

УДК:004.4

Орловський Д.І.¹, Неласа Г.В.²

¹ студ. гр. РТ-818 НУ «Запорізька політехніка»

² проф. НУ «Запорізька політехніка»

ТЕХНІКА РОЗВІДКИ ЗА ВІДКРИТИМИ ДЖЕРЕЛАМИ ІНФОРМАЦІЇ. ТЕХНОЛОГІЇ OSINT. ВИВЧЕННЯ ПРОТОКОЛУ BIT-TORRENT ЗАСОБАМИ OSINT

Open source intelligence (OSINT) – концепція добування і використання інформації із відкритих та загальнодоступних джерел. Суттєво відрізняється від інших типів розвідувальної діяльності законністю та доступністю для будь-якого громадянина.

Джерелом OSINT є: ЗМІ, форуми, соціальні мережі, блоги; публічні звіти, спостереження (супутникові знімки); академічні або професійні статі, звіти, доповіді, тощо.

В Україні тема OSINT стала відома завдяки діяльності журналістських спілок «Миротворець», InformNapalm, Bellingcat, які доводять факти російської агресії, а саме: військові частини Російської Федерації, які приймали участь у бойових діях проти України на Донбасі та в АР Криму; інформація про збиття Boeing 777 біля Донецьку, тощо.

Data Scraping – технологія отримання даних з комп'ютерної середовища у зрозумілому для людини форматі.

Поділяється на декілька видів: запис екрану; веб-скрапінг («взяття» інформації з HTML або JSON); комп'ютерно-програмний звіт (інформації з показів центрального процесору, оперативної пам'яті, жорсткого диску).

Отже, **метою** проекту є практика OSINT з використанням технології Data Scraping, а саме вивчення платформи для аналізу BitTorrent протоколу для реалізації мети автори ставить наступні завдання:

Розробка веб-інтерфейсу, на якому відображається інформація про завантажений контент певною IP-адресою з сигналізуванням наявності забороненого контенту.

Створення бази даних, з даними про IP-адреси та скачуванні файли.

Створення загальнодоступного API для інтерфейсів (боти, тощо)

Розробка системи аутентифікації користувачів на платформі.

Опрацювання CSV файлів(потокowego внесення даних таблицею).

Реалізація адмін-панелі з доступом до бази.

Поставлена мета реалізується засобами програмування JavaScript, а саме:

Платформа «Node JS(Express)»;

База даних – «MongoDB»;

Парсер веб-сторінки – Cheerio;

Сайт з інформацією - iknowwhatyoudownload.com

Одна з особливостей, яку необхідно донести, полягає в тому, що не в умовах динамічної IP-адресації наявність скачаного контенту з однієї IP-адресу не є підставою звинувачувати людину, а є натяком на можливість аудиту цієї адреси.

На фінальному етапі проекту була виконана мета і був створений загальнодоступний веб-сайт: <https://scrambleproject.herokuapp.com>.

Автори планують розвивати свій проект за допомогою таких нововведень:

Перенесення інтерфейсу на React JS (швидкість інтерфейсу)

Доведення до кінця адмін-панелі.

Додавання іншого функціоналу із практики OSINT. Наприклад: пошук людей за нік-неймом у мережі, аналіз мобільних номерів через платформу OLCX, тощо.

Таким чином, завдяки принципу OSINT, можливо отримати інформацію про завантаження файлів у BitTorrent протоколі певною людиною, зробити аналіз наявності порушення законодавства тощо. З іншого боку, наявність у відкритому доступі значної кількості компрометуючої інформації спонукає захищати персональні дані, користуватись VPN, TOR, вивчати правила веб-гігієни, тощо.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. OSINT. Що це? -<https://ru.wikipedia.org/wiki/OSINT>

2. Документація NODE.JS - <https://nodejs.org/uk/docs/>
3. MongoDB Guide - <https://docs.mongodb.com/guides/>
4. PassportJS(аутентифікація) - <http://www.passportjs.org/docs/>