DOI https://doi.org/10.36059/978-966-397-490-3-16

ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ ТА ВІДКРИТИХ ДЖЕРЕЛ У ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ: МОЖЛИВОСТІ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Калюга К. В.
доктор юридичних наук, професор,
заступник завідувача кафедри кримінального права, процесу
та криміналістики
Інституту економіки та права
Класичний приватний університету
м. Запоріжжя, Україна

Сучасний інформаційний простір значно впливає на методи та підходи до оперативно-розшукової діяльності (ОРД) [1]. Соціальні мережі, форуми, відкриті бази даних, державні дані: відкриті звіти, декларації, пресконференції тощо, всі види ЗМІ, академічні публікації, професійні роботи, «сіра» література: патенти, технічні звіти, спостереження: радіо, аерофотозйомки, комерційні дані: зображення, фінансові та промислові оцінки, бази даних і різноманітні онлайн-ресурси стали важливим інструментом для правоохоронних органів у процесі виявлення, профілактики та розслідування правопорушень. Використання інформації з відкритих джерел (OSINT – Open Source Intelligence) [3-5] дозволяє отримувати важливі відомості про підозрюваних осіб, їх зв'язки, місця перебування та інші аспекти, що можуть допомогти в слідчих діях. Водночас, ефективність такого підходу залежить від низки викликів, серед яких точність отриманих даних, правові аспекти використання та питання конфіденційності.

Соціальні мережі є багатим джерелом інформації для оперативно-розшукових заходів. Вони дозволяють отримувати значний обсяг даних. Ідентифікація осіб – користувачі залишають особисті дані, світлини, відео, інформацію про місце проживання, роботи та навчання, хобі та інтереси тощо. Які можуть свідчити, наприклад, про наявність у них певних компетентностей (знань, умінь та особистих якостей, досвіду, навичок), що у тому числі дає нам уяву про здатність особи виконувати певну діяльність або приймати рішення у конкретній сфері. Що дозволяє оперативним працівникам швидко визначати особу підозрюваного або свідка, аналізувати його профіль та складати попередній «криміналістичний портрет» [2]. Визначення зв'язків – аналіз друзів, підписників та взаємодій допомагає виявити коло спілкування підозрюваних. Використовуючи

інструменти соціального графу (різноманітних соціальних зв'язків), можна виявити неочевидні зв'язки між особами, що може бути корисним при розслідуванні злочинних угруповань або змові. Геолокація – деякі сервіси (наприклад, Instagram, Facebook, Twitter) містять дані про географічне розташування, що допомагає відстежувати переміщення осіб. Наприклад, фотографії з геотегами можуть підтвердити присутність підозрюваного в певному місці під час вчинення правопорушення. Моніторинг діяльності – аналіз постів, коментарів, лайків дозволяє отримати інформацію про плани, наміри та звички підозрюваних. Наприклад, екстремістські або агресивні висловлювання, участь у сумнівних групах можуть свідчити про можливу причетність до злочинної діяльності.

Виявлення ознак злочинної діяльності (в умовах неочевидності, коли користувачі намагаються приховати свої наміри) – спостереження за контентом, що поширюється в соціальних мережах, може свідчити про можливі правопорушення. Наприклад, торгівля забороненими речовинами, незаконний продаж зброї, вербування у злочинні угруповання або розповсюдження фейкових новин з метою дестабілізації ситуації. Також, можуть мати значення: незвичайна активність, закриті або приватні профілі (чи пропозиції перейти у такі профілі), використання кодових слів або символів, часті зміни імені користувача або профільної інформації, публікації з геолокаціями зони підвищеного ризику, підозрілі зв'язки, обмін зашифрованими або самознищуваними повідомленнями, публікації, що демонструють розкішний спосіб життя без видимих джерел доходу, поширення контенту, пов'язаного з незаконними темами, використання VPN або інших засобів для приховування місцезнаходження, публікація екстремістського контенту, поширення дезінформації, пропозиція підозрілих послуг або товарів, використання фейкових профілів, публікація компроментуючого контенту про інших, порушення авторських прав, незаконний збір та обробка персональних даних, використання декількох облікових записів, надмірна увага до конфіденційності (особливо постійне видалення контенту), публікації з обмеженим доступом, незвичайні або спеціалізовані групи та спільноти, часті зміни місцезнаходження (без видимих причин), використання рідкісних або спеціалізованих платформ (перехід на менш відомі або спеціалізовані соціальні мережі та платформи), незвичайні патерни взаємодії (наприклад, отримання великої кількості лайків або коментарів від облікових записів з низькою активністю або нещодавно створених профілів), публікації з обмеженим часом доступу, використання специфічних додатків або сервісів (призначених для приховування активності, з високим рівнем шифрування), незвичайні або надмірні запити до інших користувачів, незвичайні фінансові транзакції, поширення шкідливих посилань або файлів, використання спеціалізованих жаргонів або сленгу (використання мови, яка характерна для певних

підпільних спільнот або незаконних діяльностей), публікації контенту з геолокаціями, що не відповідають реальному місцезнаходженню, використання незвичайних методів оплати тощо.

Важливо зазначити, що наявність одного або декількох з цих показників не обов'язково свідчить про незаконну діяльність. Однак, їх сукупність або поєднання з іншими факторами можуть бути підставою для більш детального аналізу або спостереження.

Сучасний інформаційний простір значно впливає на методи та підходи до оперативно-розшукової діяльності (ОРД). Соціальні мережі, форуми, відкриті бази даних і різноманітні онлайн-ресурси стали важливим інструментом для правоохоронних органів у процесі виявлення, профілактики та розслідування правопорушень. Використання інформації з відкритих джерел (OSINT – Open Source Intelligence) дозволяє отримувати важливі відомості про підозрюваних осіб, їх зв'язки, місця перебування та інші аспекти, що можуть допомогти в слідчих діях. Водночас, ефективність такого підходу залежить від низки викликів, серед яких точність отриманих даних, правові аспекти використання та питання конфіденційності.

Замість висновків. Використання соціальних мереж та відкритих джерел у оперативно-розшуковій діяльності є потужним інструментом, що значно розширює можливості правоохоронних органів. Однак, ефективність цього підходу залежить від вирішення низки викликів, зокрема правових, етичних та технічних аспектів. Подальший розвиток технологій OSINT, інтеграція штучного інтелекту та міжнародна співпраця сприятимуть вдосконаленню методів протидії злочинності в цифрову добу.

Література:

1. Закон України «Про оперативно-розшукову діяльність» від 18 лютого 1992 р. № 2135-XII. *Відомості Верховної Ради України.* 1992. № 22. Ст. 303.

2. Калюга К. В. Мистецтво здобувати та використовувати інформацію щодо особи злочинця : монографія. Харків : Право, 2019. 256 с.

3. Матвієнко О. OSINT для журналістів: із чого почати та чим користуватися. *Накіпіло освіта.* URL: https://osvita.nakypilo.ua/osint-dlya-zhurnalistiv-iz-chogo-pochaty-ta-chym-korystuvatysya/?gad_source=1&gclid=CjwKCAiAh6y9BhBREiwApBLHC79o1Cci9EW-p3Pxxp49LGC9Tsja1NjzOIFWmRozckuYtivVHQbx9hoCSjQQAvD_BwE

4. Розвідка з відкритих джерел (Open-source intelligence – OSINT). URL: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/

5. Розвідка на основі відкритих джерел. *Вікіпедія. Вільна енциклопедія.* URL: https://uk.wikipedia.org/wiki/Розвідка_на_основі_відкритих_джерел