Список використаних джерел

1. Heli Tiirmaa-Klaar. Building national cyber resilience and protecting critical information infrastructure. *Journal of Cyber Policy*. 2016. 1:1. P. 94–106.
2. Cyberspace 2025: Today's Decisions, Tomorrow's Terrain, Microsoft Report. June 2014. URL: https://query.prod.cms.rt.microsoft.com/cms/api/ am/binary/REXXtS.
3. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommen dation and Companion Document, OECD 2015. URL: https://www.oecd.org/publications/ digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm.
4. UK Centre for the Protection of National Infrastructure/ URL: https://www.protectuk.police.uk/news-views/centre-protection-national-infrastructure-cpni-has-evolved-become-national-protective#.

Денисенко Богдан Анатолійович,
експерт з питань спеціалізованих
правоохоронних органів
Консультативної місії Європейського
Союзу в Україні

МЕТОДОЛОГІЧНІ ЗАСАДИ OSINT

Процес цифровізації (діджиталізації), та, таким чином, генерування все більше і більше даних та інформації онлайн (та офлайн), не спинити. Таким чином, збільшується можливість більше, глибше та детальніше знаходити та верифікувати дані, інформацію щодо осіб, компаній, транспортних засобі, інших об'єктів та елементів дослідження, таким чином створюючи аналітичну розвідку (intelligence) з відкритих джерел (OSINT).

То *що ж таке OSINT (Opens Source Intelligence)*? Компанія «Reuser's Information Service» (RIS) у своєму тренінгу «OSINT Pathfinder» фокусує увагу на численних маніпуляціях з цим поняттям та визначенням. OSINT необхідно розглядати як процес, інструмент, механізм збору та продажу програмних продуктів. OSINT є спільною, інтегрованою методологією та процесом створення, де вимоги клієнта щодо аналітичної розвідки співпадають з наданою дієвою аналітичною розвідкою (*actionable intelligence*), створеною через процес синтезу та аналізу репрезентативної вибірки інформації з відкритих джерел, яка була валідованою, є надійною, вчасною та точною.

RIS також наголошує на змішуванні понять OSINT та OSINF. Оскільки, OSINF (*Open Source Information*) чи відкриті джерела є всією інформацією у будь-якому форматі, що може бути здобута будь-ким законним та етично-прийнятним шляхом без жодних обмежень, чи то безкоштовно, чи на платній основі. RIS наголошує на наступних обмеженнях та, відповідно, підсумовує, що простий збір, направлення необробленої сирої інформації не є OSINT. Під час збору інформації необхідно враховувати обмеження щодо авторського права, ліцензування та інтелектуального права власності. Хакерство, незаконне втручання у комп'ютерні мережі, злом паролів є незаконним та не може вважатись OSINT дослідженням. З етичної точки зору, наявність деяких ресурсів у відкритому доступі, у той час як вони не передбачені для відкритого доступу, не може вважатись інформацією з відкритих джерел.

RIS наголошує, що стандартний цикл аналітичної розвідки (*intelligence cycle*) не відповідає потребам OSINT-дослідження оскільки кількість кроків дослідження може змінюватись (відповідно до потреб конкретного дослідження). Особливістю запропонованого аналітично-розвідувального циклу OSINT є те, що клієнт, або замовник перебувають в центрі процесу. Сам цикл складається з 3-х під-циклів: підготовчий цикл, цикл звітування та цикл аналітичної розвідки. Аналітично-розвідувальний цикл OSINT передбачає трансформацію даних в зміни через, відповідно, формування інформації, аналітичної розвідки та рішень [1]. Кожен з під-циклів передбачає «звірку годинників» з клієнтом, або замовником, що наближає дослідження до задоволення реальних запитів та потреб клієнта або замовника (в нашому випадку – слідчого, керівника підрозділу, служби). Відповідно, для досягнення бажаного результату (мети дослідження), бажано мати чіткий план (з чітким аналізом вимог) та постійний контакт з замовником.

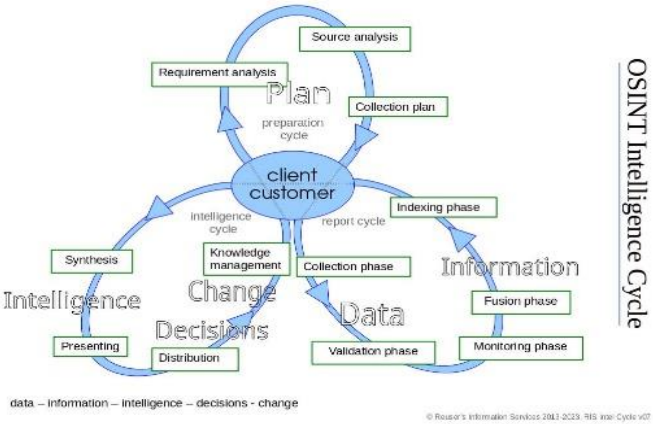

Рис. 1. Цикл OSINT (*джерело: Reuser's Information Service*)

Дані, інформація є основою для подальшого аналізу під час будь-якого дослідження, у тому числі OSINT. Кількість даних, інформації збільшується кардинально щоденно. Так, дослідження «International Data Corporation (IDC)», що є провідним світовим постачальником ринкової аналітичної розвідки (intelligence) та консультаційних послуг [2], показує, що станом на 2018 рік загальна кількість даних у світі становила 33 зетабайти (*зеттабайт – трильйон гігабайт*) та передбачалось, що їх кількість зросте до 175 зетабайт до 2025 року [3]. Дослідженням вже станом на 2020 рік встановлено, що загальний обсяг створених, зібраних, скопійованих і спожитих даних у всьому світі становив 64,2 зетабайти. Переглянутим дослідженням передбачається, що до 2025 року створення даних на глобальному рівні зросте вже до понад 180 зетабайт [4].

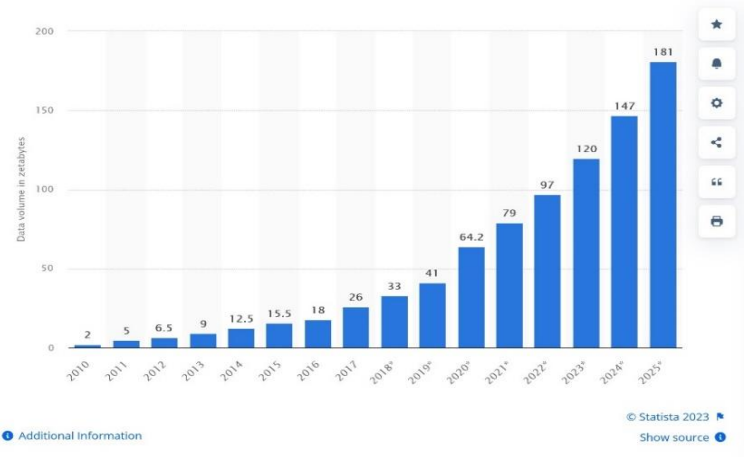

Рис. 2. Тренд зростання цифрових даних [5]

Станом на 2018 рік прогнозування передбачало, що протягом наступних семи років (до 2025 року) індустрія зберігання даних відвантажить 42 зетабайт (ZB) ємностей (пристроїв для зберігання даних); на пристроях IoT буде створено 90 ZB даних; 49 відсотків даних зберігатимуться в загальнодоступних хмарних середовищах; майже 30 відсотків згенерованих даних буде використовуватися в режимі реального часу [6]. Тенденції зберігаються та розвиваються, доповнюючись розвитком квантумних комп'ютерних можливостей, можливістю зберігання даних на молекулах ДНК, що є технологічним трендом 2023 року. Однак, цей процес зберігання є на даний час дуже коштовним та синтезування 1 мегабайту даних вартує біля 3,500 доларів США [7]. Однак, станом на 2019 рік науковці прогнозували, що до 2024 року ціна може впасти до 100 доларів США за синтез 1 терабайту даних, у випадку відповідного інвестування [8].

Ті незначні можливості архіваторів, як от ті, які надаються Wayback Machine, таким чином, не задовольняють всі потреби на запити історичних даних, у той же час, є потужним джерелом, у випадку, якщо архіватори все-таки змогли зберегти відповідні дані.

У сучасному світі все залишає цифрові сліди. Все більше пристроїв «інтернету речей» (Internet of things/IoT), тобто «розумних» пристроїв з'являються та використовуються у будь-

якій сфері життєдіяльності. Станом на кінець 2020 рік, з 21,7 мільярда активних підключених пристроїв у всьому світі понад 11,7 мільярда (54 %) є IoT пристроями [9].

Отже, розуміючи зростаючу тенденцію приросту відповідних пристроїв, розуміємо, що інформація про спосіб життя людини (через пристрої, що відслідковують переміщення, як от координати, швидкість, дані щодо зупинок та перебування, стан здоров'я, таке інше), у тому числі «розумні будинки», у тому числі пристрої для відео-спостереження та інші можливості, все менше і менше залишають можливостей зберігати анонімність людям, що користуються відповідними технологіями та пристроями. Та, відповідно, дають можливість тим, хто використовує ці зібрані дані – отримувати інформацію щодо способу життя фігуранта, будь-які інші відповідні дані «не виходячи з дому». Це, в свою чергу, викликає занепокоєння у багатьох правозахисних організацій.

Список використаних джерел

1. URL: https://opensourceintelligence.biz/osint-unlocked//
2. URL: https://www.idc.com/about
3. URL: https://www.networkworld.com/article/3325397/ idc-expect-175-zettabytes-of-data-worldwide-by-2025.html.
4. URL: https://www.statista.com/statistics/871513/worldwide-data-created/
5. URL: https://www.statista.com/statistics/871513/worldwide-data- created/.
6. URL: https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html.
7. URL: https://wyss.harvard.edu/technology/dna-data-storage/
8. URL: https://www.synbiobeta.com/read/dna-is-the-future-for-data-storage-that-future-is-coming-very-soon
9. URL: https://telecom.economictimes.indiatimes.com/news/at-12-billion-iot-connections-to-surpass-non-iot-devices-in-2020/79318722.