УДК 004.62

Сторчак А.С., канд. техн. наук
Самойлов І.В. канд. техн. наук
Національний технічний університет України «КПІ ім. Ігоря Сікорського»,
storchakanton@gmail.com

ВИКОРИСТАННЯ OSINT-ТЕХНОЛОГІЇ В СУЧАСНИХ СЕРВІСАХ

Питання комплексної допомоги військовим на полі бою, серед іншого, забезпечується шляхом пошуку та своєчасного надання інформації. Для цієї мети використовується OSINT – розвідка за допомогою публічно доступних даних. Аналізуються цифрові сліди, які користувачі залишають на відкритих платформах [1].

OSINT – це метод збору інформації з публічних або інших відкритих джерел, який можуть використовувати експерти з безпеки, національні розвідувальні агентства або кіберзлочинці. Метою використання кіберзахисниками є виявлення публічно доступної інформації, пов'язаної з їхньою організацією, яку можуть використовувати зловмисники. Одним з основних джерел розвідки, яке важко не помітити, є велика кількість публічно доступної інформації, яку створюють споживачі та блогери щодня [2]. Враховуючи великі обсяги інформації у різних форматах, виникає завдання скорочення часу збору інформації та підвищення надійності та повноти отриманих даних.

Для вирішення поставленого завдання доцільно проаналізувати засоби OSINT та розробити алгоритм використання OSINT-технології у сучасних сервісах.

Запропонований OSINT-алгоритм призначений передусім для вивчення об'єктів, які використовують соціальні мережі та сучасні сервіси (включаючи розважальні). Метою алгоритму є збір даних про групу людей на основі сервісів (TikTok, YouTube Shorts, тощо) з використанням публічно доступних засобів OSINT для аналізу, збору та обробки даних.

Для реалізації запропонованого алгоритму необхідно виконати послідовність дій:

Крок 1: Визначити основну мету операції OSINT. Проаналізувати засоби, які будуть використані для кожного окремого випадку (Shodan, Google Docker, Metagoofil, Whois і т.і.).

Крок 2: Вибрати робоче місце. Забезпечити безпечне підключення до Інтернету.

Крок 3: Обрати мобільний емулятор.

Крок 4: Поєднати засоби з кроків 2 і 3, у віртуальну машину. Створити обліковий запис у потрібному сервісі: використовувати ті ж дані, що й у об'єкта дослідження.

Крок 5: Максимально деталізувати отриману інформацію про об'єкт і застосовувати її при налаштуванні рекомендацій.

Крок 6: Зібрати дані, що отримано в результаті спостережень.

Крок 7: Визначити геопозицію об'єкта на основі отриманого масиву даних.

Крок 8: Деталізувати отримані в процесі розвідки персональні дані. Написати звіт.

Основою збору даних є низький рівень кібергігієни об'єктів дослідження, необережне ставлення до поширення своїх конфіденційних даних. Шляхом ефективного використання OSINT-інструментів та дотримання систематичного підходу можна отримати цінні відомості з публічно доступних даних. Ця інформація може бути вирішальною для різних завдань: військова розвідка, кібербезпека, правоохоронна діяльність. Але важливо зберігати баланс між збором даних для законних цілей і повагою до прав особистої приватності.

Список посилань

1. NATO Open Source Intelligence Handbook [Electronic resource]. – Режим доступу: https://archive.org/details/NATOOSINTHandbookV1.2

2. Tanabe, Roberto & Albuquerque, Robson & Da Silva Filho, Demetrio & Alves-da-Silva, Daniel & Gondim, Joao. (2023). OSINT Methods in the Intelligence Cycle. 10.1007/978-3-031-30592-4_4. / International Conference on Computer Science, Electronics and Industrial Engineering – pp.42-54.