УДК 351.74

ВИКОРИСТАННЯ МЕТОДУ OSINT ПІД ЧАС ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ В УКРАЇНІ

Цуркан Іван Олексійович
Шимко Артем Олегович
Верзілов Микита Русланович
Стецик Роман Мирославович
курсанти факультету № 4
Харківського національного університету внутрішніх справ
Онищенко Юрій Миколайович
заступник декана з навчально-методичної роботи факультету № 4
Харківського національного університету внутрішніх справ
кандидат наук з державного управління, доцент,
http://orcid.org/0000-0002-7755-3071

«Хто володіє інформацією, той володіє світом»
(Нотан Ротшильд).

В умовах воєнного стану отримання достовірної інформації в найкоротші терміни є необхідним не тільки для Збройних сил України, а й для підрозділів Національної поліції. Саме тому все частіше можна зустріти інформацію, що поліція використовує методи OSINT в своїй службовій діяльності. Певний період часу OSINT асоціювався виключно з поняттям «конкурентна розвідка» та здебільшого використовувався в сфері бізнес-індустрії. Але обставини, в яких знаходиться наша країна, вимагають оперативних заходів, зокрема в інформаційному просторі.

OSINT (Open-source Intelligence) – це розвідка на основі відкритих джерел. Сама назва говорить про те, що під час проведення розвідки використовуються виключно відкриті джерела, які доступні усім [1].

Даний метод розвідки отримав свою популярність через зростання ролі Інтернету у суспільстві. Під час війни з рф для України надзвичайно важливо отримувати інформацію швидше та якісніше ніж ворог. Саме для виконання цього завдання Збройними Силами України, Національною поліцією та іншими

правоохоронними органами успішно використовується технологія OSINT, як складова технічного інструментарію для перемоги над ворогом та боротьби зі злочинністю.

Відповідно до ст. 1 Закону України «Про інформацію» інформація являє собою будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. У такий спосіб законодавець відносить до змісту інформації «відомості та/або дані», що означає – важливою є саме інформація, трансформована в певну форму представлення, тобто у вищезазначені дані або відомості, а не інформація як знання про факти, події і речі, які, у свою чергу, не є інформацією в чистому вигляд [2].

Джерела OSINT зазвичай розділяють на 6 категорій інформаційного потоку:

- ЗМІ: газети, журнали, радіо та телебачення;

- Інтернет, онлайн-публікації, блоги, дискусійні групи, медіа громадян (наприклад, відео з мобільних телефонів, контент, створений користувачами), YouTube та інші відеохостинги, вікі-довідники та вебсайти соціальних медіа (наприклад, Facebook, Twitter, Instagram тощо). Ці джерела випереджають безліч інших джерел через своєчасність та легкість доступу;

- державні дані, публічні урядові звіти, телефонні довідники, прес-конференції, вебсайти та виступи офіційних посадових осіб. Ці джерела є офіційними і публічно доступними, отже можуть використовуватися відкрито і вільно;

- професійні та академічні публікації, інформація, отримана з журналів, конференцій, симпозіумів та наукових праць;

- комерційні дані, комерційні зображення, фінансові та промислові оцінки, бази даних;

- так звана «сіра» література: технічні звіти, препринти, патенти, робочі та ділові документи [3].

Структурно реалізацію методу OSINT можна представити у вигляді низки

етапів або фаз, які безперервно повторюються, утворюючи циклічне коло: «Первинна постановка завдання – Збір інформації – Оцінка – Обробка (узагальнення) – Аналіз – Поширення (підготовка звіту, дайджесту, аналітичної довідки) – Повторна оцінка» і далі по колу.

На теперішній час існує багато методів отримання загальних відомостей про об’єкти, їх можна поділити на пасивні та активні.

Пасивні методи спираються на збір даних за допомогою спеціальних програм, що спрощують обробку отриманої інформації. Фактично таким видом розвідки можуть займатися всі, хто має доступ до мережі Інтернет. Частіше за все запити на таку інформацію роблять представники бізнесу аби проаналізувати репутацію та бекґраунд потенційного співробітника чи партнера. Таку роботу проводять, щоб впевнитися у його доброчесності й уникнути репутаційних й фінансових ризиків [4].

До пасивних методів можна віднести:

- **Аналіз соціальних мереж** (Facebook, Instagram, Twitter тощо). Аналізуючи дані соціальні мережі, можна отримати інформацію про суспільний стан, настрої громадськості, місце перебування осіб та об’єктів, що представляють інтерес та багато іншого, що особливо під час війни набуває важливості, а іноді навіть критичності.
- **Аналіз супутникових знімків, відкритих джерел відеозаписів та фотографій** може надати важливі відомості про військові об’єкти: місцезнаходження, переміщення та зміни стратегічної інфраструктури.
- **Моніторинг документів і звітів** дає можливість аналізувати відомості про конфлікт, які можуть містити дані про його хід та наслідки.
- **Отримання геолокаційних даних** про ворожі об’єкти, сили та засоби за допомогою загальнодоступних ресурсів, таких як Google Maps.

До активних методів належать:

- **Збір даних на закритих ресурсах,** куди інформація надходить раніше.
- **Використання програм для парсингу сайтів** з метою збору,

обробки та аналізу інформації.

• **Створення фальшивих вебресурсів,** наприклад каналів у месенджерах, підроблені вебресурси та фішингові сайти, які збирають дані про користувачів [5].

У якості інструментів забезпечення використання методу OSINT для автоматизації збирання відомостей з відкритих джерел на національному рівні застосовуються різноманітні засоби автоматизації, наприклад:

- Octoparse (www.octoparse.com) для вилучення вебданих;
- Microsoft Defender Threat Intelligence – платформа, що накопичує інформацію про різні мережні ресурси та надає можливість її структурованої обробки і аналізу;
- Hunchly (hunch.ly) та Kuiper (github.com/DFIRKuiper/Kuiper) – використовується з метою автоматизації процесу накопичення та обробки даних та здійснення взаємного обміну відповідними відомостями з колегами та керівництвом.

Окремі програмні інструменти активно застосовуються під час аналізу здобутої інформації, наприклад:

- MS Excel – для аналізу ступеня небезпеки організованих злочинних угруповань
- IBM i2 Analysts Notebook – для аналізу фінансових транзакцій;
- Gephi – для мережного аналізу груп в Telegram;
- Pajek – для мережного аналізу великих даних з соціальних мереж;
- Maltego – для аналізу результатів криміналістичної розвідки (FORINT) та розвідки з відкритих джерел (OSINT).

Враховуючи вищевикладене, а також опираючись на висновки Розвідувального управління Міністерства оборони США (DIA), необхідно зазначити, що близько 80 % розвідувальних даних DIA сьогодні надходить із матеріалів з відкритих джерел [6]. Можливість використання цієї маси інформації дала можливість всьому світу дізнатися про страшні злочини рф у війні з Україною та зрозуміти критичність ситуації у нашій країні.

Таким чином, застосування методу OSINT в умовах війни є актуальним, ефективним та доступним інструментом для Збройних Сил України та правоохоронних органів України, що використовується з метою наближення нашої перемоги над державою-терористом та здійснення ефективної боротьби зі злочинністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. OSINT: чому цей напрям такий перспективний і кому він може знадобитися? URL: https://www.issp.training/post/osint-chomu-tsey-napryam-takyy-perspektyvnyy-i-komu-vin-mozhe-znadobytysya (дата звернення 13.06.2024).

2. Бакумов О.С., Марчук М.І., Гудзь Т.І., Венглінський О. О. Інформація: до питання про змістову еволюцію терміна. Право і безпека – Право и безопасность – Law and Safety. 2021. No 3 (82). С.24. URL: https://pb.univd.edu.ua/index.php/PB/article/view/494/385 (дата звернення 13.06.2024).

3. Онищенко Ю.М. Використання методу OSINT під час підготовки фахівців з кібербезпеки / Ю.М. Онищенко // Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 17 листопада 2023 р. Одеса : ОДУВС, 2023. С. 24-26.

4. Що таке OSINT і як робити “звіт про людину” URL: https://filter.mkip.gov.ua/shho-take-osint-i-yak-zrobyty-zvit-pro-lyudynu/

5. Як OSINT впливає на війну в Україні? ITEDU//Blog. URL: http://surl.li/qgeog (дата звернення 13.06.2024).

6. Defense Intelligence Agency Expected to Lead Military’s Use of ‘Open Source’ Data. URL: https://www.wsj.com/articles/defense-intelligence-agency-expected-to-lead-militarys-use-of-open-source-data-11639142686 (дата звернення 13.06.2024).