концептуальну основу сучасних колективних OSINT-досліджень та мережевої безпекової аналітики.

Список використаних джерел:

1. L. Rosenberg, G. Willcox, H. Schumann (2023). Towards Collective Superintelligence, a Pilot Study. *International Conference on Human-Centered Cognitive Systems*. URL: https: //arxiv.org/pdf/2311.00728v1

«ВИКОРИСТАННЯ OSINT У ЦИФРОВІЙ КРИМІНАЛІСТИЦІ (DIGITAL FORENSICS)»

Синюкова Анастасія
здобувачка вищої освіти Інститут права та безпеки
Одеський державний університет внутрішніх справ
Науковий керівник: ***Грезіна Олена Миколаївна***
доктор філософії в галузі права,
доцент кафедри кримінального аналізу
та інформаційних технологій
Одеський державний університет внутрішніх справ

Стрімкий розвиток інформаційних технологій та масове поширення відкритих цифрових джерел зумовили появу нового напряму у правоохоронній і слідчій діяльності — використання методів розвідки на основі відкритих джерел (OSINT, Open Source Intelligence) у цифровій криміналістиці [1]. OSINT охоплює збір, аналіз та верифікацію даних із загальнодоступних ресурсів: соціальних мереж, публічних реєстрів, геопросторових сервісів, новинних порталів та інших відкритих платформ. Інтеграція цього підходу в цифрову криміналістику дозволяє значно розширити доказову базу, встановлювати особи підозрюваних і відновлювати хронологію подій — навіть у випадках, коли традиційні слідчі методи виявляються недостатніми [2].

Цифрова криміналістика (digital forensics) — це галузь судової науки, що займається виявленням, збором, аналізом та документуванням цифрових доказів для цілей кримінального або цивільного судочинства [6]. Традиційно вона спирається на вилучення даних із комп'ютерів, мобільних пристроїв, хмарних сховищ та

мереж. OSINT доповнює ці методи, надаючи слідчим змогу досліджувати цифровий слід фігурантів справ у відкритому інформаційному просторі [2].

Ключова відмінність OSINT від класичних криміналістичних методів полягає в тому, що дані збираються без прямого доступу до пристроїв підозрюваних і без необхідності отримувати судові ордери на кожне джерело [4]. Це робить OSINT особливо цінним на початкових етапах розслідування — для формування гіпотез, побудови мереж зв'язків та визначення пріоритетних напрямів подальшої роботи [1].

Серед найбільш поширених методів OSINT у цифровій криміналістиці виокремлюють такі напрями[1;2]:

Аналіз соціальних мереж, а саме Facebook, Instagram, Telegram, X (Twitter) та LinkedIn, містять колосальні масиви інформації про осіб: фотографії, геомітки, коло спілкування, хронологію активності. Інструменти на зразок Maltego, Sherlock, SpiderFoot дозволяють автоматизувати збір і систематизацію таких даних [1].

Використання Google Maps та супутникових знімків (Sentinel Hub, Planet Labs) допомагає верифікувати місця подій, відстежувати переміщення підозрюваних і реконструювати обстановку [5].

Цифрові файли (фотографії, документи, відео) можуть містити приховані метадані — EXIF-інформацію з координатами, часом зйомки, моделлю пристрою. Утиліти ExifTool і Jeffrey's Exif Viewer широко застосовуються для їх вилучення [6].

OSINT-фахівці використовують спеціалізовані пошукові системи (Ahmia, OnionSearch) та моніторингові платформи для відстеження активності злочинних угруповань у прихованих сегментах мережі [7].

Сервіси Shodan, WHOIS, VirusTotal, Censys допомагають встановлювати власників веб-ресурсів, виявляти фішингові сайти та відстежувати інфраструктуру кіберзлочинців [3].

На практиці OSINT успішно застосовується в розслідуванні кіберзлочинів, тероризму, торгівлі людьми, шахрайства та корупції [5]. Показовим прикладом є діяльність міжнародної групи Bellingcat, яка за допомогою виключно відкритих джерел встановила осіб причетних до катастрофи MH17 та задокументувала численні воєнні злочини. Правоохоронні органи США, Євросоюзу

та України все активніше впроваджують OSINT-методики у стандартні процедури розслідування [3;4].

Разом із тим, використання OSINT у криміналістиці стикається з низкою суттєвих викликів. По-перше, постає питання допустимості доказів: суди різних юрисдикцій мають відмінні стандарти щодо прийнятності даних, зібраних із відкритих джерел, а неправильне документування процесу збору може знецінити докази [4]. По-друге, зростання алгоритмів дезінформації та deepfake-контенту вимагає обов'язкової верифікації знайдених матеріалів [7]. По-третє, виникають етико-правові колізії між ефективністю розслідування та захистом приватності осіб, які потрапляють у поле зору слідчих [2].

OSINT став невід'ємним компонентом сучасної цифрової криміналістики, що суттєво розширює можливості слідчих у роботі з відкритим інформаційним простором [1;2]. Ефективне поєднання традиційних криміналістичних методів та OSINT-інструментів дозволяє вирішувати складні справи, які раніше залишались нерозкритими [5;6]. Водночас розвиток галузі потребує розробки єдиних стандартів збору та верифікації даних, навчання фахівців і формування відповідної нормативно-правової бази, здатної збалансувати інтереси правосуддя та захист прав людини [4;7].

Список використаних джерел:

1. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. — Одеса : Юридика, 2024. — 180 с. URL: https://doi.org/10.32837/11300.27740.

2. Пашковський М. І. Цифрова інформація з відкритих джерел. Відкриті цифрові дані у кримінальному провадженні. Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н. В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. — Харків, 2024. — С. 233–274. DOI: https://doi.org/10.31359/9786178612139.

3. Василенко В. М. Цифрова трансформація правоохоронних органів: ризики в умовах гібридних загроз та шляхи їх подолання. Вісник Кримінологічної асоціації України. 2024. Т. 32, № 2. С. 945–958. URL: https://doi.org/10.32631/vca.2024.2.74.

4. Шехавцов Р. М. Правове регулювання використання OSINT та його результатів під час встановлення обставин кримінальних правопорушень. Науковий вісник Львівського державного

університету внутрішніх справ. Серія юридична. 2025. URL: https://journals.lvduvs.lviv.ua/index.php/law/article/view/1013.

5. Тітко І. А. Використання методик OSINT у межах розслідування кримінальних правопорушень: успішні кейси у практиці іноземних правоохоронних органів та інститутів громадянського суспільства. Аналітично-порівняльне правознавство. 2026. URL: https://journal-app.uzhnu.edu.ua/article/view/358390.

6. Криміналістика і судова експертиза : міжвідом. наук.-метод. зб. / КНДІ судових експертиз ; редкол.: О. Г. Рувін та ін. — Київ : Ліра-К, 2023.

7. Використання OSINT у кримінальному провадженні: правові засади та проблеми захисту персональних даних. Юридичний науковий електронний журнал. 2024. № 11. С. 108. URL: https://www.lsej.org.ua/11_2024/108.pdf

ІНСТРУМЕНТИ, МЕТОДИ ТА АЛГОРИТМИ ЗАСТОСУВАННЯ OSINT У АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ

Щурат Тарас Григорович
доцент кафедри оперативно-розшукової діяльності навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС, кандидат юридичних наук, доцент
Тритяк Марія Володимирівна
курсант 201 взводу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС

Оперативно-розшукова діяльність (ОРД) є одним із ключових напрямів діяльності правоохоронних органів, що забезпечує отримання, аналіз та використання інформації з метою протидії злочинності. В умовах цифровізації суспільства та зростання ролі інформаційного середовища особливого значення набуває аналітична складова ОРД, яка базується на обробці великих масивів даних. Одним із сучасних інструментів такої діяльності є OSINT (Open Source Intelligence) — розвідка з відкритих джерел [1].