структура кожного з них відповідає класичним уявленням про зміст організації ОРД. Враховуючи зазначене, з усіх можливих елементів організації діяльності, обираємо ті, що мають ключове значення саме для організації процесу забезпечення спеціального досудового розслідування.

Список використаних джерел

1. Кримінальний процесуальний кодекс України: Закон від 13.04.2012 р. URL: http://zakon3.rada.gov.ua/laws/show/4651-17.

2. Войтович Є. М., Тичина Д. М., Антощук А. О. Основи методики розслідування насильницького зникнення людини : монографія. Київ : 7БЦ, 2022. 176 с.

3. Про оперативно-розшукову діяльність: Закон України № 2135-XI від 18 лют. 1993 р. URL: http://zakon2.rada.gov.ua/laws/show/2135-12/ed20160301.

4. Єрошкін М. В. Особливості доказування у кримінальних провадженнях про насильницьке зникнення: дис…канд. юрид. наук: 12.00.09. Маріуполь, 2021. 238 с.

Оперук Віталій Ігорович,
професор кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук, доцент

МОЖЛИВОСТІ ВИКОРИСТАННЯ OSINT-РОЗВІДКИ З МЕТОЮ ВИЯВЛЕННЯ ОСІБ, ЯКІ ПЕРЕХОВУЮТЬСЯ ВІД ОРГАНІВ ДОСУДОВОГО РОЗСЛІДУВАННЯ

Інформація у XXI столітті виступає найбільш ціннім ресурсом з усіх наявних. Використовуючись в економіці, політиці, військовій та правоохоронній сфері, вона є важливим чинником для прийняття стратегічних та тактичних рішень.

Розслідування злочинів в інформаційну епоху потребує застосування широкого спектра інструментів, включно з розвідкою з відкритих джерел (OSINT). Використання даних із відкритих джерел як доказів у кримінальних провадженнях є однією з найбільш затребуваних навичок українських прокурорів і слідчих, які розслідують злочини загалом та злочини пов'язані з російською агресією зокрема. У контексті війни цінність розвідувальних даних із відкритих джерел значно зростає зокрема й через відсутність фізичного доступу до місць злочину чи доказів [1].

Супутникові знімки, дрони, безпілотники, найрізноманітніше програмне забезпечення, OSINT – і це далеко не весь перелік технологій, які можуть застосовуватись правоохоронними органами з метою виявлення осіб причетних до скоєних злочинів.

Розвідка з відкритих джерел або OSINT – це пошук та використання інформації, відкритих реєстрів, сайтів та статистичних даних. Людину, яка збирає й аналізує цю інформацію, називають OSINT-спеціалістом або «осінтером». Особливість OSINT полягає у тому, що цей метод розвідки дозволяє отримувати інформацію з відкритих джерел, не вдаючись до незаконних дій. Адже інформація, з якою працює OSINT-спеціаліст – відкрита. Тобто, це збільшує можливості правоохоронців щодо пошуку інформації відносно осіб, які становлять інтерес для оперативних працівників та органів досудового розслідування.

Інтернет – ресурси містять велику кількість різного виду інформації, де у популярних соціальних мережах («Інстаграм», «Фейсбук», «Вконтакті», «Однокласники» та інших) практично завжди наявна інформація про фізичну особу. Це пов'язано з тим, що громадяни за власною ініціативою та виключно на добровільній основі розміщують свої персональні дані (ПІБ, дату народження, місце проживання, коло спілкування, інтереси, особисті побутові фотознімки та відеозаписи), створюючи тим самим потужний інформативний масив цифрових даних, що містять антропометричні ознаки зовнішності людини, анкетні дані, зображення місць фактичного проживання тощо.

Наявність такої інформації (саме у відкритому доступі) надає можливість правоохоронним органам безперешкодно використовувати останню в оперативних цілях, оскільки результати її аналізу дають змогу отримувати орієнтуючу інформацію, а інколи й відразу ідентифікувати особу [2, с. 144–145].

За таких підстав особливий інтерес для правоохоронців становить технологія автоматичної ідентифікації особи за елементами зовнішності за її відображенням на фотографії або відеозаписі, яка має широке комерційне та наукове застосування. Дана технологія цікава тому, що може здійснюватися без контакту з об'єктом пошуку.

За результатами пошуку сервіси надають користувачу масив, що складається з переліку максимально схожих осіб, із відсотковим зазначенням збігу зовнішності обличчя знайденої особи з досліджуваною. Тобто отримані результати не містять інформацію про індивідуально-конкретну тотожність осіб, оскільки до такого висновку можна дійти або шляхом суб'єктивної оцінки співпадаючих ознак зовнішності людини, або використовуючи спеціальні методи портретної експертизи. При цьому важливо розуміти, що візуальне сприйняття ознак зовнішності особами, які не є спеціалістами в галузі судово-портретної експертизи, ґрунтується лише на підставі суб'єктивної оцінки окремих ознак та внутрішнього переконання. І навпаки, спеціалісти оцінюють збіг зовнішності порівнюваних осіб, застосовуючи науково-обґрунтовані спеціальні методи портретної

експертизи, що дає змогу об'єктивно проаналізувати результати пошуку [2, с. 146].

У всесвітній мережі є онлайн-сервіси існує безліч інструментів, які використовують «осінтери» у своїй роботі:

1. Інструменти для пошуку людей:

– X-Ray.contact – сервіс, що дозволяє знаходити людину за фото, електронною адресою, телефоном чи іменем, звичайні користувачі можуть знайти загублених друзів, або перевірити нового знайомого з додатків для знайомств;

– Pipl – платформа, яка пропонує розширений пошук людей в інтернеті. Може шукати інформацію, базуючись на великій кількості джерел відкритої інформації;

– Spokeo – збирає інформацію з різних відкритих джерел;

– PeekYou – знаходить профілі користувачів у соціальних мережах та інших веб-сайтах.

2. Веб-скрапери (програми, які автоматично збирають інформацію з вебсайтів):

– Scrapy – потужний і гнучкий інструмент для витягування даних;

– BeautifulSoup — бібліотека для аналізу HTML і XML документів;

– Octoparse: інструмент для автоматизованого збору великих обсягів даних з веб-сайтів [2].

Вищезазначені інструменти не є вичерпними, так як інформаційні ресурси, що використовуються з метою пошуку інформації з відкритих джерел постійно вдосконалюються та з'являються нові.

Отже, використання відкритих даних та методів OSINT-розслідування в роботі правоохоронних органів з пошуку осіб які переховуються від органів досудового розслідування є дієвим інструментом з пошуку підозрюваних, обвинувачених, оскільки значно прискорює виявлення та розшук таких осіб.

Таким чином, використання технології OSINT для збору, узагальнення та аналізу інформації на основі відкритих джерел інформації має великий потенціал у правоохоронній сфері. Неперервний розвиток цієї технології та її поєднання з іншими інноваційними підходами відкривають шлях до нових можливостей і досягнень у майбутньому.

Список використаних джерел

1. Українські слідчі та прокурори покращили свої навички розвідки з відкритих джерел (OSINT). URL: https://www.coe.int/uk/web/kyiv/-/ukrainian-investigators-and-prosecutors-strengthened-their-osint-skills.

2. Одерій О.В., Кожевніков О.А. Отримання криміналістично-значущої інформації шляхом аналізу відкритих Інтернет-джерел. Правовий часопис Донбасу № 4 (73) 2020. С. 144–155.

3. Онлайн-безпека: як використати OSINT на користь України URL: https://itarena.ua/ua/onlajn-bezpeka-yak-vykorystaty-osint-na-korysty-ukrayini/.

Павленко Сергій Олексійович,
провідний науковий співробітник відділу організації та захисту прав інтелектуальної власності Національної академії внутрішніх справ, доктор юридичних наук, доцент

СПОСОБИ ПСИХОЛОГІЧНОГО ВПЛИВУ ДОВЕДЕННЯ ДО САМОГУБСТВА НЕПОВНОЛІТНІХ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

Аналіз наукової літератури [1, с. 456; 2; 3] свідчить про те, що злочинці, які вчиняють злочини у сфері інформаційно-телекомунікаційних технологій, зазвичай, є членами добре організованих, мобільних і технічно оснащених висококласним обладнанням і спеціальною технікою (нерідко оперативно-технічного характеру) злочинних груп і співтовариств. Осіб, які входять до їх складу, загалом можна характеризувати як висококваліфікованих спеціалістів із вищою юридичною, економічною (фінансовою) і технічною освітою. Злочини носять багатоепізодний характер, обов'язково супроводжуються діями, спрямованими на приховання злочинів.

Крім того, учасники організованих злочинних об'єднань, діяльність яких спрямована на доведення неповнолітніх до самогубства через мережу Інтернет, мають високий рівень знань у галузі психології та інших наук [1, с. 456].

Зокрема, результати психологічних досліджень доводять, що маніпулювання свідомістю дитини через соціальні мережі здійснюється шляхом психологічного впливу, з використанням нейролінгвістичного програмування.

Варто зауважити, що суб'єктом нейролінгвістичного впливу є спеціаліст (інструктор). Таким спеціалістом у групах, що пропагують суїцид у соціальних мережах, є куратор, який веде онлайн-листування індивідуально з кожним учасником «групи смерті» та дає їм завдання, що у підсумку призводять до самогубства [1, с. 457; 2].

Вивчення зазначеної проблематики дало змогу виокремити способи психологічного впливу, які організатори «груп смерті»