

НАКОПИЧЕННЯ Й АНАЛІЗ ОПЕРАТИВНО-РОЗШУКОВОЇ ІНФОРМАЦІЇ З КОМП'ЮТЕРНИХ МЕРЕЖ

ACCUMULATION AND ANALYSIS OF OPERATIVE AND SEARCH INFORMATION FROM COMPUTER NETWORKS

Перепелиця М.М.,

кандидат юридичних наук, доцент,

професор кафедри оперативно-розшукової діяльності

Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної міліції

Харківського національного університету внутрішніх справ

Плукар В.В.,

кандидат юридичних наук, доцент кафедри кримінально-правових дисциплін

Львівського державного університету внутрішніх справ

У статті проаналізовано становлення системи інформаційно-аналітичного забезпечення оперативно-розшукової діяльності. Сформульовано окремі проблемні питання, які виникають у цій сфері. Наголошується, що сучасна система інформаційно-аналітичного забезпечення оперативно-розшукової діяльності потребує впровадження нової концепції розвитку з інтегруванням кращих зарубіжних і вітчизняних практик. Підкреслено важливість накопичення й аналізу для потреб оперативно-розшукової діяльності відкритої інформації з локальних і глобальних комп'ютерних мереж. Розглянуто окремі особливості такого збирання. Запропоновано додаткові джерела пошуку оперативно-розшукової інформації та шляхи вдосконалення інформаційно-аналітичного забезпечення оперативно-розшукової діяльності в Україні.

Ключові слова: комп'ютерна мережа, оперативно-розшукова інформація, оперативно-розшукова діяльність, інформаційно-аналітичне забезпечення, соціальні мережі.

В статье проанализировано становление системы информационно-аналитического обеспечения оперативно-розыскной деятельности. Сформулированы отдельные проблемные вопросы, которые возникают в этой сфере. Отмечается, что современная система информационно-аналитического обеспечения оперативно-розыскной деятельности нуждается во внедрении новой концепции развития с интегрированием лучших зарубежных и отечественных практик. Подчеркивается важность накопления и анализа для потребностей оперативно-розыскной деятельности открытой информации из локальных и глобальных компьютерных сетей. Рассмотрены отдельные особенности такого сбора. Предложены дополнительные источники поиска оперативно-розыскной информации и пути совершенствования информационно-аналитического обеспечения оперативно-розыскной деятельности в Украине.

Ключевые слова: компьютерная сеть, оперативно-розыскная информация, оперативно-розыскная деятельность, информационно-аналитическое обеспечение, социальные сети.

Formation of the system of the information analysis maintenance of special investigation activity is analysed in the article. Separate problem questions which arise up in this sphere are formulated. It is marked that the modern system of the information analysis maintenance of special investigation activity needs introduction of new conception of development with integration of the best foreign and domestic practices. Importance of accumulation and analysis for the necessities of special investigation activity of the opened information is underlined from local and global computer networks. The separate features of such collection are considered. The additional sources of special investigative information and ways of improvement of the information analysis maintenance of special investigation activity are offered in Ukraine.

Key words: computer network special investigative information, special investigation activity, information analysis maintenance, social networks.

Актуальність теми. Використання нових технологій в оперативно-розшуковій діяльності на сьогодні є запорукою успішності її здійснення. Викриття Е. Сноудена продемонстрували, що застосування нових технологій у негласній роботі правоохоронних органів і спецслужб дають змогу реалізувати концепцію випереджального впливу на негативні події. Велику роль при цьому відіграють вчасне, кваліфіковане опрацювання та систематизація одержаної оперативно-розшукової інформації. До того ж значно актуалізувалося питання накопичення й обробки такої інформації з відкритих джерел, зокрема комп'ютерних мереж, що в завершеному вигляді надає неоціненну

допомогу правоохоронним органам під час виявлення, запобігання й розслідування злочинів.

Варто зазначити, що для оперативних підрозділів органів внутрішніх справ повноцінний інформаційний обіг у формі збирання, одержання, аналізу та використання отриманої інформації є першочерговим завданням і зумовлює саму наявність основної діяльності щодо боротьби зі злочинністю [1, с. 124]. При цьому забезпечувальний персонал, який провадить таку діяльність, відіграє значну роль у потужних правоохоронних органах світу. Наприклад, у структурі ФБР США станом на 31 жовтня 2014 року налічувалося 35 104 працівники, із яких 13 260

спеціальних агентів і 18 306 осіб забезпечувально-го персоналу (аналітиків розвідувальної інформації, лінгвістів, учених, фахівців у сфері інформаційних технологій тощо) [2].

З наведеного випливає, що дослідження проблемних питань застосування інформаційно-аналітичного забезпечення боротьби зі злочинністю як у світі, так і в Україні є достатньо актуальним завданням. Одним із відповідних проблемних питань, яке потребує наукового вивчення, є організація накопичення й аналізу інформації з комп'ютерних мереж для потреб оперативно-розшукової діяльності.

Дослідженням питань інформаційно-аналітичного забезпечення оперативно-розшукової діяльності займалися низка зарубіжних і вітчизняних фахівців. Серед них заслуговують на увагу роботи О.М. Бандурки, В.Д. Гавловського, В.Ю. Журавльова, В.П. Захарова, І.П. Козаченка, М.Ю. Літвінова, В.А. Лукашова, О.В. Манжая, А.В. Мовчана, А.С. Овчинського, В.С. Овчинського, С.С. Овчинського, А.М. Ташмагамбетова, О.Б. Фаріон, В.В. Шендрика та багатьох інших авторів.

Мета статті полягає у визначенні проблемних питань інформаційного забезпечення оперативно-розшукової діяльності, шляхів їх вирішення, а також організаційних особливостей накопичення й аналізу оперативно-розшукової інформації з комп'ютерних мереж.

Вклад основного матеріалу. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності пройшло досить тривалий шлях до свого сучасного вигляду. Як відзначає А.В. Мовчан, за останні два десятиріччя було створено обліки міжвідомчого характеру, розвинуто міждержавні обліки, активізувалося використання інтегрованих банків Інтерполу; відбувся розвиток технологій аналітичної та комп'ютерної розвідки; упроваджено в оперативну практику мультимедійні технології; розроблено технології здійснення інформаційно-аналітичної роботи в транспортних телекомунікаційних мережах та електронних інформаційних мережах [3, с. 237]. Водночас означені напрями потребують постійної модернізації й покращення, що в умовах обмежених ресурсів і політичних катаклізмів стає вкрай проблематичним.

Українська правоохоронна практика свідчить, що на сьогодні інформаційно-аналітична робота у сфері оперативно-розшукової діяльності перебуває не на належному рівні. Багато в чому це зумовлено недостатнім фінансуванням і матеріально-технічним забезпеченням. Розвинуті країни заходу пішли далеко вперед у цьому сенсі. Існують проблеми й іншого плану. Так, на сьогодні значна частина діяльності інформаційно-аналітичних підрозділів органів внутрішніх справ України зосереджена на накопиченні та аналізі статистичних даних. Така стратегія видається не зовсім правильною, адже, як зауважує А.П. Злочевський, оцінювання криміногенної обстановки не має ґрунтуватися тільки на статистичних даних (без урахування взаємозалежності цифрових показників, факторів зовнішнього середовища й

функціонування оперативних підрозділів), оскільки не в повному обсязі відображає її реальний стан. При цьому брак оперативно-розшукової інформації, як і її надлишок, однаково шкідливі [4, с. 117].

Загальним недоліком інформаційних систем правоохоронних структур є вузьковідомчий характер накопичення й отримання інформації, відсутність можливості одержання та об'єднання в короткі терміни інформації з різних відомчих джерел, неможливість у більшості випадків її комплексного отримання в режимі он-лайн з інформаційних баз даних різних державних і недержавних структур [5, с. 128].

Одним із проблемних питань залишається створення єдиної інформаційно-пошукової системи правоохоронних органів. При цьому, як слушно відзначає А.Ю. Кійко, без вирішення проблеми інтеграції оперативно-розшукової інформації неможливе якісне поліпшення аналітичної роботи. Під приводом можливого несанкціонованого доступу та використання негласної інформації штучно стримуються процеси її автоматизованої обробки [6, с. 7].

Усе це дає підстави вважати, що сучасна система інформаційно-аналітичного забезпечення оперативно-розшукової діяльності потребує впровадження нової концепції розвитку з інтегруванням кращих зарубіжних та вітчизняних практик. Одним із напрямів удосконалення інформаційно-аналітичного забезпечення оперативно-розшукової діяльності є формування оперативно-розшукової інформації за результатами обробки даних із комп'ютерних мереж.

Такі дані можна умовно поділити на два види: з локальних і глобальних мереж. Як приклад першого виду можна навести різного штибу дані, які циркулюють у міських мережах, організованих провайдерами. Нерідко в таких мережах можна знайти інформацію, яка містить ознаки вчинення кримінальних правопорушень (дитячу порнографію, контрафактне програмне забезпечення, бази персональних даних, документи обмеженого доступу тощо). Другий вид інформації, найбільший за обсягом, – це дані з мережі Інтернет. Це різного штибу стрічки новин, форуми, спеціалізовані сайти й сервіси тощо. Особливу категорію становлять дані соціальних мереж.

Важливість аналітичної обробки соціальних мереж зумовлена значним оперативно-розшуковим інформаційним ресурсом, який у них міститься. Як відзначає з цього приводу А.О. Сукманов, нерідко ці Інтернет-ресурси використовуються зловмисниками для здійснення протиправних діянь, тим самим залишаючи в мережі різного штибу сліди й докази своєї винності; більшість «соціальних мереж» – це, по своїй суті, унікальні бази даних, у яких можна знайти інформацію, яка становить оперативний інтерес; це унікальний засіб інформування населення та одержання важливих відомостей [7, с. 18].

Останнім часом в Україні почастишали випадки застосування соціальних мереж екстремістами, зокрема їх використовували для організації та координації сепаратистських виступів на сході й півдні України. Тому увага до них правоохоронних органів є виправданою.

Незважаючи на значний обсяг відкритої інформації в мережах, її накопичення та обробка з оперативного-розшуковою метою супроводжується певними складнощами.

По-перше, здійснюючи оперативно-розшукові заходи в мережі, оперативний працівник ризикує перейти межі конституційних прав громадян, що охороняються [8, с. 68].

По-друге, збирання інформації, доступної через відкриті джерела, може класифікуватися як посягання на недоторканність приватного життя. Зокрема, Європейським судом з прав людини у справі «Шведія проти Сегерстед Віберг» (*Segerstedt-Wiberg v. Sweden* [9]) дії поліції зі збирання інформації, яка є відкритою для користувачів мережі Інтернет, кваліфіковано як порушення права на недоторканність приватного життя, гарантоване ст. 8 Конвенції Ради Європи «Про захист прав людини і основоположних свобод» від 04.11.1950 р. (ратифікована Верховною Радою України 17.07.1997 р.). Систематичне збирання інформації розцінюється як втручання у приватне життя у зв'язку з тим, що особа, яка розміщує інформацію, розраховує на зберігання відомостей і відсутність моніторингу за його профілем. Збирання відомостей є допустимим тільки згідно із Законом і з метою боротьби зі злочинністю (ст. 8 (2) Конвенції) [10, с. 131].

Враховуючи викладене, оперативні працівники в праві накопичувати безособову відкриту інформацію, а відомості щодо окремих осіб мають право збирати лише в межах заведеної оперативно-розшукової справи або відкритого кримінального провадження. У цьому випадку стає в нагоді норма Кримінального процесуального кодексу України, у якій наголошується, що здобуття відомостей з електронних інформаційних систем або їх частин, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов'язаний із подоланням системи логічного захисту, не потребує дозволу слідчого судді [11, п. 2. ст. 264].

Водночас не всяка інформація з комп'ютерних мереж є оперативно-розшуковою. З цього приводу потрібно звернутися до деяких теоретичних положень.

А.С. Овчинський, провівши ґрунтовні дослідження змісту поняття «оперативно-розшукова інформація», дійшов висновку, що оперативно-розшукова інформація – це той зміст оперативних повідомлень, ті складові відомостей із відкритих джерел, ті елементи даних електронних банків і автоматизованих систем, ті компоненти кримінологічних, психологічних, демографічних та інших знань, які, з одного боку, інтерпретовані, оброблені та проаналізовані, виходячи із завдань виявлення осіб і фактів, які становлять оперативний інтерес, їх перевірки й з'ясування обставин, а також з метою розкриття злочинів, розшуку злочинців, представлення доказів у кримінальному процесі, а з іншого боку, можуть бути використані безпосередньо для профілактики, запобігання та припинення злочинної діяльності шляхом контролю, дії й у результаті управління кримінальною ситуаці-

єю як кримінально-процесуальними заходами, так і заходами, які знаходяться поза кримінально-правовою сферою [12, с. 33].

В.О. Білецький головними вимогами до оперативного-розшукової інформації визначає точність, вірогідність, лаконічність, логічність викладу, оптимальність, повноту, комплексність, відповідність рівня надходження та використання оперативного-розшукової інформації для прийняття рішень, цінність (корисність) [13, с. 177–178].

Використання оперативної інформації як доказу може бути здійснено тільки після того, як буде встановлено джерело її походження. Без цієї умови оперативна інформація не може мати жодної доказової цінності. Якщо ж джерело оперативної інформації хоча й відоме, але засекречене, не підлягає розголошенню, одержані від нього фактичні дані також не мають доказового значення [14, с. 46].

На думку А.Б. Свістільнікова та В.І. Кулешова, система оперативного-розшукової інформації має включати відомості про таке: стан оперативної обстановки, причини й умови вчинення злочинів, а також засоби, методи та результати профілактичного впливу на злочинність; ознаки підготовлюваних і вчинених злочинів; осіб, які готують злочини, раніше засуджених, а також тих, як становлять іншу кримінальну небезпеку [15, с. 105]. Ми переконані, у цій класифікації відсутні відомості про предмети, пов'язані з учиненням злочину, а також невідомі трупні й безвісті зниклих осіб.

Характеризуючи останній вид, хотілося б відмітити, що в Харківському національному університеті внутрішніх справ існує позитивний досвід аналізу даних соціальних мереж для пошуку безвісти зниклих дітей, який проводиться у взаємодії з підрозділами кримінальної міліції у справах дітей.

Опрацьовувати накопичену оперативно-розшукову інформацію варто за спеціалізованими алгоритмами. Один із таких алгоритмів пропонує О.Б. Фаріон. Разом із тим у цьому алгоритмі інформація для аналізу надається оперативним працівником [16, с. 200]. З погляду збирання інформації з комп'ютерних мереж такий підхід видається не зовсім виправданим. Адже оперативний працівник зазвичай не може в силу своїх можливостей збирати бази даних тих самих соціальних мереж, поштових сервісів тощо. Водночас витоки інформації в мережі та використання парсерів для створення баз даних дають змогу аналітику самому збирати корисну в оперативному плані інформацію, яка у випадку надходження кримінально значимої інформації від оперативного працівника надасть можливість у комплексі побудувати відповідні зв'язки, хронологію подій тощо.

Окремі можливості для інформаційно-аналітичного забезпечення оперативного-розшукової діяльності забезпечуються через використання наявних баз даних без завантаження їх змісту. У цьому сенсі заслуговує на увагу твердження О.В. Манжая та І.А. Осятинської, що одним зі способів установлення особи за мережним ідентифікатором є використання систем відновлення паролів різних ресурсів, зокрема

так можна встановити номери телефонів, віднайти профіль особи в соціальних мережах тощо. Надалі, аналізуючи зміст і геопозначки відповідних фотографій, можна встановити місця перебування особи в певний проміжок часу. Знаючи місця пересування особи, можна у 95% випадків однозначно її ототожити, що на практиці було доведено дослідниками із Массачусетського технологічного інституту (MIT) і Католицького університету в Левені [17, с. 257].

Крім наведених методів, можна запропонувати як джерела для пошуку оперативного-розшукової інформації сервіси доступу до камер відеоспостереження (www.insecam.org), одержання інформації про мобільний телефон (www.locatio.me), сервіс пошуку вразливостей (www.shodanhq.com). Наприклад, якщо ввести в останньому пошуковому сервісі запит `DVR port:80 country:UA city:"Kharkov"`, то побачимо перелік доступних відеокamer у м. Харків.

Для опрацювання великих обсягів даних з виводування відповідних зв'язків корисно використовувати спеціалізоване програмне забезпечення. У цьому сенсі можна запропонувати, наприклад, і2 від компанії IBM.

Заслуговує на увагу створення за аналогією із реєстрацією у провідних західних країнах кримінальної інформації різнокольорових бланків-шаблонів для фіксації оперативного-розшукової інформації за різними категоріями злочинів [18, с. 117–118]. У шаблонах потрібно передбачити питання, відповіді на які дають змогу інформаційно-аналітичним підрозділам ефективно провести аналіз інформації та зробити висновки. Уведення такої новачки надасть можливість значно спростити роботу як оперативних, так і інформаційно-аналітичних підрозділів.

У результаті обробки даних інформаційно-аналітичні підрозділи мають надавати не лише довідко-

ву інформацію, а й перелік рішень, які можуть бути прийняті за результатами аналізу. Серед іншого, це можуть бути рекомендації щодо активних дій оперативних працівників у комп'ютерних мережах.

Збираючи інформацію в комп'ютерних мережах для потреб оперативного-розшукової діяльності, не можна переступати ту тонку грань, яка відділяє оперативного-розшукову діяльність від «політичного розшуку». Так, наприклад, в одній із праць російських учених чомусь розглядається невластивий для демократичного суспільства моніторинг органами внутрішніх справ сайтів регіональних відділень опозиційних громадських організацій. Автори зазначають: «Ці сайти можна щодня (або ж з іншим інтервалом) переглядати, й у разі виявлення інформації, що становить оперативний інтерес, допрацювавши її з використанням інших джерел, доповідати зацікавленому суб'єктові, у тому числі й у «ЦОРИ ГИАЦ МВД Росії». Так уже діють працівники «ЦОРИ КМ ГУВД» по Ставропольському краю і «ЦОРИ КМ ГУВД» по Санкт-Петербургу й Ленінградській області. Отримувана від них інформація становить інтерес, перевіряється, допрацьовується й доповідається керівництву МВС Росії» [19, с. 67]. Виникає питання, яке оперативного-розшукове завдання вирішується таким способом? Які підстави для здійснення оперативного-розшукової діяльності стосовно конкретного суб'єкта? Усе це дає підстави сумніватися в законності таких дій.

Висновки. Враховуючи викладені думки, хотілося коротко підвести підсумок статті. Отже, інформаційно-аналітична робота має здійснюватися законно, орієнтуватися на запобігання злочинам, характеризуватися постійним упровадженням інновацій і зміною підходів до її організації відповідно до сучасних умов розвитку суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Тямкин А.В. Особенности информационного обеспечения деятельности оперативных подразделений органов внутренних дел по налоговым преступлениям / А.В. Тямкин, Е.Н. Щеглов // Вестник Воронежского института МВД России. – 2010. – № 4. – С. 124–128.
2. Quick Facts [Електронний ресурс]. – Режим доступу : <http://www.fbi.gov/about-us/quick-facts>.
3. Мовчан А.В. Историчні аспекти становлення та розвитку інформаційно-аналітичної роботи в оперативного-розшуковій діяльності / А.В. Мовчан // Науковий вісник Національної академії внутрішніх справ. – 2013. – № 3. – С. 230–238.
4. Золочевский А.П. Аналитическая работа в оперативных подразделениях органов внутренних дел: ее роль и проблемы / А.П. Золочевский // Ученые труды Российской академии адвокатуры и нотариата. – 2014. – № 2 (33). – С. 116–118.
5. Мовчан А.В. Окремі аспекти законодавчого регулювання інформаційно-аналітичної роботи в оперативного-розшукової діяльності / А.В. Мовчан // Право і Безпека. – 2011. – № 5. – С. 125–128.
6. Кийко А.Ю. Место информационно-аналитической работы в оперативного-розыскной деятельности подразделений ФСКН России / А.Ю. Кийко // Вестник Тюменского института повышения квалификации сотрудников МВД России. – 2014. – № 1 (2). – С. 4–8.
7. Сукманов А.О. Понятие и сущность оперативно-розыскного мониторинга открытых источников информации / А.О. Сукманов // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2011. – № 1. – С. 17–19.
8. Алябьев А.А. Проблемы осуществления оперативно-розыскных мероприятий в информационном пространстве сети Интернет / А.А. Алябьев, А.В. Лагуточкин // Проблемы правоохранительной деятельности. – 2013. – № 1. – С. 66–69.
9. Case of Segerstedt-Wiberg and Others v. Sweden [Електронний ресурс]. – Режим доступу : <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591>.
10. Ташмагамбетов А.М. Оперативно-розыскные мероприятия с использованием социальных сетей: опыт Великобритании и Республики Казахстан / А.М. Ташмагамбетов // Наука и бизнес: пути развития. – 2013. – № 11 (29). – С. 129–133.
11. Кримінальний процесуальний кодекс України від 13.04.2012 р. // Голос України. – 2012. – № 90–91.
12. Овчинский А.С. Информация и оперативно-розыскная деятельность : [монография] / А.С. Овчинский ; под ред. засл. юриста РФ, доктора юридических наук, профессора В.И. Попова. – М. : ИНФРА-М, 2002. – 97 с.
13. Білецький В.О. Інформаційне забезпечення оперативно-розшукової діяльності у прикордонній сфері / В.О. Білецький // Публічне управління: теорія та практика. – 2013. – Вип. 2. – С. 176–180.

14. Фролова Е.В. Некоторые особенности информации, полученной в процессе оперативно-розыскной деятельности / Е.В. Фролова // Вестник Воронежского института МВД России. – 2008. – № 2. – С. 44–47.
15. Свистильников А.Б. Теоретические аспекты информационного обеспечения оперативно-розыскной деятельности горрайорганов внутренних дел по линии уголовного розыска / А.Б. Свистильников, В.И. Кулешов // Вестник Санкт-Петербургского университета МВД России. – 2010. – № 4. – С. 102–106.
16. Фаріон О.Б. Алгоритм опрацювання оперативно-розшукової інформації для забезпечення потреб кримінального аналізу злочинної діяльності / О.Б. Фаріон // Збірник наукових праць Національної академії Державної прикордонної служби України. Серія «Військові та технічні науки». – 2013. – № 1. – С. 194–203.
17. Манжай О.В. Встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами / О.В. Манжай, І.А. Осятинська // Актуальні питання розслідування кіберзлочинів : матеріали міжнарод. наук.-практ. конф. (Харків, 10 грудня 2013 р.) / МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2013. – С. 256–258.
18. Вязовец Р.Н. Использование информационных систем в раскрытии преступлений / Р.Н. Вязовец // Труд и социальные отношения. – 2010. – № 5. – С. 117–120.
19. Агеев В.В. К вопросу о поиске оперативно-розыскной информации в Интернете / В.В. Агеев, Е.В. Агеева // Криминологический журнал Байкальского государственного университета экономики и права. – 2011. – № 1. – С. 65–70.