роботи інструментів в умовах постійних змін інтерфейсів та обмежень. Підкреслено значення візуального аналізу та геолокацій, роль міжплатформної інтеграції й архівації як елементів цифрової криміналістики. Визначено можливості та обмеження OSINT-інструментів, призначених для дослідження соціальної мережі. Зроблено висновок про необхідність поєднання технічних рішень з правовими та етичними підходами для забезпечення достовірності, безпеки та легітимності досліджень у сфері OSINT. Дослідження акцентує увагу на важливості вибору правильного підходу до збору та аналізу даних залежно від функціональних особливостей кожної соціальної мережі для досягнення максимальної ефективності та релевантності отриманої інформації.

Ключові слова: *OSINT, відкриті джерела інформації, соціальні мережі, цифрова безпека, інформаційні загрози.*

MOGYLEVYCH DMYTRO, MOHYLEVYCH VADYM, KONONOVA IRYNA
Igor Sikorsky Kyiv Polytechnic Institute

ANALYSIS OF OSINT TOOLS FOR RESEARCHING SOCIAL NETWORKS

The article discusses the importance of social networks as a source of intelligence and analyzes the features of using specialized tools to obtain, process, and analyze data from various social platforms. The effectiveness of using social media for OSINT depends on the research goals, the type of information sought, the target audience, and the technical capabilities of the platform. The combined use of multiple sources allows you to create a holistic picture of the research object and increase the accuracy of analytical conclusions.

Given the rapid growth of open data on Facebook, Twitter (X), and Instagram, modern OSINT tools have been classified and evaluated according to their functional purpose, collection methods, analytical capabilities, and information visualization. The advantages and limitations of both official APIs (Graph API, Twitter API, Instagram Graph API) and unofficial solutions (Twint, OSINTgram, Maltego with extensions, archiving tools, etc.) are analyzed. It was found that the effective use of OSINT tools depends on the technical characteristics of the platform, data availability, privacy policy, and the stability of the tools in the context of constantly changing interfaces and restrictions. The importance of visual analysis and geolocation, the role of cross-platform integration and archiving as elements of digital forensics are emphasized. The capabilities and limitations of OSINT tools designed for social network research are identified. It concludes that technical solutions must be combined with legal and ethical approaches to ensure the reliability, security, and legitimacy of OSINT research. The study emphasizes the importance of choosing the right approach to data collection and analysis depending on the functional characteristics of each social network in order to achieve maximum efficiency and relevance of the information obtained.

Keywords: *OSINT, open sources of information, social networks, digital security, information threats.*

Стаття надійшла до редакції / Received 03.09.2025
Прийнята до друку / Accepted 05.11.2025

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

У сучасному інформаційному суспільстві соціальні мережі відіграють ключову роль як джерело даних, комунікаційна платформа та середовище формування громадської думки. Зростання обсягів відкритої інформації в таких мережах, як Facebook, Twitter (X), Instagram та інших, створює нові можливості для її аналітичного опрацювання, водночас ставлячи перед дослідниками складні завдання щодо ефективного збору, обробки та інтерпретації цих даних.

У цьому контексті інструменти відкритої розвідки (OSINT − Open Source Intelligence) набувають особливої актуальності. Вони дозволяють автоматизувати процеси виявлення публікацій, профілів, зв'язків між користувачами, геолокаційної інформації, динаміки поширення контенту тощо. Проте з огляду на велику кількість доступних OSINT-інструментів, їх різну функціональність, ступінь автоматизації та обмеження в доступі до даних соціальних платформ, постає необхідність у їх системному аналізі та порівнянні.

Таким чином, аналіз OSINT-інструментів у контексті дослідження соціальних мереж, є обґрунтованим

як з наукової, так і з прикладної точки зору.

Аналіз досліджень та публікацій

В роботах [1] та [2] описано основи та методологію OSINT, підкреслена важливість структурованого підходу до збору, перевірки та аналізу інформації з відкритих джерел, подано огляд фаз OSINT-циклу: від виявлення джерел до побудови аналітичного висновку. Аналіз наявних можливостей і викликів, пов'язаних із застосуванням OSINT, дає змогу сформувати цілісне уявлення про сучасний стан теоретичних засад і практичних підходів у цій сфері.

У статті [3] розглянуто поточний стан і основні тенденції у сфері безпеки OSINT. Особливу увагу приділено аналізу загроз та кіберзлочинів, що можуть виникнути внаслідок зловживання даними, отриманими за допомогою OSINT. З метою протидії цим викликам автори пропонують низку вимог до забезпечення безпеки, які можуть бути застосовані в середовищі OSINT. Ці вимоги охоплюють аспекти безпечного збору, зберігання, доступу та використання інформації. Їх реалізація спрямована на мінімізацію потенційної шкоди, спричиненої кіберзлочинною діяльністю у сфері OSINT.

У [4] досліджуються ризики використання технологій OSINT у контексті національної безпеки України. Автори акцентують увагу на загрозах, пов'язаних із несанкціонованим збором персональних даних, аналізом критичної інфраструктури та організацією кібератак. Розглянуто реальні випадки витоку інформації, правові та етичні аспекти використання OSINT, а також методи протидії, включно з контррозвідкою, анонімізацією та мінімізацією цифрового сліду. Особливу увагу приділено ролі держави у нормативному регулюванні та захисті відкритих даних.

У статті [5] проаналізовано сучасні інструменти та методології OSINT як ключового елементу комплексної розвідки поряд з HUMINT, SIGINT, IMINT та GEOINT. Розглянуто основні джерела відкритих даних, етапи збору та аналізу інформації, а також функціональні можливості провідних OSINT-інструментів, зокрема Maltego та Shodan. Особливу увагу приділено геопросторовій розвідці, автоматизації процесів, загрозам конфіденційності та стратегіям протидії витокам даних. Автори підкреслюють важливість захисту персональної інформації та роль OSINT в умовах цифрової трансформації.

У дослідженні [6] проаналізовано потенціал використання інструментів OSINT для фіксації воєнних злочинів у контексті національної безпеки. Автор розглядає вітчизняний і зарубіжний досвід збору інформації з відкритих джерел, класифікує відповідні джерела та пропонує перелік ефективних інструментів. Особливу увагу приділено перевагам OSINT — зокрема оперативному збору доказів, аналітичному забезпеченню керівництва держави та публічному розкриттю злочинів РФ. Наголошено на необхідності правового регулювання, дотримання принципів верховенства права, неупередженості та прозорості в діяльності розвідувальних і правоохоронних органів.

Таким чином, на основі проведеного аналізу літератури встановлено, що хоча існує широкий спектр OSINT-інструментів для дослідження соціальних мереж, актуальними залишаються питання ефективної інтеграції, автоматизації, інтерпретації результатів, а також правового регулювання їхнього застосування.

Формулювання цілей статті

Метою статті є проведення порівняльного аналізу OSINT-інструментів, які використовуються для дослідження соціальних мереж, визначення їх можливостей, переваг, недоліків і сфер ефективного застосування.

Виклад основного матеріалу

Соціальні мережі стали невід'ємною частиною сучасного цифрового простору, суттєво впливаючи на повсякденне життя користувачів та формування їхньої поведінки. Вони активно використовуються для комунікації, пошуку інформації про товари та послуги, оцінки репутації брендів, а також для особистого самовираження. У зв'язку з цим зростає значення аналізу контенту та активностей у соціальних мережах для різноманітних сфер – від маркетингу до розслідувань.

З огляду на обсяг даних, які щоденно генеруються в соціальних мережах, вони стали важливим джерелом відкритої інформації для проведення OSINT-досліджень. Користувачі добровільно публікують фотографії, геолокаційні дані, коментарі, контактну інформацію, що дозволяє дослідникам, журналістам та аналітикам отримувати цінну інформацію без порушення закону.

Проте кожна соціальна мережа має свої специфічні особливості: архітектуру, політику конфіденційності, обмеження щодо доступу до даних. Саме тому ефективне використання OSINT-інструментів потребує глибокого розуміння функціоналу тієї чи іншої платформи та відповідного підходу до збору і аналізу інформації. У даній роботі досліджуються сучасні OSINT-інструменти, їхні можливості, обмеження та сфери застосування при роботі з найпопулярнішими соціальними мережами.

Facebook є однією з найпопулярніших та найінформативніших соціальних мереж для OSINT завдань, завдяки поширеній реєстрації під справжніми іменами, наявності сторінок публічних осіб, компаній, відкритих груп. Аналіз показав, що інструменти для збору даних з Facebook можна класифікувати таким чином:

1. Офіційні ресурси компанії Meta (Graph API [7], Ad Library [8], CrowdTangle [9] (припинено з 14.08.2024 р.)) відіграють важливу роль у забезпеченні надійного та достовірного доступу до відкритих даних платформи Facebook. Ці інструменти доцільно застосовувати для аналізу публічних сторінок, вивчення інформаційних кампаній впливу, а також моніторингу політичної реклами. Завдяки широким можливостям агрегування та фільтрації інформації, зазначені сервіси є особливо ефективними при роботі з великими масивами даних, а також під час виявлення динаміки інформаційних трендів у цифровому середовищі.

2. Аналітичні платформи, такі як Maltego [10] у поєднанні з розширенням Social Links [11],

відкривають широкі можливості для глибинного OSINT-аналізу завдяки побудові соціальних графів, які візуалізують взаємозв'язки між об'єктами дослідження. Ці інструменти дозволяють ідентифікувати групи впливу, мережі взаємодії та приховані інформаційні вузли, що є ключовим для стратегічної розвідки у відкритих джерелах. Високий рівень інтеграції з іншими соціальними платформами та зовнішніми базами даних забезпечує міжплатформну кореляцію інформації, сприяючи більш точній атрибуції цифрових об'єктів. Завдяки цьому, зазначені платформи особливо ефективні в умовах комплексного аналізу інформаційного середовища та виявлення структурованих впливів.

3. Неофіційні інструменти, такі як IntelTechniques [12] та StalkFace [13], вирізняються простотою у використанні та забезпечують оперативний доступ до публічно доступної інформації користувачів. Вони є ефективними засобами для індивідуального аналізу профілю, відстеження активності, а також первинного збору OSINT-даних без потреби в складній технічній підготовці. Водночас, використання таких інструментів супроводжується певними обмеженнями, зокрема нестабільністю функціонування, що пов'язана з частими оновленнями інтерфейсу та DOM-структури платформи Facebook, які можуть призводити до втрати працездатності окремих функцій або сервісів. Незважаючи на це, подібні рішення залишаються корисними в рамках точкових або короткострокових досліджень.

4. Методи архівації (archive.ph, Wayback Machine [14]) забезпечують довгостроковий доступ до динамічного веб-контенту, включно з публікаціями у соціальних мережах. Ці інструменти дозволяють зберігати зафіксовані копії веб-сторінок у незмінному вигляді, що є надзвичайно важливим для документування цифрових доказів, проведення ретроспективного аналізу інформаційних кампаній, а також виявлення фактів видалення або редагування контенту. Архівування слугує надійним способом збереження інформації, яка з часом може стати недоступною через зміни політики конфіденційності, цензуру або свідоме приховування слідів онлайн-активності. У контексті OSINT-досліджень ці методи значно підвищують доказову цінність зібраних матеріалів, доповнюючи можливості інструментів реального часу системним історичним виміром. Допомагають створювати доказову базу у криміналістиці та журналістських розслідуваннях.

Порівняння інструментів аналізу Facebook представлено в табл. 1.

Таблиця 1

Порівняння інструментів аналізу Facebook

Інструмент / Сервіс	**Основні функції**	**Переваги**	**Обмеження**	**Формат / Тип**
Facebook Graph API	Отримання публічних даних сторінок, груп, подій	Офіційний API, детальна документація, доступ до метаданих	Потребує access token, обмежений доступ до особистих профілів	API / JSON
CrowdTangle (Meta)	Аналіз публічних сторінок, груп, поширення контенту	Візуалізація популярності постів, трендів, авторів	Тільки для публічного контенту, потрібна заявка на доступ	Веб / API
Meta Ad Library	Пошук політичної та комерційної реклами, інформація про витрати	Зручна для OSINT у контексті впливу, дезінформації	Обмежена до рекламного контенту	Веб
Intel Techniques / Facebook Tools	Збір ID, пошук за фото, місцем, телефоном	Придатно для атрибуції, виявлення фейкових акаунтів	Частина інструментів застаріла через зміни політики Facebook	Веб-інструменти
Maltego + Facebook Transforms	Побудова графів зв'язків між акаунтами, групами, подіями	Візуалізація соціальних структур, інтеграція з іншими OSINT-джерелами	Потрібен доступ до API або ручне налаштування, частково платний	OSINT-платформа
Google Dorking + site:facebook.com	Пошук відкритих профілів, постів, фото, коментарів	Обхід вбудованих обмежень пошуку Facebook	Працює тільки з індексованим контентом, частина сторінок прихована	Google Search
archive.ph / Wayback Machine	Архівація профілів, постів, сторінок Facebook для аналізу в часі	Фіксація контенту, який може бути видалений	Потрібно вручну додавати URL або автоматизувати	Веб / архів

Аналіз можливостей та обмежень OSINT-інструментів, призначених для дослідження соціальної мережі Facebook, засвідчив низку важливих технічних, організаційних та правових бар'єрів. По-перше, доступність персоналізованих даних, зокрема вмісту особистих сторінок, дописів і комунікацій, значною мірою залежить від індивідуальних налаштувань конфіденційності користувачів, що обмежує можливості спостереження. По-друге, значна частина неофіційних інструментів (зокрема вебскрейперів і скриптів) є вразливою до змін у DOM-структурі та інтерфейсі платформи, що спричиняє їхню швидку втрату актуальності. По-третє, офіційний API Facebook (Graph API), хоча й забезпечує структурований доступ до даних, вимагає проходження процедури авторизації та має чітко визначені обмеження щодо типів інформації, доступної для

збору. Також, необхідно враховувати юридичні аспекти. Тому, що автоматизований збір або обробка даних без згоди користувача може суперечити політиці конфіденційності платформи й вимогам чинного законодавства України. Це накладає додаткові етичні та правові зобов'язання на дослідника.

Twitter (X) є ідеальною платформою для моніторингу актуальних подій у реальному часі завдяки коротким повідомленням, хештегам і геотегам. На основі аналізу інструментів OSINT, застосовуваних до платформи Twitter (X), доцільно здійснити їх класифікацію за функціональним призначенням і охопити кілька ключових напрямів, кожен із яких забезпечує окремий рівень аналітичної глибини у межах OSINT-досліджень.

Така класифікація дозволяє систематизувати підходи до дослідження публічної активності користувачів, інформаційного ландшафту та соціальних взаємодій у цій мережі.

1. Інструменти збору та агрегування відкритих даних. До цієї категорії належать інструменти, що забезпечують масштабний доступ до відкритої інформації на платформі Twitter без необхідності використання офіційного API. У контексті сучасних обмежень, запроваджених Twitter щодо обсягу та способів отримання даних, такі рішення є особливо актуальними. Twint [15] є одним із основних інструментів цього класу, надаючи можливість збору великих обсягів твітів, хештегів, згадок, метаданих та геолокаційної інформації без потреби в аутентифікації. Завдяки своїй швидкодії та універсальності, цей інструмент є ефективним для оперативного моніторингу публічного дискурсу, а також для побудови часових моделей інформаційного поширення під час кризових або суспільно значущих подій. Як і офіційні інструменти Meta для Facebook, Twint відіграє важливу роль у забезпеченні доступу до актуальної, публічно доступної інформації, придатної для дослідницьких та аналітичних завдань.

2. Інструменти контентного аналізу та тематичного структурування. Ці засоби зосереджені на глибокій семантичній обробці отриманого контенту з метою виявлення ключових наративів, тем та емоційного забарвлення публікацій. TweetBeaver є функціональним аналітичним інструментом, що дозволяє здійснювати поглиблений аналіз контенту конкретних користувачів або цілих масивів твітів. Він забезпечує ідентифікацію часових закономірностей, визначення тональності дописів, частоти вживання окремих слів чи хештегів, а також реакцій аудиторії на певні інформаційні події. Завдяки цьому TweetBeaver може ефективно використовуватись для формування якісних профілів інформаційного впливу.

3. Інструменти соціального аналізу та візуалізації взаємодій. Цей сегмент охоплює інструменти, орієнтовані на вивчення структури соціальної взаємодії, побудову мережевих графів та виявлення ключових інформаційних вузлів у комунікаційному середовищі Twitter. NodeXL [16] надає можливість створювати соціальні графи, що дозволяють візуалізувати мережі зв'язків між користувачами, виявляти лідерів думок, кластери взаємодії та центри поширення інформації. Maltego (з відповідними розширеннями для Twitter) є потужним інструментом OSINT-розвідки, що дозволяє поєднувати дані з Twitter з іншими джерелами, включно з відкритими базами даних і цифровими слідами з інших платформ. Це розширює межі аналітики, дозволяючи будувати міжплатформні моделі впливу та відстеження інформаційних потоків.

Отже, кожна з вказаних категорій інструментів виконує важливу роль у контексті дослідження Twitter як джерела відкритої інформації. Їхнє комплексне застосування дозволяє сформувати багатовимірну картину інформаційного середовища платформи, виявити ключові тренди, ідентифікувати суб'єкти впливу та аналізувати динаміку соціальних зв'язків.

Порівняння інструментів аналізу Twitter представлено в табл. 2.

Таблиця 2

Порівняння інструментів аналізу Twitter

Інструмент / Сервіс	Основні функції	Переваги	Обмеження	Формат / Тип
Twitter API v2 (офіційний)	Пошук твітів, профілів, аналітика взаємодій, геолокація	Законний, стабільний, широкі можливості аналітики	Потребує API-ключів, обмеження на кількість запитів, платні рівні доступу	API / JSON
Tweepy (Python)	Підключення до Twitter API для збору твітів, фоловерів, лайків	Гнучкість, автоматизація, інтеграція з іншими Python-інструментами	Потребує програмування та API-ключів	Python / CLI
Twint (неофіційний)	Пошук твітів, профілів, фоловерів, хештегів без API	Не потребує авторизації, гнучкий пошук, зручний для швидкого OSINT	Частково не працює після API-змін Twitter (потрібні обхідні рішення)	Python / CLI
Social Links + Maltego	Візуалізація зв'язків між профілями, локації, хештеги, згадки	Висока деталізація, інтеграція з іншими платформами	Платний, потребує Maltego та доступу до API	GUI / Maltego
TweetBeaver	Аналіз облікового запису: фоловери, спільні фоловери, час створення, згадки	Безкоштовно, проста у використанні	Обмежені функції, не працює зі складною мережею зв'язків	Веб

Продовження Таблиці 2

Foller.me	Базова аналітика акаунта: активність, популярні теми, хештеги	Швидкий огляд профілю	Не глибокий аналіз, лише загальні дані	Веб
Hoaxy (Indiana University)	Візуалізація поширення твітів і дезінформації	Наукова точність, відстеження фейкових кампаній	Працює лише з відкритими твітами, обмежена база даних	Веб
Social Searcher	Моніторинг ключових слів, хештегів у режимі реального часу	Багатоплатформний, зручний для медіа-моніторингу	Не має доступу до закритих даних, базова деталізація	Веб
GeoSocial Footprint	Виявлення геолокації твітів, профілювання користувача за місцезнаходженням	Простий інтерфейс, корисний для геоаналізу	Потребує твітів із геоданими, обмежений доступ після змін Twitter API	Веб / Інтерактивна карта

OSINT-аналіз платформи Twitter (X) супроводжується низкою обмежень, які впливають на якість і достовірність досліджень. Із впровадженням нової політики доступу до офіційного API, значно звужено можливості безкоштовного збору та обробки даних, зокрема у великому обсязі чи з високою частотою запитів. Це істотно обмежує застосування традиційних інструментів аналізу, орієнтованих на масштабний моніторинг інформаційних потоків у реальному часі. Неофіційні інструменти збору даних, такі як Twint, хоч і залишаються популярними серед дослідників завдяки можливості обходити обмеження API, демонструють високу залежність від поточної DOM-структури інтерфейсу платформи, що часто змінюється. Це зумовлює нестабільність їх роботи та потребу в постійному технічному супроводі. Крім того, особливості самої платформи створюють серйозні виклики щодо верифікації інформації. Високий рівень анонімності користувачів, відсутність вимог до реєстрації з використанням справжніх ідентифікаційних даних, а також поширеність фейкових облікових записів значно ускладнюють встановлення достовірності джерел та вимагають додаткових крос-платформених перевірок. Висока насиченість Twitter (X) нерелевантним контентом − спамом, рекламними повідомленнями та бот-активністю − вимагає використання додаткових інструментів фільтрації та семантичної обробки, що підвищує складність дослідницької процедури.

Отже, для ефективного OSINT-аналізу у середовищі Twitter необхідним є ретельно виважений вибір інструментарію, поєднання автоматизованих та аналітичних методів, що забезпечують точність дослідження.

Instagram є цінним джерелом даних для аналізу візуального контенту, зокрема фотографій і відео, а також для дослідження геолокацій, актуальних тем і цифрових трендів. Завдяки своїй орієнтації на візуальну комунікацію, платформа надає широкі можливості для ідентифікації об’єктів, виявлення соціальних взаємозв’язків та моніторингу динаміки інформаційних процесів у цифровому середовищі. Аналіз OSINT-інструментів, застосовуваних для дослідження платформи Instagram, дозволяє виокремити кілька ключових категорій інструментів відповідно до їх функціонального призначення. Така класифікація сприяє цілеспрямованому підходу до обробки публічної інформації, залежно від дослідницьких цілей і завдань.

1. Інструменти збору та агрегування відкритих даних. Ця група охоплює інструменти, що забезпечують автоматизований доступ до великого масиву відкритої інформації, включаючи дописи, коментарі, сторіз, хештеги, геолокації та інші метадані. Зокрема, Instaloader [17] та OSINTgram [18] дозволяють здійснювати структурований збір даних без використання офіційного API, що є особливо актуальним в умовах обмеженого доступу до внутрішніх сервісів платформи.

2. Інструменти візуального аналізу та зворотного пошуку зображень. Instagram як візуально орієнтована платформа потребує залучення технологій комп’ютерного зору. Засоби на кшталт PimEyes, TinEye, Google Reverse Image Search чи Amazon Rekognition дають змогу ідентифікувати осіб, об’єкти, локації, а також виявляти повторне використання зображень в інших джерелах. Це відкриває можливості для перевірки автентичності контенту та розпізнавання прихованих зв’язків.

3. Інструменти соціального аналізу та атрибуції. Інструменти цієї категорії спрямовані на дослідження мережевих зв’язків, взаємодій між акаунтами та ідентифікацію центрів впливу. Maltego (з інтеграцією плагінів Social Links або ShadowDragon) та SocioSpy [19] дозволяють створювати соціальні графи, виявляти групи користувачів із підвищеною активністю або інформаційним впливом, що є цінним для досліджень у сфері інформаційної безпеки, атрибуції й моніторингу.

4. Інструменти часової аналітики та трендового моніторингу. Ці сервіси забезпечують аналіз динаміки змін у поведінці користувачів, популярності тем чи профілів. Social Blade та IG Audit надають статистичну інформацію про зростання аудиторії, рівень взаємодій та ефективність публікацій. Такий підхід дозволяє виявляти інформаційні кампанії або аномальні сплески активності.

5. Інструменти архівації та збереження цифрових слідів. У цій категорії варто відзначити сервіси Wayback Machine, archive.ph та Hunchly [20] , які забезпечують фіксацію й архівацію вебсторінок або вмісту акаунтів. Зважаючи на динамічність Instagram-контенту (зокрема, сторіз або видалених публікацій), архівація відіграє критичну роль у забезпеченні доказової бази для подальшого аналізу.

Порівняння інструментів аналізу Instagram представлено в табл. 3.

OSINT-аналіз платформи Instagram супроводжується низкою обмежень, зумовлених як технічними, так і правовими чинниками. Насамперед, офіційний API Instagram має жорсткі обмеження щодо доступу до даних, особливо контенту приватних профілів, історій та повідомлень, що значно звужує спектр досліджуваної інформації. Неофіційні інструменти та скрипти, які дозволяють обхід цих обмежень, часто втрачають працездатність через регулярні оновлення платформи й посилення політики безпеки. Водночас анонімність користувачів, поширення фейкових акаунтів та бот-активності ускладнюють ідентифікацію джерел та перевірку достовірності інформації. Особливу складність становить автоматизований аналіз візуального контенту, який потребує використання інструментів комп'ютерного зору та розпізнавання образів. До того ж геолокаційні мітки не завжди є надійними через можливість їх зміни або фальсифікації.

Таблиця 3

Порівняння інструментів аналізу Instagram

Інструмент / Сервіс	Основні функції	Переваги	Обмеження	Формат / Тип
Maltego + Social Links Pro	Аналіз профілю, взаємодій, мережі зв'язків, фото, геомітки	Потужна графова візуалізація, точні зв'язки, підтримка багатьох соцмереж	Платний доступ, потребує навичок роботи з Maltego	GUI / Maltego
Instagram Graph API (офіційний)	Отримання мета-даних профілю, підписок, лайків (для бізнес-акаунтів)	Законне джерело даних, стабільність	Потребує авторизації, лише для бізнес-акаунтів, обмежений доступ	API / SaaS
Instaloader	Завантаження фото, історій, описів, профілю, тегів, аналіз фоловерів	Відкритий код, можна автоматизувати, підтримка CLI	Потрібен авторизований обліковий запис для повного доступу	Python / CLI
Hunchly + Instagram + Web	Збереження сторінок, доказова база, повна історія сторінки	Цифрова криміналістика, фіксація змін у профілі	Не виконує аналіз — тільки архівація	Desktop Tool
OSINTgram	Аналіз профілю, лайків, фоловерів, геотеги, сторіс, коментарі	Спеціально створено для Instagram, Python-CLI, автоматизований збір	Потрібен авторизований сесійний файл (cookie), постійні API-зміни Instagram	Python / CLI
Inflact (раніше Ingramer)	Пошук по хештегах, профілях, геолокації, аналітика впливу	Зручний веб-інтерфейс, частково безкоштовно	Комерційна модель, обмеження Instagram API	Веб
Social Searcher / Mentionlytics	Моніторинг згадок у соцмережах, хештеги, ключові слова	Підходить для медіа-моніторингу, багатоплатформність	Обмежена деталізація профілю Instagram, лише публічні дані	Веб / SaaS

Загалом, ефективність використання соціальних мереж для OSINT залежить від цілей дослідження, типу шуканої інформації, цільової аудиторії та технічних можливостей платформи. Комбіноване використання кількох джерел дозволяє створити цілісну картину об'єкта дослідження та підвищити точність аналітичних висновків.

Недоліки аналітики соціальних медіа мають кілька важливих аспектів, які можуть вплинути на точність та достовірність результатів досліджень. По-перше, соціальні медіа можуть стати джерелом упередженої інформації. Користувачі часто публікують матеріали, що відповідають їхнім особистим переконанням, що може призвести до спотворення загальної картини. Це особливо важливо враховувати при аналізі думок та відгуків, оскільки без урахування всіх аспектів ситуації можуть виникнути хибні або неповні висновки.

По-друге, існує проблема перевантаження інформацією. Соціальні медіа генерують величезні обсяги даних в реальному часі, що створює складнощі у відборі важливих та релевантних відомостей. Без спеціалізованих інструментів або алгоритмів фільтрації важко обробити ці дані ефективно і виділити те, що дійсно важливе для дослідження. Крім того, під час збору та аналізу даних існує ризик порушення конфіденційності користувачів. Соціальні медіа не завжди гарантують належний захист особистих даних, і навіть публічно доступна інформація може містити чутливі або приватні відомості. Це створює потенційні юридичні та етичні проблеми, які вимагають обережності та відповідальності.

Ще однією проблемою є недостовірність інформації. У соціальних мережах часто поширюються фальшиві новини, чутки та маніпуляції. Тому дуже важливо ретельно перевіряти всі джерела та проводити крос-перевірку даних, щоб уникнути помилок в аналізі, оскільки інформація може бути спотворена або неправдива.

Залежність від алгоритмів соціальних медіа є ще однією значною проблемою. Ці платформи використовують складні алгоритми для фільтрації та поширення контенту, що може призвести до того, що користувачам буде доступна лише частина інформації. Важливі повідомлення можуть бути проігноровані або приховані через персоналізовані алгоритми, що обмежує об'єктивність і повноту даних.

Також слід врахувати необхідність постійного оновлення даних. Інформація в соціальних медіа змінюється дуже швидко, і дані, зібрані для аналізу, можуть швидко застаріти. Це означає, що для забезпечення актуальності результатів потрібен постійний моніторинг та оновлення зібраної інформації.

Нарешті, існує ризик зловживання даними. Дані з соціальних медіа можуть бути використані зловмисниками для маніпуляцій, шахрайства чи створення фальшивих образів. Неправильне або неповне проведення аналізу може призвести до того, що ці дані будуть використані для створення дезінформаційних кампаній або маніпуляцій громадською думкою. Ці недоліки вимагають ретельної уваги та розвитку стратегій для мінімізації ризиків, забезпечення точності та етики у процесі аналітики соціальних медіа.

Висновки

У результаті проведеного дослідження встановлено, що інструменти для OSINT-аналізу дозволяють збирати, обробляти та інтерпретувати інформацію, що циркулює в соціальних мережах, зокрема на платформах Facebook, Twitter (X) та Instagram. Зростання обсягів відкритих даних, динаміка їх оновлення та специфіка цифрової взаємодії зумовлюють необхідність ретельного аналізу як можливостей, так і обмежень застосування відповідних інструментів в аналітичній діяльності.

У процесі порівняльного аналізу виявлено низку важливих аспектів: офіційні програмні інтерфейси (API), попри дотримання правових вимог, обмежують дослідника у доступі до деяких категорій даних та вимагають автентифікації й попередньої реєстрації; неофіційні інструменти та скрипти (зокрема, Twint, OSINTgram) демонструють ширші можливості у збиранні відкритої інформації, однак є вразливими до змін у політиках платформ і не гарантують стабільного функціонування; універсальні платформи OSINT-аналізу, такі як Maltego (у поєднанні з розширеннями типу Social Links або ShadowDragon), забезпечують інтеграцію даних із різних джерел, побудову графів зв'язків та структурну візуалізацію, проте передбачають наявність відповідної підготовки та обмежені можливості без ліцензійного доступу; інструменти цифрового архівування (archive.ph, Wayback Machine, Hunchly) відіграють ключову роль у збереженні доказового матеріалу та реконструкції динаміки цифрових подій, особливо в контексті розслідувань інформаційних операцій.

Отже, найбільш результативним підходом є комбіноване застосування інструментів для OSINT-аналізу, орієнтоване на специфіку завдань дослідження, з урахуванням динаміки розвитку платформ, правових та етичних обмежень.

Перспективними напрямами подальших досліджень у цій галузі є розробка інтегрованих рішень для багатоканального OSINT-моніторингу, автоматизація процесів фільтрації та верифікації даних із відкритих джерел.

Література

1. Basel M. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information / Basel M. – 9th ed. IntelTechniques. – Independently published, 2023. 528 p.

2. Szymoniak S. Open Source Intelligence Opportunities and Challenges – A Review: [Electronic resource] / S. Szymoniak, K. Foks // Advances in Science and Technology Research Journal. – 2024. №18 (3). – P. 123–139 – Mode of access: https://doi.org/10.12913/22998624/186036.

3. Hwang Y.-W. Current Status and Security Trend of OSINT [Electronic resource] / Y.-W. Hwang, I.-Y.Lee, H. Kim, H. Lee, D. Kim // Wireless Communications and Mobile Computing. – 2022. –Vol. 1. – P. 1 – 14. – Mode of access: https://doi.org/10.1155/2022/1290129.

4. Івкова В.С. OSINT-технології як загроза кібербезпеці держави [Електронний ресурс] /В.С. Івкова, І.Р. Опірський // Кібербезпека: освіта, наука, техніка. – 2025. – №3 (27). –С 165–179. – Режим доступу: 10.28925/2663-4023.2025.27.749.

5. Ivkova V.S. Research of Existing Osint Tools and Approaches in the Context of Personal and State Information Security [Electronic resource] / V.S. Ivkova, I.R. Opirskyy // Academic Journals and Conferences. – 2025. – Vol. 7, № 1. – P. 143 – 159. – Mode of access: https://doi.org/10.23939/csn2025.01.143.

6. Тома М.Г. Інструменти OSINT: Фіксація воєнних злочинів в Україні [Електронний ресурс] / М.Г. Тома, О.В. Василова // Аналітично-порівняльне правознавство. – 2025. – № 02. – С. 905 – 909. Режим доступу: https://doi.org/10.24144/2788-6018.2025.02.134.

7. Overview [Electronic resource]. – Mode of access: https://developers.facebook.com/docs/graph-api/overview l (date of access: 01.07.2025). – Title from screen.

8. Ad Library API [Electronic resource]. – Mode of access: https://developers.facebook.com/docs/graph-api/reference/ads_archive?locale=ru_RU (date of access: 11.05.2025). – Title from screen.

9. CrowdTangle [Electronic resource]. – Mode of access: https://transparency.meta.com/ru-ru/researchtools/other-datasets/crowdtangle/ (date of access: 09.06.2025). – Title from screen.

10. Monitor social media in real-time using AI-driven analysis to manage large data volumes [Electronic

resource]. – Mode of access: https://www.maltego.com/ (date of access: 23.07.2025). – Title from screen.

11. Industry-leading OSINT solutions [Electronic resource]. – Mode of access: https://sociallinks.io/ (date of access: 17.06.2025). – Title from screen.

12. IntelTechniques [Electronic resource]. – Mode of access: https://www.inteltechniques.net/ (date of access: 17.06.2025). – Title from screen.

13. StalkFace [Electronic resource]. – Mode of access: https://stalkface.com/en/ (date of access: 17.06.2025). – Title from screen.

14. About the Internet Archive [Electronic resource]. – Mode of access: https://archive.org/about/ (date of access: 02.05.2025). – Title from screen.

15. Scrape Twitter Without Limits Using Twint [Electronic resource]. – Mode of access: https://www.ahmedbesbes.com/case-studies/scrape-twitter-with-twint (date of access: 19.05.2025). – Title from screen.

16. Marc Smith Connect to Networks with [Electronic resource]. – Mode of access: https://www.smrfoundation.org/2023/11/22/free-book-connect-to-networks-with-nodexl/ (date of access: 15.07.2025). – Title from screen.

17. Instaloader [Electronic resource]. – Mode of access: https://instaloader.github.io/ (date of access: 18.04.2025). – Title from screen.

18. Collecting information on Instagram with Osintgram on Kali Linux [Electronic resource]. – Mode of access: https://spy-soft.net/osintgram-kali-linux/ (date of access: 22.06.2025). – Title from screen.

19. The world's data [Electronic resource]. – Mode of access: https://shadowdragon.io/company/ (date of access: 22.06.2025). – Title from screen.

20. Hunchly is for investigative professionals, online researchers, and anyone else who needs to do unbiased fact-finding with no room for error [Electronic resource]. – Mode of access: https://hunch.ly/online-investigation-software (date of access: 22.06.2025). – Title from screen.

References

1. Basel M. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information / Basel M. – 9th ed. IntelTechniques. – Independently published, 2023. 528 p.

2. Szymoniak S. Open Source Intelligence Opportunities and Challenges – A Review: [Electronic resource] / S. Szymoniak, K. Foks // Advances in Science and Technology Research Journal. – 2024. №18 (3). – P. 123–139 – Mode of access: https://doi.org/10.12913/22998624/186036.

3. Hwang Y.-W. Current Status and Security Trend of OSINT [Electronic resource] / Y.-W. Hwang, I.-Y.Lee, H. Kim, H. Lee, D. Kim // Wireless Communications and Mobile Computing. – 2022. –Vol. 1. – P. 1 – 14. – Mode of access: https://doi.org/10.1155/2022/1290129.

4. Івкова В.С. OSINT-технології як загроза кібербезпеці держави [Електронний ресурс] /В.С. Івкова, І.Р. Опірський // Кібербезпека: освіта, наука, техніка. – 2025. – №3 (27). –С 165–179. – Режим доступу: 10.28925/2663-4023.2025.27.749.

5. Ivkova V.S. Research of Existing Osint Tools and Approaches in the Context of Personal and State Information Security [Electronic resource] / V.S. Ivkova, I.R. Opirskyy // Academic Journals and Conferences. – 2025. – Vol. 7, № 1. – P. 143 – 159. – Mode of access: https://doi.org/10.23939/csn2025.01.143.

6. Тома М.Г. Інструменти OSINT: Фіксація воєнних злочинів в Україні [Електронний ресурс] / М.Г. Тома, О.В. Василова // Аналітично-порівняльне правознавство. – 2025. – № 02. – С. 905 – 909. Режим доступу: https://doi.org/10.24144/2788-6018.2025.02.134.

7. Overview [Electronic resource]. – Mode of access: https://developers.facebook.com/docs/graph-api/overview 1 (date of access: 01.07.2025). – Title from screen.

8. Ad Library API [Electronic resource]. – Mode of access: https://developers.facebook.com/docs/graph-api/reference/ads_archive?locale=ru_RU (date of access: 11.05.2025). – Title from screen.

9. CrowdTangle [Electronic resource]. – Mode of access: https://transparency.meta.com/ru-ru/researchtools/other-datasets/crowdtangle/ (date of access: 09.06.2025). – Title from screen.

10. Monitor social media in real-time using AI-driven analysis to manage large data volumes [Electronic resource]. – Mode of access: https://www.maltego.com/ (date of access: 23.07.2025). – Title from screen.

11. Industry-leading OSINT solutions [Electronic resource]. – Mode of access: https://sociallinks.io/ (date of access: 17.06.2025). – Title from screen.

12. IntelTechniques [Electronic resource]. – Mode of access: https://www.inteltechniques.net/ (date of access: 17.06.2025). – Title from screen.

13. StalkFace [Electronic resource]. – Mode of access: https://stalkface.com/en/ (date of access: 17.06.2025). – Title from screen.

14. About the Internet Archive [Electronic resource]. – Mode of access: https://archive.org/about/ (date of access: 02.05.2025). – Title from screen.

15. Scrape Twitter Without Limits Using Twint [Electronic resource]. – Mode of access: https://www.ahmedbesbes.com/case-studies/scrape-twitter-with-twint (date of access: 19.05.2025). – Title from screen.

16. Marc Smith Connect to Networks with [Electronic resource]. – Mode of access: NodeXL https://www.smrfoundation.org/2023/11/22/free-book-connect-to-networks-with-nodexl/ (date of access: 15.07.2025). – Title from screen.

17. Instaloader [Electronic resource]. – Mode of access: https://instaloader.github.io/ (date of access: 18.04.2025). – Title from screen.

18. Collecting information on Instagram with Osintgram on Kali Linux [Electronic resource]. – Mode of access: https://spy-soft.net/osintgram-kali-linux/ (date of access: 22.06.2025). – Title from screen.

19. The world's data [Electronic resource]. – Mode of access: https://shadowdragon.io/company/ (date of access: 22.06.2025). – Title from screen.

20. Hunchly is for investigative professionals, online researchers, and anyone else who needs to do unbiased fact-finding with no room for error [Electronic resource]. – Mode of access: https://hunch.ly/online-investigation-software (date of access: 22.06.2025). – Title from screen.