УДК:343.983
https://orcid.org/0000-0002-0892-1694
DOI https://doi.org/10.32703/2663-6352/2021-1-9-97-104

Михайлов Володимир Олександрович,
старший викладач кафедри правосуддя
Юридичного факультету
Інституту управління, технологій та права
Державного університету інфраструктури та технологій,
м.Київ Україна

ПИТАННЯ ВИКОРИСТАННЯ МЕТОДІВ OSINT У КРИМІНАЛІСТИЦІ

Анотація. *Дана робота окреслює певний ряд можливостей та проблем використання методів OSINT у криміналістиці. У статті наведений перелік програмного забезпечення для пошуку та аналізу інформації.*

Ключові слова: методи OSINT, відкриті данні, програмне забезпечення для пошуку та аналізу інформації, антикорупційна діяльність, правоохоронні органи, криміналістика, кримінальний процес, адміністративне законодавство.

Annotation. *Current world's trends tend to digitalize all activities and the internet has accumulated large amounts of information that can be used in solving and investigating of crimes.*

OSINT-a term that translates as Open - source intelligence-is a method of searching, collecting, selecting, and analyzing information of operational interest from open sources. The data obtained in this way is used by marketers, journalists, computer and internet security specialists, etc. existing OSINT tools can also be used by criminologists to investigate and solve crimes, collect information about the identity of the criminal, etc. But unfortunately, the use of these methods is not enshrined in law either in the Criminal Procedure legislation or in the law on operational search activities, although in practice these methods are used by some law enforcement officers. This paper outlines a number of opportunities and problems of using OSINT methods in criminalistics. The article provides a list of software for searching and analyzing information.

The Internet has accumulated a large amount of information that can be used in the investigation of crimes, the collection of information about the identity of the offender and the study of digital footprints. The above list of tools is not exhaustive, we did not disclose the topics of open state registers, which simplify the request for information, the possibility of using bots and Telegram, WhatsApp, Viber. The issue of the large number of databases that have emerged online as a result of information leaks from public and private organizations also remains open.

In our opinion, modern methods of search, collection and analysis of information should be constantly researched, updated, systematized and used in the investigation of crimes. It is also necessary to develop legislation to legalize these methods in criminal proceedings and operational and investigative activities. In addition, it is necessary to study these methods in forensics and in retraining and

advanced training courses for law enforcement officers. Or even organize units of specialists to help investigators and judges obtain and legalize information in the process.

Keyword: OSINT methods, open data, software for searching and analyzing information, anti-corruption activities, law enforcement, criminology, criminal procedure, administrative legislation.

Постановка проблеми. В сучасних умовах діджиталізації світу, у мережі інтернет накопичилось великі обсяги інформації, яку можна використовувати у розкритті та розслідуванні злочинів.

OSINT- термін який перекладається як Open-source intelligence, - це методи пошуку, збору, вибору та аналізу інформації яка являє оперативний інтерес з відкритих джерел. Отримані дані таким чином використовують маркетологи, журналісти, фахівці з комп'ютерної та інтернет-безпеки та ін [1]. Існуючі OSINT-інструменти можуть використовувати і криміналісти для роботи по розслідуванню та розкриттю злочинів, збору інформації про особу злочинця та ін. Але нажаль використання даних методів не закріплено законодавчо ні в кримінально-процесуальному законодавстві ні в законі про оперативно-розшукову діяльність, хоча на практиці ці методи застосовують деякі правоохоронці, а науковці пропонують адаптацію правових норм під методи OSINT.

Огляд останніх досліджень і публікацій. Проблеми щодо використання методів OSINT досліджувалися у працях таких вчених та науковців як С.В. Албул, В.В. Антонюк, В.В. Білоус, В.В. Бірюков, К.С. Ісмайлов, О.Ю. Іохов, І.І. Карташов, О.О. Кожушко, Д.В. Ланде, О.В. Манжай, О.В. Минько, В.Т. Оленченко, С.А. Постолов, В.Г. Путятин, Н.Ф. Ржевська, П.С. Романько. В.Д. Щербань та інші автори.

Формулювання завдання дослідження. Метою роботи є виявлення та окреслення проблем щодо можливостей використання методів OSINT у криміналістиці. Узагальнити перелік програмного забезпечення та методів для пошуку та аналізу інформації. Запропоновати шляхи вдосконалення чинного законодавства стосовно впровадження методів OSINT у правоохоронну діяльність.

Основні матеріали дослідження.

Для пошуку за відкритими даними розроблено безліч автоматизованих рішень. У статті зазначені найпопулярніші з них, починаючи від найбільш автоматизованих, закінчуючи ручним збором інформації зі спеціалізованих сервісів.

Програмне забезпечення для автоматичного збору інформації з відкритих джерел:

- Maltego - це інструмент аналітики з відкритим вихідним кодом і графічного аналізу посилань для збору і зв'язку інформації для дослідницьких завдань.

- SpiderFoot - це інструмент для професіоналів, які хочуть автоматизувати OSINT для аналізу загроз, виявлення активів, моніторингу поверхні атаки або оцінки безпеки.

- Creepy - це інструмент геолокації з відкритим вихідним кодом. Він збирає інформацію про геолокації за допомогою різних платформ соціальних мереж і послуг хостингу зображень, які вже опубліковані десь ще [4].

Цей список не є вичерпним, однак це найпопулярніше програмне забезпечення для збору інформації.

Сервіси і фреймворки для пошуку інформації:

- OSINT Framework - орієнтований на збір інформації з безкоштовних інструментів або ресурсів, його мета - допомогти людям знайти безкоштовні ресурси OSINT. Деякі з включених сайтів можуть вимагати реєстрації або пропонувати більше даних за оплату, але залишається можливість отримати хоча б частину доступної інформації безкоштовно.

- Shodan.io - це пошукова система, яка збирає інформацію про вразливі пристрої, які підключені до мережі. Коли хакерам лінь зламувати системи відеоспостереження, модеми, холодильники, wi-fi роутери, праски, телевізори з мікрофоном або навіть чайники, вони просто заходять в Shodan і беруть доступ до домашніх пристроїв прямо з ресурсу.

Google Dorking - теж є інструментом для пошуку вразливих ресурсів і даних.

Правильне використання пошукової системи Google допоможе знайти величезну кількість інформації. Якщо відоме ім'я та прізвище, мобільний телефон особи, що представляє оперативний інтерес, необхідно при запиті помістити їх в лапки, інакше Google наддасть перелік подібних популярних запитів, які не відповідають тому, що конкретно необхідно знайти.

Не слід обмежуватись одним Google: перевіряти данні про особу необхідно також в інших пошукових системах - Bing, DuckDuckGo. Можливо вони покажуть іншу інформацію.

Отже, якщо пошук по реальному імені нічого не дав або потрібна додаткова інформація, необхідно пробувати шукати комбінації ПІБ, назви електронної пошти або домену сайту, яким людина володіє. Найпростіший спосіб - пошукати ці комбінації в пошукових системах.

GetContact, Eyecon, PhoneInfoga мабуть, самі відомі сервіси для сканування телефонних номерів. PhoneInfoga використовує тільки безкоштовні ресурси та працює для будь-яких міжнародних номерів з великою точністю. Далі PhoneInfoga визначає VoIP провайдера і інші дані, за допомогою яких можна продовжити шукати цифрові сліди.

Пошук по фотографії чи зображення, стало актуальним з появою великої кількості камер відео спостереження та таких систем як «Безпечне місто».

Для того щоб дізнатися, де використовувалося зображення або де воно з'явилося вперше, використовуйте пошук по зображеннях. Він є в основних пошукових системах - Google Images, Bing Images, Baidu Images. Також варто скористатися сервісом TinEye, чиї алгоритми відрізняються від Google. Пошук по зображеннях є і в соціальних мережах: Findclone і Findmevk.com. Крім цього

існують спеціалізовані плагіни - RevEye для Chrome, Image Search Options для Firefox. Мобільні додатки на зразок CamFind можуть впізнати речі з реального світу. А Image Identification Project використовує для цього штучний інтелект. Якщо зображення містить EXIF-дані (інформацію про камеру, геокоординати, режиму зйомки і т.п.), то варто їх проаналізувати. Побачити (і змінити) їх можна за допомогою будь-якого редактора зображень або невеликої програми Exiftool. Є також схожі онлайн-сервіси - exifdata.com і viewexifdata.com. Видалити EXIF-дані можна за допомогою exifpurge.com або verexif.com. Інший ресурс, stolencamerafinder.com, визначає камеру за серійним номером і шукає в інтернеті, які ще фото були зроблені нею. Перевірити зображення на предмет монтажа та інші маніпуляції можна за допомогою Forensically або FotoForensics. Якщо ви не хочете завантажувати картинку в інтернет, використовуйте програми Phoenix або Ghiro. У Ghiro функції більш автоматизовані і дають більше можливостей, ніж попередні сервіси.

Якщо потрібно зробити зображення більш чітким, наприклад погано відобразився номер державної реєстрації авто на фото, чи інше, то зможуть допомогти наступні програмні інструменти:

- Smartdeblur - прибирає розмиття, відновлює фокус, а також вміє покращувати в цілому чіткість картинки.
- Blurity - прибирає розмиття.
- Letsenhance.io - покращує і масштабує зображення онлайн, використовуючи штучний інтелект [3].

Велику кількість інформації можна знайти при зборі та моніторингу даних в соціальних мережах.

Facebook:

- Stalkscan - показує всю публічно доступну інформацію про людину.
- ExractFace - вивантажує дані з Facebook для оффлайн-використання і подальшого аналізу.
- Facebook Sleep Stats - показує приблизний режим сну людини, беручи за основу онлайн і оффлайн-статуси. Lookup-id.com - знаходить ID профілю або групи Twitter.

Instagram:

- www.picodash.com - вивантажує статистику конкретного користувача або обраного хештега в форматі CSV. Також вивантажує лайки і коментарі.
- https://web.stagram.com - підходить для перегляду і вивантаження відео і зображень.
- https://codeofaninja.com/tools/find-instagram-user-id - знаходить ID користувача. Ім'я облікового запису користувач може змінювати, за допомогою ID можна не втратити його з поля зору.
- http://instadp.com - показує зображення профіля в повному розмірі.
- https://sometag.org - шукає популярні хештеги, локації і акаунти. Крім того, порівнює акаунти і вивантажує статистику по передплатникам і хештег.

LinkedIn InSpy - Python-програма, яка вміє знаходити працівників тієї чи іншої компанії. Також знаходить технології, що застосовуються в компанії, за заданими ключовими словами.

LinkedInt - знаходить e-mail людей, які працюють в одній і тій же компанії. Вміє визначати поштові скриньки також по заданому домену, який належить компанії.

Серед проблем правового забезпечення методів OSINT вірно вказано у статті Щербаня В.Д. з посиланнями на Закону України «Про оперативно-розшукову діяльність». У пункті 15 частини 1 статті 8 Закону України «Про оперативно-розшукову діяльність» від 18.02.1992 № 2135-XII [6] встановлено, що ще одним із прав оперативних підрозділів органів внутрішніх справ є право отримувати від юридичних чи фізичних осіб безкоштовно або за винагороду інформацію про злочини, що готуються або вчинені, та про загрозу безпеці суспільства і держави. У даному контексті варто зробити уточнення, що дане положення доцільно розглядати як адміністративно-правовий метод здійснення OSINT у сфері антикорупційної діяльності правоохоронних органів лише у тому випадку, коли у такий спосіб отримується інформація, не віднесена законом до інформації з обмеженим доступом (офіційна інформація, інформація, що видається громадськими організаціями, комерційними компаніями і засобами масової інформації), і при цьому вона не порушує таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, та не є конфіденційною [7].

Гарантія обов'язку суб'єктів владних повноважень визначити спеціальні підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації також має безпосередній вплив і на функціонування OSINT у сфері антикорупційної діяльності, адже в розвідці з відкритих джерел може використовуватись будь-яка інформація із відкритих джерел. У свою чергу, відкритими є не лише ті джерела, які безпосередньо пов'язані із особою, а й різноманітні державні бази даних. Гарантія здійснення державного і громадського контролю за додержанням законодавства про інформацію означає, що використання права вільно збирати, зберігати та використовувати інформацію забезпечена державним і громадським контролем, а отже, правоохоронні органи також можуть скористатись даним правом. Гарантія встановлення відповідальності за порушення законодавства про інформацію також більшою мірою стосується різноманітних державних баз даних, проте її варто віднести до тих передумов, які спрощують функціонування OSINT у сфері антикорупційної діяльності в правоохоронних органах [12].

У правоохоронній сфері OSINT використовується, не тільки в антикорупційної діяльності, а в цілому для запобігання, розслідування та переслідування злочинів пов'язаних з Інтернетом. Особливо це стосується протидії терористичним організаціям, незаконному відмиванню та легалізації грошей отриманих злочинним шляхом, боротьбі з розповсюдження наркотичних речовин, зброї тощо. Пошук у соціальних мережах потенційно небезпечних груп та індивідуумів є важливою частиною роботи міжнародних правоохоронних організаціях таких як Europol чи Interpol [9].

Забезпечення права доступу до інформації з відкритих джерел передбачено і у нормах Закону України «Про доступ до публічної інформації» від 13.01.2011 р. № 2939-VI4. У ст. 3 встановлено, що право на доступ до

публічної інформації гарантується: 1) обов'язком розпорядників інформації надавати та оприлюднювати інформацію, крім випадків, передбачених законом; 2) визначенням розпорядником інформації спеціальних структурних підрозділів або посадових осіб, які організовують у встановленому порядку доступ до публічної інформації, якою він володіє; 3) максимальним спрощенням процедури подання запиту та отримання інформації; 4) доступом до засідань колегіальних суб'єктів владних повноважень, крім випадків, передбачених законодавством; 5) здійсненням парламентського, громадського та державного контролю за дотриманням прав на доступ до публічної інформації; 6) юридичною відповідальністю за порушення законодавства про доступ до публічної інформації [10].

Відповідно до статті 4 Закону України "Про захист персональних даних" від 01.06.2010 р. № 2297-VI: "Суб'єктами відносин, яка пов'язана з персональними даними, є: - суб'єкт персональних даних; - власник бази персональних даних; - розпорядник бази персональних даних; - третя особа; - уповноважений державний орган з питань захисту персональних даних; - інші органи державної влади і органи місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних"[11].

В українському законодавстві передбачено повідомний характер обробки персональних даних. Власник або розпорядник (оператор) до початку обробки персональних даних зобов'язаний повідомити уповноважений орган із захисту прав суб'єктів персональних даних про свій намір здійснювати обробку персональних даних. Потім дані про власників або розпорядників (операторів) вносяться до спеціального реєстру операторів. Інформація, що міститься в реєстрі операторів, стає загальнодоступною. Закони про персональні дані стосуються більшості населення як учасників процесу "обробки" даних. А так як суб'єктом персональних даних є кожна людина, то Закон має загальний характер і стосується кожного. Зокрема, персональні дані широко використовуються в соціальних мережах і сервісах електронної пошти. Сучасна Інтернет-компанія збирає і обробляє різні категорії персональних даних – своїх співробітників, своїх контрагентів за договорами і деякі дані користувачів своїх сервісів. Люди, що розміщують інформацію про себе в соціальних мережах або службах знайомств, свідомо роблять її відкритою для всіх користувачів ресурсу, і по закону її можна трактувати як "загальнодоступну", а значить, дотримання особливого режиму конфіденційності щодо її не потрібно, але в соціальних мережах є і інформація, яку користувач приховує, роблячи її доступною тільки для окремої групи користувачів ("друзів"). У цьому випадку Інтернет-ресурс повинен передбачати для неї спеціальні засоби захисту [13].

Для легалізації інформації у кримінальному провадженні отриманими за допомогою методів OSINT учасниками кримінального процесу, які знайшли її у відкритих джерелах в мережі Інтернет, і яка є загальнодоступною, для її обробки без згоди суб'єкта персональних даних, все ж таки потрібно звертатися с запитом до власника бази даних. Однак при цьому обов'язок доведення, що оброблювані персональні дані є загальнодоступними, покладається на власника або розпорядника. А це означає, що необхідно або накопичувати докази того, що

дані взяті з загальнодоступних джерел, або отримувати згоду від суб'єкта персональних даних і потім долучати цей документ до матеріалів провадження. Інакше є ймовірність, що така інформація буде визнана неналежним та недопустимим доказом. Крім того, потрібно мати документ, що підтверджує загальнодоступність джерела персональних даних. При цьому залишається без відповіді проблемні питання доведеності того, що власник інформаційного ресурсу (веб-сайту) володіє письмовою згодою на обробку чи взагалі зареєстрований в Україні та має тут представництво. Тому питання потребує подальшого вивчення та запровадження відповідних змін в законодавстві.

Висновки.

Отже, стрімке зростання ролі та цінності інформації, розвиток інформаційних технологій, програмних та апаратних засобів, доступність мережі Інтернет, збільшення інформаційного потоку відкритої інформації з одного боку та запровадження методів OSINT, як складової криміналістики з іншого боку ставить збір та аналіз інформації з відкритих джерел одним із дієвих сучасних засобів протидії кримінальним правопорушенням. Серед методів аналізу інформації із відкритих джерел можна відзначити будь-які загальнонаукові методи та криміналістичні методи, які дозволяють зробити висновки, щодо вчинення злочину.

Слід зазначити, що у мережі інтернет накопичилась велика кількість інформації, яку можна використовувати при розслідуванні злочинів, зборі інформації про особу злочинця та вивченню цифрових слідів. Зокрема, останнім часом набув популярності метод моніторингу у режимі реального часу оновлень на особистих сторінках у мережах Facebook, Instagram та інших соціальних мережах.

Усі методи та перелік інструментів, у даній роботі не є вичерпним, ми не стали розкривати у повному обсязі теми відкритих державних реєстрів, які спрощують запит інформації, можливості використання ботів та *Telegram*, WhatsApp, Viber. Також залишається відкритим питання великої кількості баз даних, які з'явились у мережі у результаті витоку інформації з державних та приватних організацій.

На нашу думку сучасні методи пошуку, збору та аналізу інформації слід постійно досліджувати, оновлювати, систематизувати та використовувати при розслідувані злочинів. Також необхідно розробка законодавства для легалізації цих методів у кримінальному процесі та оперативно-розшуковій діяльності. Крім того необхідно вивчати данні методи в рамках криміналістики та на курсах перепідготовки та підвищення кваліфікації співробітників правоохоронних органів. Або навіть організовувати підрозділи спеціалістів, які будуть допомагати слідчим та суддям отримувати та легалізувати інформацію у процесі.

Без вивчення та дослідження даної проблеми, та без імплементації відповідних змін в кримінальний процес, система правосуддя загальмує, з впровадженням сучасних цифрових доказів, а практикуючі криміналісти не матимуть повноцінний інструмент виявлення, попередження та розкриття злочинів.

Література:

1. Как найти информацию о человеке: Гид по OSINT-инструментам. URL:https://factcheck.kz/metodika-fch/kak-najti-informaciyu-o-cheloveke-gid-po-osint-instrumentam/.
2. Инструмент анализа данных и OSINT для всех.URL: https://lampyre.io/
3. Находите, интерпретируйте и сообщайте значимые закономерности и идеи на основе данных. URL: https://www.ibm.com/ru-ru/products/i2-analysts-notebookм
4. Чорний" ринок даних і розвідка для чайників. URL: https://www.epravda.com.ua/columns/2020/12/30/669656/
5. OSINT Framework. URL: https://osintframework.com/
6. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text
7. Щербань В.Д. Адміністративно-правові методи функціонування OSINT у сфері антикорупційної діяльності правоохоронних органів. URL: https://soclaw.com.ua/index.php/journal/article/view/301
8. Албул С.В. Реалізація розвідувальної функції у діяльності поліцейських органів зарубіжних країн: компаративний аналіз. Вісник Харківського національного університету внутрішніх справ. 2015. № 4 (71)
9. CYBER INTELLIGENCE by Europol. URL: https://www.europol.europa.eu/activities-services/services-support/intelligence-analysis/cyber-intelligence
10. Про доступ до публічної інформації: Закон України від 13.01.2011 Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text
11. Про захист персональних даних: Закон України від 01.06.2010 Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
12. Щербань В.Д. Система гарантій функціонування OSINT у сфері антикорупційної діяльності в правоохоронних органах. URL: https://chasprava.com.ua/index.php/journal/article/download/127/115/
13. Ланде Д.В. Правові питання конкурентної розвідки. URL: http://ippi.org.ua/sites/default/files/7_16.pdf
14. Аброськін В. В. «Open Source Intelligence» як складова кіберрозвідки в протидії кримінальним правопорушенням. URL: http://elar.naiau.kiev.ua/bitstream/123456789/18860/1/%D0%92%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B4%D0%BE%D1%81%D1%8F%D0%B3%D0%BD%D0%B5%D0%BD%D1%8C%20%2025.02.2021_p018-022.pdf