Роль OSINT у виявленні та нейтралізації інформаційної зброї

УДК 327.8:004.056.55
Дмитро Рабчун[1], Діана Примаченко[2]
Державний університет інформаційно-комунікаційних технологій,
[1]rabchundima92@gmail.com, [2]d.prymachenko@duikt.edu.ua

Інформаційне протиборство стало невід'ємною складовою гібридних конфліктів. Одним із ключових інструментів у боротьбі з інформаційною агресією є OSINT (Open Source Intelligence) — розвідка на основі відкритих джерел. Цей підхід дозволяє ефективно виявляти, аналізувати та нейтралізувати дезінформацію та інші форми інформаційної зброї. OSINT охоплює збір та аналіз інформації з відкритих джерел, таких як соціальні мережі, новинні ресурси, супутникові знімки та інші публічні дані. Цей метод став особливо актуальним у контексті сучасних конфліктів, де інформація відіграє стратегічну роль.

Під час війни в Україні OSINT відіграв ключову роль у викритті та спростуванні російської дезінформації. Наприклад, організація Bellingcat використовувала відкриті джерела для розслідування обставин збиття рейсу MH17 та інших інцидентів, пов'язаних з агресією Росії. Також українська волонтерська спільнота InformNapalm активно застосовує OSINT для ідентифікації російських військових та документування воєнних злочинів. Їх робота демонструє, що навіть без доступу до секретної інформації можна встановити факти та відповідальність агресора [1].

Сучасні технології значно розширили можливості OSINT. Платформи на кшталт DISINFOX дозволяють структурувати та аналізувати інциденти дезінформації, використовуючи стандарти STIX2 та DISARM TTPs. Крім того, використання супутникових знімків, аналізу трафіку в реальному часі та інших цифрових інструментів забезпечує оперативне реагування на інформаційні загрози [2].

Такі технології перетворюють OSINT на системну аналітичну практику, яка може застосовуватись як у військових структурах, так і в журналістиці та правозахисній діяльності.

В Україні використання OSINT стало особливо масовим після 2014 року, коли почалась російська агресія проти Криму та Донбасу. Добровольці, журналісти, ІТ-фахівці та аналітики об'єднали зусилля, щоб викривати фейки, документувати військову присутність РФ, спростовувати ворожу пропаганду. Одним з яскравих прикладів стало використання геолокації знімків, метаданих, соціальних профілів для підтвердження пересування техніки, ідентифікації солдатів та виявлення їх участі у бойових діях.

Поширення фейкової інформації є одним із ключових методів ведення інформаційної війни. Зокрема, Росія активно використовує багаторівневу мережу сайтів, телеграм-каналів та ботів для впливу на свідомість як українських громадян, так і західної аудиторії.

У таких умовах OSINT відіграє роль своєрідного щита — інструменту швидкої верифікації новин, перевірки джерел та виявлення аномалій у наративі. Це дозволяє не тільки виявляти фейки, а й відслідковувати шляхи їх поширення, джерела фінансування та організаторів інформаційних кампаній.

Серед інструментів OSINT, які використовуються як у професійному, так і у волонтерському середовищі, варто відзначити Maltego, SpiderFoot, Shodan, а також сервіси аналізу метаданих та відкритих супутникових зображень (табл.1). Їх поєднання дозволяє створити комплексний портрет об'єкта розслідування — від IP-адрес і цифрових слідів до географічного положення та зв'язків між учасниками інформаційних атак. Такі дані нерідко стають підґрунтям для кримінальних справ або офіційних звітів міжнародних організацій [3].

Таблиця 1

Порівняння OSINT-інструментів

Назва	**Призначення**	**Джерела**	**Сфера використання**
Maltego	Візуалізація зв'язків	WHOIS, DNS, соцмережі	Кіберрозвідка, OSINT
SpiderFoot	Автоматизований збір OSINT	IP, домени, email	Автоматизований моніторинг
Shodan	Сканування пристроїв	IP-адреси, порти	Кібербезпека

Особливої уваги заслуговує взаємодія між OSINT-спільнотами та державними структурами. У багатьох випадках волонтерські OSINT-ініціативи виявляють загрози раніше, ніж це роблять офіційні служби. Однак така взаємодія вимагає правових механізмів, які б регулювали передачу та обробку даних, захищали джерела інформації та гарантували її використання винятково в законний спосіб. Україна, наприклад, поступово впроваджує відповідні механізми співпраці між СБУ, Мінцифри, ЗСУ та громадськими OSINT-групами.

Окрім безпосередньої протидії фейкам, OSINT застосовується і в стратегіях контрнаративу — формування альтернативних, правдивих інформаційних потоків, що спростовують ворожі наративи. Це можуть бути як візуальні кейси з доказами, так і мультимедійні формати, які легко поширюються у соцмережах.

Ефективне використання OSINT можливе лише за умов високої цифрової грамотності користувачів. Це ставить перед державою і громадянським суспільством завдання з навчання, просвітництва та підвищення загальної інформаційної культури.

1. Akhgar B. OSINT as an integral part of the national security apparatus. Open source intelligence investigation. Cham, 2016. P. 3–9. URL: https://doi.org/10.1007/978-3-319-47671-1_1

2. Korystin O. E., Svyrydiuk N. P. Foreign Experience in the Anti-Terrorist Use of OSINT. *Uzhhorod national university herald. series: law*. 2024. Vol. 2, no. 82. P. 177–181. URL: https://doi.org/10.24144/2307-3322.2024.82.2.28

3. Staniforth A. Open source intelligence and the protection of national security. *Open source intelligence investigation*. Cham, 2016. P. 11–19. URL: https://doi.org/10.1007/978-3-319-47671-1_2

Використання OSINT для захисту персональних даних

УДК 004.056.5:004.738.5:342.7

Михайло Різак[1], Олександр Котик[2]
ДУ «Київський авіаційний інститут»,
[1]mykhailo.rizak@npp.kai.edu.ua, [2]kotyk.oleksandr.81@gmail.com

У сучасному цифровому середовищі персональні дані стали об’єктом постійних загроз з боку кіберзлочинців. Одним із ефективних методів як атак, так і захисту є OSINT (Open Source Intelligence) – розвідка на основі відкритих джерел. Технології OSINT широко застосовуються не лише злочинцями, а й фахівцями з інформаційної безпеки для виявлення витоків даних, оцінки цифрового сліду користувачів та посилення кіберзахисту. В умовах зростаючих вимог GDPR щодо конфіденційності персональної інформації особливо актуальним є використання OSINT для превентивного виявлення ризиків і зменшення потенційних загроз.

Метою даної роботи є дослідження можливостей використання інструментів OSINT для виявлення вразливостей, які можуть призвести до втрати або витоку персональних даних, а також демонстрація їх потенціалу в підвищенні рівня захисту інформації в організаціях та у приватному секторі.

Питання використання OSINT в інформаційній безпеці активно обговорюється в науковій та прикладній літературі. Зокрема, у роботі [1] розглядаються практичні аспекти використання OSINT для збору інформації з відкритих джерел, підкреслюючи важливість анонімності та правових аспектів. Інше дослідження [2] акцентує увагу на ризиках, пов'язаних із використанням OSINT зловмисниками для збору персональних даних та доксингу. Окрема увага приділяється питанням інтеграції OSINT в системи кіберзахисту підприємств, зокрема, через виявлення цифрового сліду, ризиків соціальної інженерії та витоків даних. У публікаціях останніх років також аналізується досвід застосування OSINT у військовій сфері, зокрема під час повномасштабної агресії проти України, що підтверджує ефективність інструментів відкритої розвідки як для оборони, так і для безпеки цивільного сектору.

OSINT – це метод збору та аналізу інформації з відкритих джерел: вебсайтів, соціальних мереж, форумів, даркнету тощо. Для захисту персональних даних OSINT використовується в кількох напрямках:

1) виявлення витоків інформації. Наприклад, за допомогою сервісу Have I Been Pwned [3] можна перевірити, чи були зламані облікові записи або електронна пошта;

2) аналіз цифрового сліду. Інструменти на кшталт Maltego або SpiderFoot дозволяють зібрати дані про особу або організацію та виявити потенційно небезпечну інформацію, що публічно доступна [4,5];