УДК 004.056.53

МЕТОДОЛОГІЯ ТА ІНСТРУМЕНТИ OSINT У КІБЕРРОЗВІДЦІ

Ю. В. Стадник[1], О. М. Барановський[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У роботі розглядається роль OSINT як ефективного інструменту кіберрозвідки в умовах сучасного інформаційного простору. Проаналізовано методологічні основи побудови розвідувального процесу, класифікацію джерел відкритої інформації, а також основні інструменти, що використовуються для збору та аналізу даних. Особливу увагу приділено етапам розвідувального циклу та їх практичному застосуванню в OSINT-аналізі. Результатом є демонстрація важливості системного підходу до роботи з відкритими даними для виявлення цифрових загроз.

Ключові слова: OSINT, кіберрозвідка, відкриті джерела, розвідувальний цикл.

Вступ

У сучасних умовах інформаційної війни та гібридних загроз, розвідка на основі відкритих джерел стала ключовим інструментом для аналітиків, спеціалістів з кібербезпеки та державних структур. OSINT дозволяє легально отримувати та обробляти дані з відкритих джерел з метою виявлення загроз, оцінки репутаційних ризиків та проведення цифрових розслідувань. Ця доповідь спрямована на дослідження основних етапів OSINT-процесу, класифікацію джерел інформації та аналіз практичних інструментів, що використовуються у сфері кіберрозвідки.

1. Теоретичні засади методології OSINT

1.1. Поняття та визначення OSINT

Згідно з NATO Open Source Intelligence Handbook [1, стор. 5] розвідка з відкритих джерел (Open Source Intelligence, або OSINT) – це не засекречена інформація, яка була цілеспрямовано виявлена, відібрана, оброблена та поширена серед визначеної аудиторії з метою відповіді на конкретне питання. Вона забезпечує дуже надійну основу для інших розвідувальних дисциплін. При систематичному використанні продукти OSINT можуть зменшити навантаження на засоби збору засекреченої інформації, обмежуючи запити лише тими питаннями, на які не можна відповісти за допомогою відкритих джерел.

1.2. Цикл OSINT-розвідки

Розвідка на основі відкритих джерел є не просто процесом збору інформації, а структурованим аналітичним підходом, який реалізується через чітку послідовність етапів – розвідувальний цикл. Цей цикл дозволяє систематизувати роботу аналітика, забезпечити якість даних та підвищити ефективність прийняття рішень на основі зібраної інформації. У випадку OSINT кожен етап — від формування запиту до презентації результатів – має свою специфіку, оскільки працює виключно з відкритими джерелами, які потребують критичної оцінки та обережної інтерпретації. Розуміння структури циклу є фундаментом для грамотного застосування OSINT у кібербезпеці, цифровій розвідці та аналізі ризиків.

Етапи розвідувального циклу [2] поділяються на (рис. 1):

- Підготовка – це етап, на якому оцінюються потреби та вимоги запиту, зокрема визначаються цілі завдання та ідентифікуються найкращі джерела для пошуку необхідної інформації.
- Збір – основний та найважливіший етап, що передбачає отримання даних та інформації з якомога більшої кількості релевантних джерел.
- Обробка – це організація або впорядкування зібраних даних та інформації.
- Аналіз та створення продукту – це інтерпретація зібраної інформації з метою осмислення її змісту, наприклад, виявлення шаблонів або формування хронології подій. На цьому етапі створюється звіт, який містить відповіді на розвідувальні запитання, висновки та рекомендації щодо подальших дій.
- Розповсюдження – це представлення та передача результатів розвідки з відкритих джерел, наприклад, у вигляді письмових звітів, хронологій, рекомендацій тощо. На цьому етапі надається відповідь на розвідувальне запитання зацікавленим сторонам.

2. Джерела та інструменти OSINT

2.1. Класифікація відкритих джерел

У контексті OSINT, відкриті джерела класифікуються за типами інформаційних потоків. Ця кла-

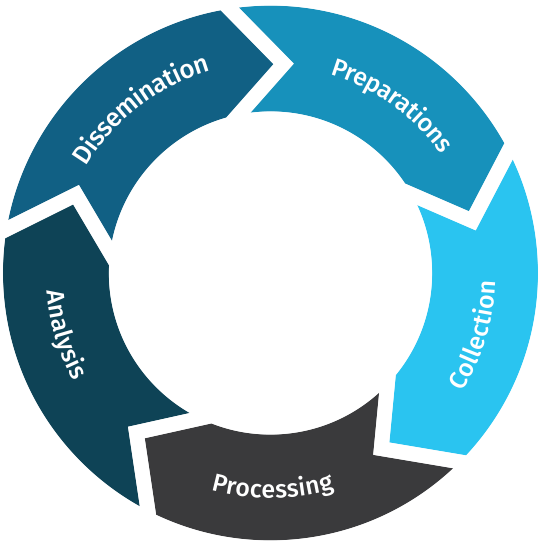

Рис. 1. Етапи розвідувального циклу [2]

сифікація допомагає систематизувати процес збору та аналізу даних. Згідно з джерелами, такими як Data.europa.eu [3], основні категорії відкритих джерел включають:

1. Медіа: Друковані газети, журнали, радіо та телебачення з різних країн.
2. Інтернет: Онлайн-публікації, блоги, форуми, громадянські медіа (наприклад, відео з мобільних телефонів, контент, створений користувачами), YouTube та інші соціальні медіа-платформи (наприклад, Facebook, Twitter, Instagram).
3. Публічні урядові дані: Публічні урядові звіти, бюджети, слухання, телефонні довідники, прес-конференції, веб-сайти та виступи.
4. Професійні та академічні публікації: Інформація, отримана з журналів, конференцій, симпозіумів, академічних робіт, дисертацій та тез.
5. Комерційні дані: Комерційні зображення, фінансові та промислові оцінки, бази даних.
6. Сіра література: Технічні звіти, препринти, патенти, робочі документи, бізнес-документи, неопубліковані роботи та інформаційні бюлетені.

Ця класифікація дозволяє ефективно організовувати процес збору інформації та забезпечує структурований підхід до аналізу відкритих джерел.

2.2. Інструменти для збору та аналізу інформації

Інструменти OSINT відіграють ключову роль у процесі автоматизованого збору, структурування та аналізу відкритої інформації. Залежно від поставленого завдання – чи це пошук технічних даних, соціальних профілів чи зв'язків між об'єктами — використовуються різні інструменти з відповідним функціоналом.

Інструменти технічного OSINT

Ці інструменти орієнтовані на збирання інформації про мережеву інфраструктуру, домени, IP-адреси, порти, сертифікати тощо:

- theHarvester – пошук email-адрес, доменів, субдоменів і метаданих.
- Recon-ng – модульна платформа для розвідки, яка працює за принципом фреймворку з можливістю підключення API.
- Shodan, Censys – пошукові системи для виявлення відкритих пристроїв і сервісів в Інтернеті.

Інструменти візуалізації та побудови зв'язків Використовуються для створення графів зв'язків між об'єктами (людьми, організаціями, адресами, телефонами тощо):

- Maltego – потужна графічна платформа для побудови зв'язків між цифровими сутностями.
- SpiderFoot – фреймворк, який дозволяє повністю автоматизувати збір даних про IP, домени, email, акаунти в соцмережах, витоки тощо.

Інструменти соціального OSINT Застосовуються для збору інформації з соціальних мереж та онлайн-платформ:

- Social-Searcher, Twint – пошук публікацій та активності користувачів у соціальних мережах.
- InVID – інструмент для перевірки відео та зображень, корисний при аналізі фейків та геолокації.

Універсальні інструменти та фреймворки

- OSINT Framework – структурований набір посилань на сотні інструментів, класифікованих за типами інформації.
- Google Dorking – метод глибокого пошуку у пошукових системах за допомогою спеціалізованих операторів.

Інтеграція цих інструментів у розвідувальний цикл дозволяє зменшити витрати часу, знизити ризик пропуску важливої інформації та створити об'єктивну картину об'єкта дослідження.

2.3. Види збору інформації

OSINT може застосовуватись до фізичних осіб, державних установ, комерційних організацій або програмного забезпечення. Існує три підходи до збору OSINT-даних [4]: пасивний, напівпасивний та активний. Ці три стратегії збору зазвичай використовуються для пояснення того, як отримується технічна інформація про цільову IT-систему.

- Пасивний збір даних: Головна мета OSINT-збору – отримання відомостей про об'єкт, використовуючи лише публічно доступні ресурси. У цьому випадку ціль не знає про ваші дії зі збору інформації.Такий тип аналізу практично не відстежується і має проводитись приватно. З технічної точки зору, цей метод передбачає мінімальне розкриття інформації про об'єкт, оскільки не відбувається безпосередньої комунікації з цільовим сервером. Основні джерела пасивного збору обмежуються архівною інформацією. Ці дані зазвичай застарілі, нешифровані та залишені на цільових системах.
- Напівпасивний збір даних: Цей метод передбачає незначну мережеву активність у напрямку цільової системи для отримання загальнодоступної інформації про неї. Трафік імітує звичайну

інтернет-активність, щоб не привертати увагу до розвідувальної діяльності. Таким чином, ви ненав'язливо досліджуєте об'єкт, не викликаючи підозр.Хоча цей тип збору вважається частково анонімним, ціль може зафіксувати його, якщо проводитиме поглиблений аналіз. Сервер або мережеві пристрої можуть зберегти записи, але без можливості однозначно ідентифікувати вас.

- Активний збір даних: У цьому підході ви безпосередньо взаємодієте з цільовою системою, щоб отримати розвіддані про неї. Оскільки аналітик OSINT використовує більш глибокі методи для збору технічної інформації про інфраструктуру об'єкта, ціль може помітити вашу активність.Це може включати: сканування відкритих портів, пошук вразливостей, аналіз неоновлених систем Windows, перевірку програмного забезпечення веб-серверів тощо. Такий трафік може виглядати як підозрілий або шкідливий і залишає сліди в системах виявлення атак (IDS) або системах запобігання вторгнень (IPS).

3. Застосування етапів розвідувального циклу в OSINT-аналізі

Практичний аналіз відкритих джерел у кіберрозвідці здійснюється у формі покрокового застосування розвідувального циклу. Кожен етап цього циклу виконується не абстрактно, а через конкретні дії, інструменти та аналітичні рішення.

На етапі підготовки обирається об'єкт дослідження — наприклад, домен організації, IP-адресу або псевдонім користувача. Формулюються точні запитання: "Які цифрові активи прив'язані до об'єкта? "Чи є витоки пов'язаних облікових записів? "Які ризики для інформаційної безпеки вони створюють?"Визначаються джерела інформації (технічні, соціальні, геопросторові) та набір інструментів для збору (Recon-ng, SpiderFoot, Shodan тощо).

На етапі збору здійснюється запуск сканувань або ручних пошуків: шукаються WHOIS-записи, DNS-записи, зібрані email-адреси, дані з форумів чи соцмереж, IP-інфраструктура. Використовуються автоматизовані фреймворки або API.

Обробка включає сортування отриманої інформації: дублікати фільтруються, непотрібні записи відсіюються, дані структуруються за типами. Наприклад, email-адреси групуються окремо, домени — окремо, IP — із зазначенням відкритих портів.

На етапі аналізу дані починають "працювати": визначаються взаємозв'язки між сутностями (наприклад, спільна IP-інфраструктура, реєстрація на один і той самий email), виявляються витоки в базах даних або старі піддомени. Результати оформлюються у вигляді аналітичного звіту з візуалізацією графів, таблицями або хронологією подій.

Поширення — це завершальна стадія, де сформовані висновки передаються замовнику або керівництву. Висновки можуть містити рекомендації щодо підвищення конфіденційності, виявлення вразливостей або необхідність вжиття заходів реагування.

Висновки

У результаті проведеної роботи встановлено, що OSINT є важливим напрямом сучасної кіберрозвідки, який дозволяє легально та ефективно отримувати інформацію з відкритих джерел. Методологія OSINT базується на структурованому розвідувальному циклі, кожен етап якого — від підготовки до поширення — має практичне значення та спрямований на створення цінного аналітичного продукту.

Класифікація джерел відкритої інформації дозволяє системно підходити до пошуку даних, а сучасні інструменти — значно автоматизувати цей процес. У роботі було проаналізовано низку інструментів, які дають змогу здійснювати як технічну, так і соціальну розвідку, будувати зв'язки між об'єктами та виявляти потенційні загрози для інформаційної безпеки.

Таким чином, OSINT є не просто допоміжним засобом, а повноцінним інструментом кібербезпеки, який при грамотному використанні забезпечує глибоке розуміння цифрової присутності об'єкта розвідки та підтримує прийняття обґрунтованих рішень у сфері захисту інформації.

Перелік використаних джерел

1. *Kernan W. F.* NATO Open Source Intelligence Handbook. — 2001. — 5 с.
2. *Sans.* What is Open-Source Intelligence? — 02/23/2023. — URL: https://www.sans.org/blog/what-is-open-source-intelligence/.
3. *Data.europa.eu.* What is OSINT: Open-source intelligence? — 05/02/2022. — URL: https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence.
4. *Mosse-institute.* OSINT Information Gathering Types. — 2022. — URL: https://library.mosse-institute.com/articles/2022/07/osint-information-gathering-types/osint-information-gathering-types.html?highlight=osint%20information%20gathering%20types.