https://www.proconference.org/index.php/usc/article/view/usc24-00-012
DOI: 10.30888/2709-2267.2024-20-00-012

УДК 004.056.5

DATA COLLECTION IN THE OSINT INVESTIGATION TECHNOLOGY CHAIN

ЗБІР ДАНИХ В ТЕХНОЛОГІЧНОМУ ЛАНЦЮЖКУ OSINT РОЗСЛІДУВАННЯ

Korobeinikova T.I. / Коробейнікова Т.І.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0003-2487-8742
Symak I.A. / Симак І.А.
студент / student
Lviv Polytechnic National University, S. Bandera St. 12, Lviv, 79013
Національний університет «Львівська політехніка», Львів, Бандери, 12, 79013

Анотація. *Робота присвячена дослідженню процесу збору даних в рамках OSINT розслідування. Пропонуються підходи до формалізації цього процесу, зокрема модель "циклу розвідки". Основна увага приділяється моделі циклу розвідки Гібсона. Автори пропонують метод зв'язків між об'єктами розслідування для ефективного збору даних. Цей метод використовує шість основних сутностей: особу, місце, організацію, подію, дію та продукт/систему. Це дозволяє зрозуміти, як різні сутності можуть бути пов'язані або не пов'язані, та розпочати пошуки залежно від конкретного об'єкта.*

Ключові слова: *OSINT розслідування, цикл розвідки, модель Гібсона, збір даних, обробка даних.*

Abstract. *The work is devoted to the study of the data collection process within the OSINT investigation. Approaches to the formalization of this process are proposed, in particular, the "intelligence cycle" model. The focus is on Gibson's model of the intelligence cycle. The authors propose a method of links between the objects of investigation for effective data collection. This method uses six main entities: person, place, organization, event, action and product/system. This allows you to understand how different entities may or may not be related and to start searches based on a specific entity.*

Key words: *OSINT investigation, intelligence cycle, Gibson model, data collection, data processing.*

Вступ.

Існує багато різних підходів до формалізації процесу OSINT розслідування. З метою перетворення необроблених даних на оперативну розвідувальну інформацію, Офіс директора Національної розвідки США (Office of the Director of National Intelligence) розробив модель під назвою "цикл розвідки" (intelligence cycle) [1]. Ця модель застосовується до всіх джерел розвідданих, включаючи OSINT, і була прийнята Гібсоном [2], а згодом із деякими модифікаціями, Хассаном та Хіджазі [3]. Базелл пропонує практичну інтерпретацію цієї моделі, яка використовується урядовими установами США як обов'язковий навчальний посібник [4]. Інші дослідження зосереджуються на

зборі та аналізі інформації, пропонуючи моделі, орієнтовані на ці завдання. До них належать комплексна триетапна модель, розроблена Пастором [5], та модель Табатабаеї [6].

Модель циклу розвідки Гібсона.

Розглянемо модель циклу розвідки Гібсона, оскільки вона є найбільш повною та активно використовується Національною розвідкою США (рис.1).

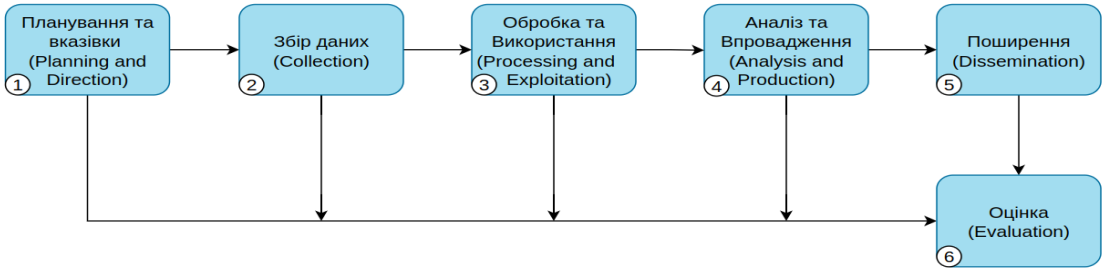

Рисунок 1 – Модель циклу розвідки Гібсона

Джерело [1]

Модель складається з шести етапів, що виконуються циклічно. Шостий крок, оцінка проводиться для кожного з інших п'яти етапів окремо і для розвідки в цілому. Розглянемо зміст кожного з процесів докладно:

Планування та вказівки. Цей етап є фундаментом циклу розвідки. Часто, вказівки передують безпосередньому плануванню. Зазвичай, у таких випадках споживач потребує конкретного продукту. Цей продукт може бути повним звітом, графічним зображенням або сирими даними, які збираються та поширюються, але оминають етап аналізу та обробки.

Збір даних. Збір даних проводиться для того, щоб зібрати неупорядковану інформацію, що стосується п'яти основних джерел розвідки (геопросторової розвідки (GEOINT), людської розвідки (HUMINT), розвідки за вимірювальними ознаками та сигналами (MASINT), розвідки з відкритих джерел (OSINT) та сигнальної розвідки (SIGINT)). Джерелами цих необроблених даних можуть бути, зокрема, новини, аерофотознімки, супутникові зображення, урядові та публічні документи.

Обробка та Використання. Цей етап передбачає залучення висококваліфікованого спеціалізованого персоналу та використання

технологічно складного обладнання для перетворення сирої інформації на зрозумілі та корисні відомості. Переклад даних, їх розшифровка та інтерпретація відзнятих зображень – це лише декілька методів перетворення даних, що зберігаються на плівці, магнітних носіях або інших носіях, в інформацію, готову до аналізу та обробки кінцевого продукту.

Аналіз та Впровадження – це етап інтеграції, оцінки, аналізування та підготовки обробленої інформації для включення її до кінцевого продукту. Цей етап також потребує залучення висококваліфікованого та спеціалізованого персоналу (аналітиків), завдання яких полягає у наданні сенсу обробленій інформації та визначенні її пріоритетності відповідно до відомих вимог. Синтезування обробленої інформації у готовий, дієвий розвідувальний продукт дозволяє зробити цю інформацію корисною для замовника.

Поширення – це етап доставлення кінцевого продукту замовнику, який його запросив, а також іншим зацікавленим сторонам. Замовник отримує готовий продукт, зазвичай, через електронну передачу. Кінцевий, готовий продукт називається “завершеною розвідкою” (finished intelligence). Після розповсюдження продукту можуть бути виявлені додаткові прогалини в розвідувальних даних, і цикл розвідки починається знову.

Оцінка – це процес постійного збору відгуків протягом циклу розвідки та їх аналізу для вдосконалення кожного окремого етапу та циклу загалом.

Процес збору даних в технологічному ланцюжку OSINT розслідування

На рис. 2 зображено схему процесу збору даних в технологічному ланцюжку OSINT, що є скаладовою авторського методу побудови зв’язків між об’єктами розслідування.

Етап збору даних є ключовим аспектом нашого дослідження в рамках цієї роботи. Для проведення ефективного розслідування на цьому етапі важливо дати відповідь на основні питання: яким є об’єкт/об’єкти дослідження? як об’єкти пов’язані чи не пов’язані? який план збору на основі операційних вимог? Для ефективної роботи, розіб’ємо етап збору даних за допомогою зв’язків між об’єктами дослідження. Це дасть змогу зрозуміти як різні

сутності/речі можуть бути пов’язані або не пов’язані та розпочати пошуки залежно від конкретного об'єкта. Розглянемо детально запропонований метод зв’язків між об’єктами розслідування, що використовує 6 основних сутностей:

1) Особа: Людина, яка брала участь у тій чи іншій події, наприклад, свідок, виконавець або жертва.
2) Місце: Фізична локація, де відбулася подія, наприклад, вулиця, місто, країна або будівля.
3) Організація: Компанія, уряд, або інша група осіб, яка пов'язана з подією, наприклад, поліція, лікарня або школа.
4) Подія: Це те, що сталося, наприклад, злочин, аварія або стихійне лихо. Також модіями є інциденти в інформаційних системах.
5) Дія: Будь-який навмисний чи не навмисний вид діяльності, що спричинив певну подію.
6) Продукт/Система: Це може бути товар, послуга або система, яка пов'язана з подією, наприклад, транспортний засіб, корпоративна мережа або програмне забезпечення.

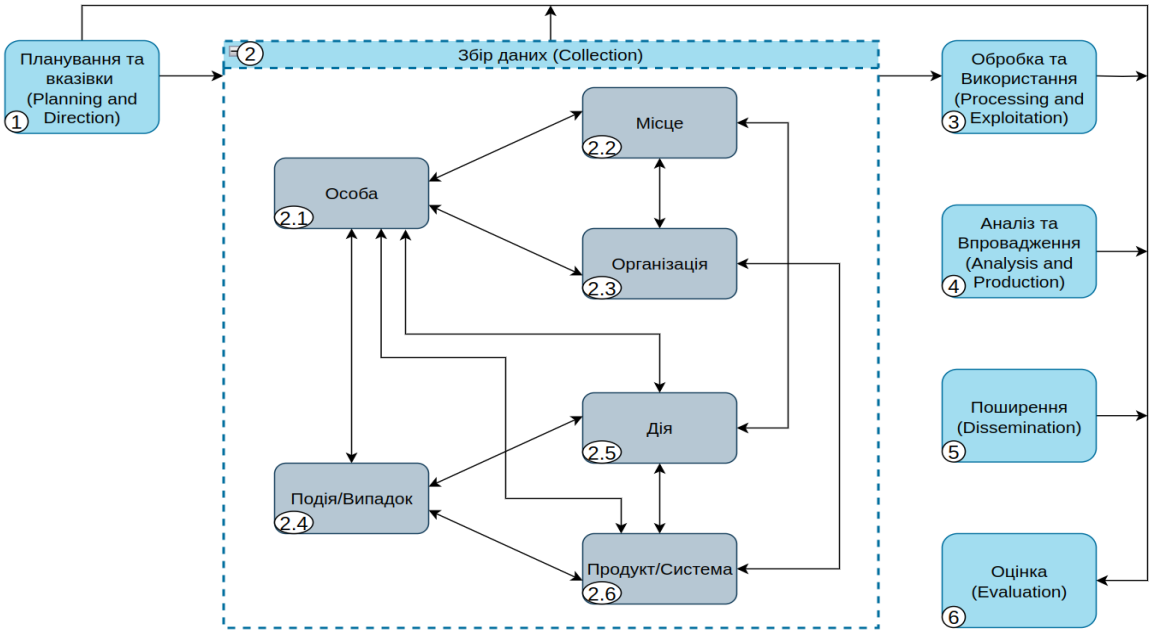

Рисунок 1 – Процес збору даних в технологічному ланцюжку OSINT

Авторська розробка

Література:

1. Office of the Director of National Intelligence [Ел. ресурс] – Режим доступу https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf.

2. Gibson H, OSINT – From Strategy to Implementation, ed. by B. Akhgar, P.S. Bayerl, F. Sampson (Springer, 2016), pp. 69 – 93

3. Hassan, Nihad A., and Rami Hijazi. Open source intelligence methods and tools. New York, NY: Apress, 2018.

4. Bazzell, Michael. Open source intelligence techniques: resources for searching and analyzing online information. CreateSpace Independent Publishing Platform, 2016.

5. J. Pastor-Galindo, P. Nespoli, F. Gómez Mármol and G. Martínez Pérez, "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends," in *IEEE Access*, vol. 8, pp. 10282-10304, 2020, doi: 10.1109/ACCESS.2020.2965257.

6. Tabatabei F, Wells D, in Open Source Intelligence Investigation – From Strategy to Implementation, ed. by B. Akhgar, P.S. Bayerl, F. Sampson (Springer, 2016), pp. 213 – 231.

Науковий керівник: к.т.н., доц. Коробейнікова Т.І.

Стаття надіслана: 19.05.2024 р.