УДК: 323.2 ***© Федонюк С. В.***

COLLABORATIVE OSINT

Відкрите співробітництво стає джерелом можливостей для вирішення різноманітних практичних завдань. Одним із напрямів застосування переваг відкритого співробітництва є використання генерованого його учасниками контенту з метою дослідження взаємозв'язку між різними об'єктами й подіями. Сьогодні, завдяки активності користувачів соціальних мереж, формуються масиви даних, достатні для того, що

б зробити достовірні висновки про діяльність як самих учасників соціальних взаємодій, так і пов'язаних з ними суб'єктів, що може бути успішно використано для досягнення цілей розвідки. Сьогодні є добре відомою така дисципліна як розвідка на основі відкритих джерел (Open source intelligence, OSINT), що включає пошук, збір і аналіз інформації, отриманої із загальнодоступних джерел. Такими джерелами є, наприклад, соціальні мережі, які вже сьогодні забезпечують достатню кількість матеріалу для проведення ефективних аналітичних досліджень у різних сферах (можливості використання потенціалу соціальних медіа в політичному аналізі узагальнено, наприклад, у роботі С. Штігліца й Л. Дан-Сюаня (2012) [5]. У практиці використовуються ефективні інструменти аналізу матеріалів з соціальних медій, як-от Crimson Hexagon, американська компанія, що спеціалізується на аналітиці в соціальних ЗМІ. У бібліотеці даних цієї компанії – більш ніж 500 мільярдів повідомлень у соціальних медіа (документи з соціальних мереж, таких як Twitter і Facebook, а також блогів, сайтів форумів, і новин [4].

Проте концепція OSINT вказує лише на загальнодоступність джерела (на відміну від секретних джерел та джерел з обмеженим використанням), і не пов'язана безпосередньо з поняттям open source або public intelligence. Такий підхід, наприклад, лежить в основі OSINT, що застосовується у практиці ЦРУ, у рамках якого з листопада 2005 р. функціонує DNI Open Source Center (OSC). OSC забезпечує отримання необхідної інформації з Інтернет, традиційних ЗМІ (наприклад, телебачення, радіо, газети, журнали), спеціалізованих журналів, матеріалів конференцій, фотографій, джерел геопросторової інформації (наприклад, карти і комерційні знімки).

Не зважаючи на те, що розвідка завжди отримувала основну масу інформації саме з відкритих джерел, суть OSINT радикально змінюється із поширенням відкритого співробітництва на основі інформаційно-комунікаційних технологій. Не випадково, що створення в ЦРУ підрозділу OSC співпало в часі саме з появою і швидким розгортанням соціальних мереж.

Ми говоримо про появу такого напряму в OSINT, який пов'язаний з діяльністю незалежних генераторів контенту в мережі Інтернет (учасники соціальних мереж, блогери,

автори фото- і відеоматеріалів на популярних медіаплатформах тощо. Також у мережі є достатньо суб'єктів, зацікавлених у тематичному зборі й аналізі інформації, які діють самостійно чи об'єднуються у співтовариствами за інтересами, які діють часто на основі вільного зацікавлення. Прикладом може бути діяльність Еліота Хіґґінса (народився у 1979 р.), відомого свого часу під псевдонімом Браун Мойсей (Brown Moses), – британського журналіста і блогера, який використовує для своїх досліджень відкриті джерела та соціальні ЗМІ. Хіґґінс найбільше відомий тим, що відкрив популярний проект Bellingcat, завдяки якому концентрує надзвичайно актуальні знання про війну в Сирії, російську військову інтервенцію в Україні і такі окремі події як збитий літак рейсу Malaysia Airlines Flight 17.

Хіґґінс працює, в основному, шляхом моніторингу більше як 450 каналів YouTube, щодня шукаючи зображення зброї та відстежуючи, де і коли, за яких обставин з'являються її нові зразки. Сам журналіст не має досвіду користування або навчання у сфері озброєнь і є повністю самоучкою, заявивши таке: «До арабської весни я не знав більше про зброю, ніж власник середньої Xbox. У мене не було ніяких знань, окрім того, що я дізнався від Арнольда Шварценеггера і Рембо» [6]. Він не говорить і не читає арабською. Але саме він першим повідомив про те, що уряд Сирії застосовує проти цивільного населення т. зв. «Бочкові бомби» великої потужності, що скидаються на житлові квартали з вертольотів, а також факти застосування урядом Асада касетних бомб, що останнім до цього наполегливо заперечувалось. Також розслідував випадки застосування урядовими силами хімічної зброї.

Аналіз систем озброєнь сирійського уряду, виконаний Хіґґінсом у вільний час в якості хобі, виявився настільки успішним, що незабаром на нього стала посилатися преса і правозахисні групи; на основі даних Хіггінса був зроблений запит в британському парламенті.

У липні 2014 р. Хіґґінс запустив вебсайт під назвою Bellingcat з метою об'єднати зусилля цивільних журналістів у розслідуванні поточних подій за відкритими джерелами, таким як відео- та фото-матеріали, супутникові знімки тощо. Серед інших проектів, Bellingcat розслідував катастрофу Боїнга 777 у Донецькій області , встановивши, що ракету, яка збила літак, випущено з установки ЗРК «Бук-М» з 53-ї бригади ППО РФ , що базується в Курську.

До методики Хіґґінса входять і використання даних геолокації, і візуальні маркери на зображеннях й інтерпретація супутникових знімків, що доступні вільно, відео, карти та іншу інформацію з відкритим кодом. Також повідомляється про використання спеціалізованих засобів автоматизованого аналізу, наприклад інструмент «Аналіз метаданих і рівня помилок» (Error Level Analysis, ELA).

На початку січня 2016 р. Bellingcat оголошує про встановлення імен 20 російських військових, які обслуговували зенітно-ракетний комплекс і отримали наказ на пуск ракети, про що Еліот Хіґґінс розповів в інтерв'ю DW [1]. Експертна група Bellingcat склала уточнений список 20 російських військовослужбовців, безпосередньо причетних до краху літака «Малайзійських авіаліній». Відповідна доповідь з докладною інформацією про кожного з військових передана прокуратурі Нідерландів. У відомстві обіцяли уважно вивчити отримані матеріали і, можливо, долучити їх до розслідування.

За словами Хіґґінса: «Для початку ми ідентифікували зенітно-ракетний комплекс «Бук», який, на нашу думку, випустив 17 липня ракету, що збила малайзійський авіалайнер рейсу MH17. По знімках, зроблених російськими громадянами в проміжку між 23 і 25 червня, ми змогли розпізнати його у військовій колоні, що рухалася в той момент по території РФ. Нам вдалося встановити, звідки йшов цей конвой: це була п'ятдесят третя зенітно-ракетна бригада під Курським. Після цього ми почали шукати всю інформацію про цей підрозділ, наявну в інтернеті. Багато військовослужбовців цієї бригади викладали інформацію в своїх профілях у соцмережах. Ми вивчили сотні, якщо не тисячі, профілів у пошуку людей, що мають відношення до справи. Встановили особи тих, хто був у цьому конвої, їх роль в бригаді. Після цього ми встановили, хто з найбільшою ймовірністю був безпосередньо причетний до запуску ракети, яка збила літак: командирів, які, ймовірно, і отримували наказ на пуск ракети, водіїв і операторів ракетної установки. У підсумку ми змогли виділити цю невелику групу людей. Ми вивчили їх сторінки, де вони викладали пости, обговорювали свою роботу. Деякі навіть викладали фотографії журналу чергувань на літні місяці 2014 року, де були перераховані всі військовослужбовці їх підрозділів. На підставі цього ми можемо судити про те, хто був задіяний, а хто – ні» [3].

По суті, можна говорити про особливу форму розвідки на основі відкритих джерел, яка базується на відкритому співробітництві – Collaborative OSINT або COSINT. Очевидно, його значення зростає, чому підтвердженням можна навести слова директора OSC ЦРУ (Douglas J. Naquin): «Організація, яка інвестує в open source сьогодні, те саме що, людина, яка інвестувала в Google протягом першого року. OSINT завжди був невід'ємним компонентом в розвідці, але протягом п'яти років, я вважаю, що його цінність може тільки зростати. Організація з високою оцінкою вартості і потенціалу OSINT буде найбільш ефективною в майбутньому» [2]. Очевидно, автор цитати мав на увазі передусім те, що можемо назвати COSINT.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bellingcat о трагедии MH17: Установлены личности управлявших «Буком» (January 5, 2016) // *Deutsche Welle (Russian).* – Retrieved 5 January 2016.

2. INTellingence: Open Source Intelligence [Electronic resource]. – Available at : https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html Posted: Jul 23, 2010 02:17 PM

3. MH17 – The Open Source Evidence – Final_ru.docx. *Bellingcat* [Electronic resource]. – Available at : https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-the-open-source-evidence/

4. Rohr, Erin (September 23, 2014). «Crimson Hexagon Indexes 500 Billion Social Media Posts For On-Demand Consumer Insight» // *Reuters.* – Retrieved 12 January 2016.

5. Stieglitz Stefan, Dang-Xuan Linh (13 July 2012) "Social media and political communication: a social media analytics framework". *Springer-Verlag.*

6. Weaver, Matthew. How Brown Moses exposed Syrian arms trafficking from his front room // *The Guardian.* – 21 March 2013.