УДК 343:13
DOI https://doi.org/10.32847/ln.2022.18.10

Виходець Ю.О.
доктор філософії, начальник
Департаменту кіберполіції Національної поліції України

Тетерятник Г.К.
доктор юридичних наук, професор, завідувач кафедри кримінального процесу
Одеського державного університету внутрішніх справ

ОКРЕМІ ПИТАННЯ ВИКОРИСТАННЯ OSINT ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ В УМОВАХ ВІЙСЬКОВОЇ АГРЕСІЇ РФ

З 2014 року в Україні відбувається збройний конфлікт, який з 24 лютого 2022 року набув характеру широкомасштабної військової агресії рф. Частину територій нашої держави тимчасово окуповано іще з 2014 року, на низці територій ведуться активні бойові відтак відсутня можливість проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій, отримання інформації за запитами та іншими традиційними способами. Станом на кінець листопада 2022 року за офіційною інформацією Офісу Генерального прокурора було зареєстровано за ст. 437 КК України (планування, підготовка, розв'язування та ведення агресивної війни) 66 проваджень, за ст. 438 КК України (порушення законів та звичаїв війни) – 48 839 проваджень [1].

Задля забезпечення ефективного розслідування злочинів у таких умовах важливу роль відіграє робота з інформацією з відкритих джерел. Розвиток інформаційних, комп'ютерних технологій виводить на якісно новий рівень процеси розслідування: отримання криміналістично значущої інформації, доказів. Особливе значення має відповідне фіксування такої інформації для можливості використання її не тільки як доказів у національних судах, але й у Міжнародному кримінальному суді (далі – МКС).

У дослідженнях останніх років значна увага приділяється OSINT – розвідці з відкритих джерел. Ця методика та її інструментарій зарекомендували себе і при розслідуванні воєнних злочинів, скоєних в Україні. До позитивних характеристик її використання слід віднести можливість опрацювання інформації з відкритих джерел не тільки спеціалістами у галузі комп'ютерних та інформаційних технологій, а і працівниками правоохоронних органів, які не мають спеціальних навичок, журналістами, які істотно допомагають у проведенні розслідувань, іншими громадянами; необмежений доступ до певних даних у соціальних мережах, публікаціях ЗМІ, сайтах, відкритих мессенджерах. Така інформація може відображатися у фото-, відео– файлах, геолокаціях, текстовій формі, Вчені також виділяють такі позитивні сторони: її використання не вимагає додаткових фінансових витрат на: придбання спеціальної техніки та програмного забезпечення, адже достатньо мати лише доступ до всесвітньої мережі Інтернет та робочу станцію ПК (смартфон, планшет); вона є у вільному доступі, а тому може бути використана не лише суб'єктами правоохоронної діяльності (представниками державної влади), а й приватними детективами, волонтерами та ін.; її використання (за певних умов) не порушує прав громадян [2, с. 147].

Питанню використання OSINT при розслідуванні злочинів, у т.ч. воєнних, останні роки значно актуалізувалося у різних галузях вітчизняної науки, йому присвячені роботи багатьох вчених: С. В. Албула, О. В. Дуфе-

нюк, А. О. Кисельова, О.А. Кожевнікова, О. О. Кожушко, О.В. Одерія, М. І. Пашковського та багато інших.

Метою статті є отримання наукового результату у вигляді теоретично обґрунтованих положень щодо окремих питань використання OSINT при розслідуванні злочинів в умовах збройної агресії рф.

Вчені по-різному визначають сутність OSINT. Перша група обмежує її отриманням інформації виключно з кіберпростору [3, с. 203]. Друга – більш розширено підходить до тлумачення, визначаючи, що це одна з форм процесу організації та управління збором розвідувальних даних (Intelligence Collection Management), що включає їх пошук і відбір із публічних загальнодоступних джерел, добування та аналіз інформації, формування розвідувального документу для прийняття відповідного рішення [3, с. 204; 4; 5]. Третя – пропонує «…розглядати OSINT як таку форму роботи з розвідувальними даними, що включає їх пошук і відбір з публічних загальнодоступних джерел, подальшу класифікацію та аналіз інформації, з формуванням висновків, що надаються керівництву та можуть слугувати підставою для прийняття управлінських рішень» [3, с. 204]. І з посиланням на американські джерела відзначають, що є наступні категорії відкритих джерел інформації: 1. широко розповсюджені дані та інформація; 2. цільові комерційні дані; 3. експертні оцінки; 4. «сіра» література [3, с. 204; 6].

Водночас, спеціалісти звертають увагу на те, що пошук значущої інформації в мережі Інтернет пов'язаний з необхідністю долати низку викликів, зумовлених великими обсягами даних, складною динамікою інформаційних потоків, багатократним дублюванням інформації, наявністю «шумової інформації», відсутністю індексації у пошукових системах значної кількості інформації (навіть такій потужній пошуковій системі Google за деякими розрахунками потрібно 300 років для індексації всієї інформації, обсяги якої, нагадаємо, далі зростають) [7, с. 309 – 310; 8, с. 38].

Крім того, слід звернути увагу на забезпечення гарантій щодо особистої, конфіденційної інформації, вразливість до неточностей, упереджень та хибності [9], специфічний механізм процесуалізації такої інформації, тобто подальшої можливості її використання як доказів у кримінальних провадженнях, особливо з урахуванням перспектив подальшого подання до МКС.

Актуальним є дослідження В.Д. Щербаня щодо системи гарантій функціонування OSINT. І хоча проблематика викладена у контексті антикорупційної діяльності правоохоронних органів, на наш погляд, окремі з них є й орієнтиром для використання OSINT у сфері розслідування:

– гарантія права правоохоронних органів вільно збирати, зберігати, використовувати інформацію, якщо це не порушує таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції та не полягає у збиранні, зберіганні, використанні конфіденційної інформації;

– гарантія створення механізмів для реалізації права на інформацію правоохоронними органами у процесі здійснення розвідки з відкритих джерел;

– гарантія забезпечення вільного доступу правоохоронних органів до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів та отримання необхідної інформації від усіх органів державної влади, підприємств, організацій і установ і т. ін. (прим. авторів – з урахуванням і процесуальних засобів отримання такої);

– гарантія одержання інформації від її розпорядників – передбачає визначення на нормативному рівні розпорядників передбачених законом видів інформації, яка не є конфіденційною та яка в обов'язковому порядку має надаватись правоохоронним органам, що здійснюють правоохоронну діяльність, на їх запит;

– гарантія максимального спрощення процедури отримання публічної інформації – дана

гарантія забезпечує швидкість та оперативність отримання інформації, якщо це не порушує таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції та не полягає у збиранні, зберіганні, використанні конфіденційної інформації [10, с. 139 – 140].

Як справедливо зазначають ІТ-фахівці: «OSINT не передбачає несанкціонований доступ до інформації через шахрайство, злами, маніпуляції та кібератаки. Аналізуються цифрові сліди, що їх залишають користувачі на відкритих платформах» [11].

Натомість попри певні складнощі OSINT зарекомендувала себе у військовій, політичній сфері, у роботі поліції та приватних детективів, при проведенні журналістських розслідувань. Одним із показових прикладів використання OSINT при розслідуванні злочинів, вчинених в умовах збройної агресії рф, є справа пасажирського літака Boeing 777 (рейс МН17), збитого 2014 році над окупованою територією Донецької області. Слід зауважити, що одними із доказів у цій справі стали саме дані з відкритих джерел: знімки та дописи з соціальних мереж російських військовослужбовців та представників т. зв. «ДНР», геодані, знімки уламків літака та ін. [12].

Іще одним прикладом є отримання інформації про вчинені воєнні злочини з відеокамер, які знаходилися у містах, що були під окупацією, за допомогою якої шляхом отримання додаткової інформації з відкритих джерел стала можливою ідентифікація російських військових. Слід зауважити, що така інформація може бути отримана з відповідних ресурсів: «Безпечне місце», камер ОСББ, реєстраторів, камер, встановлених у приватній власності, інтернет-аккаунтів, месенджерів та ін. ресурсів – відкритих джерел.

Зауважимо, що OSINT у розслідуванні злочинів використовують не тільки правоохоронні органи, але й журналісти, громадські організації та активісти. Одним із перших з часів збройного конфлікту таким став Центр «Миротворець», який є незалежною, недержавною організацією, яка створена ученими, журналістами та спеціалістами з дослідження ознак злочинів проти національної безпеки України, миру, безпеки людства та міжнародного правопорядку [13]. Активну роль у такій діяльності відіграє Українська Гельсінська спілка з прав людини, Міжнародна волонтерська спільнота Inform Napalm, до якої входять представники більш ніж 10 країн [14], та багато інших організацій та осіб, які залучаються до діяльності зі збору, аналізу інформації щодо воєнних злочинів з використанням OSINT. Прикладом, з лютого по серпень 2022 року завдяки такій роботі був створений онлайн-реєстр, що містить персональні дані військових російської армії, полонених та вбитих росіян під час війни в Україні, який на той час уже налічував понад 150 тисяч російських військових, які беруть участь у війні проти України [15].

Натомість слід враховувати, що OSINT – це не просто процес пошуку інформації, це процес її збереження, відповідної обробки, співставлення з іншою інформацією задля отримання певного результату щодо встановлення обставин, що мають значення для кримінального провадження, побудови криміналістичних версій, планування процесу розслідування. Окремі фахівці у спрощеному вигляді виділяють наступні елементи: збір інформації, чищення даних та аналіз «чистих» даних [11]. Інші виділяють: ідентифікацію джерел, колекціонування даних, обробку даних, аналіз і звітність [8, с. 38-39].

Як зазначають вчені, можливість збирання інформації з відкритих джерел може здійснюватися вручну або автоматизовано за допомогою відповідного інструментарію та алгоритмів. Наприклад, актуальним є використання програмних інструментів або сценаріїв в процесі відшукання належної інформації, наприклад для вебскрапінгу – перетворення у структуровані дані інформації з вебсторінок: python-сценарій snscrape для служб соціальних мереж (SNS), який сканує профілі користувачів, хештеги або пошукові запити, групи, канали Facebook, Instagram, Telegram, Twitter, ВКонтакте, Weibo, Mastodon, Reddit,

і повертає виявлені елементи, наприклад відповідні публікації, Hunchly [16, с. 85].

В залежності від сценарію, завдань та кінцевої мети може аналізуватися як фактичне висвітлення інформації (наприклад, що, хто зображений на відео та/ чи фотознімку, відеозаписі, знімках з геолокаційних даних), так і метадані, а в решті-решт –здійснювати комплексна їх оцінка. Метаданими є інформація, що формується видавцями електронних ресурсів як обов'язковий мінімум відомостей, що дає каталогізатору можливість використати їх при систематизації у чітко регламентованому середовищі електронного каталогу з відповідними правилами і стандартами [17]. У спрощеному розумінні – це дані про дату, час, місце створення, «цифровий відбиток» відповіднох цифрової інформації. Самі судді зазначають: «Метадані забезпечують необхідний контекст для оцінки доказів (даних) так само, як поштовий штемпель забезпечує контекст для оцінки звичайного (паперового) листа та його змісту. Суди повинні усвідомлювати потенційну доказову цінність метаданих, у випадку коли інша сторона оспорює достовірність доказу (авторство, цілісність, автентичність). Метадані можуть бути використані для відстеження та ідентифікації джерела та адресата повідомлення, даних про пристрій, який створив електронні докази, дати, часу, тривалості та типу доказів. Метадані можуть бути релевантними або як непрямі докази (наприклад, вказівки на найбільш релевантну версію документа), або як прямі докази (наприклад, якщо даними файлу маніпулювали). Ця настанова також релевантна у випадку втрати метаданих» [18].

Ось чому правильне фіксування інформації з відкритих джерел під час розслідування відіграє дуже важливе значення. На сьогодні методичним путівником є Протокол Берклі – це практичний посібник з використання цифрової інформації з відкритим вихідним кодом при розслідуванні порушень міжнародного кримінального права, права людини та гуманітарного права, розроблений школою права Університету Каліфорнії в Берклі разом з представниками ООН Протокол Берклі про дослідження цифрових відкритих джерел. У ньому містяться керівні положення щодо міжнародних стандартів для проведення інтернет-розслідувань передбачуваних порушень, керівництво про методи та процедури для збирання, аналізу та зберігання цифрової інформації з дотриманням професійних, правових та етичних принципів [19]. Відповідно до нього алгоритм передбачає (1) процес виявлення інформації (он-лайн запити, моніторинг); (2) процес попередньої оцінки даних; (3) процес колекціонування даних (4) процес збереження даних, тобто фіксація і вилучення цифрової інформації з Інтернету в такий спосіб, що дозволяє підтвердити певні факти навіть тоді, коли з першоджерела інформація була видалена (резервне копіювання даних, завантаження контенту, виготовлення скрінів екрану тощо); (5) процес верифікації (перевірка надійності джерел даних та правдивості їх змісту); (6) процес слідчого аналізу, тобто інтерпретація даних, формулювання висновків, ідентифікація прогалин, з'ясування значення отриманих даних для процесу розслідування [8, с. 40].

Таким чином, в умовах війни в Україні OSINT зарекомендував себе як ефективний інструмент роботи з інформацією з відкритих джерел. Серед вчених і фахівців на сьогодні тривають дискусії щодо поняття інформації з відкритих джерел, гарантій забезпечення законності отримання з окремих з них, апробуються різні види програмного забезпечення та методик його використання, роботи з отриманою інформацією. Водночас, слід зауважити, що важливою складовою використання отриманих за допомогою OSINT даних є перспектива їх подальшого використання у судах, у тому числі МКС, і хоча на сьогодні завдяки міжнародному досвіду та уже набутому досвіду вітчизняних фахівців напрацьовано низку стандартів, перспективним напрямком дослідження залишаються питання процесуалізації такої інформації: збирання, перевірки та оцінки отриманих фактичних даних.

Анотація

Стаття присвячена дослідженню окремих питань використання OSINT при розслідуванні злочинів в умовах військової агресії рф.

Зазначається, що в умовах тимчасової окупації окремих територій, активних бойових дій можливість проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій, отримання інформації за запитами та іншими традиційними процесуальними способами унеможливлена чи ускладнена. Автори звертають увагу на значну кількість воєнних злочинів та необхідність їх ефективного розслідування. Констатується, що розвиток інформаційних, комп'ютерних технологій виводить на якісно новий рівень процеси розслідування: отримання криміналістично значущої інформації, важливу роль у яких має OSINT.

Авторами аналізується поняття OSINT та інформації з відкритих джерел, алгоритму роботи з ними. Звертається увага, як на позитивні сторони, так і труднощі, які можуть виникнути при роботі з інформацією з відкритих джерел. Вказується необхідність забезпечення відповідних гарантій функціонування OSINT задля ефективності, виконання завдань кримінального провадження, захисту персональних даних відповідно до законодавства, можливості процесуальної фіксації і використання у процесі доказування у національних судах та Міжнародному кримінальному суді.

Вказується, що в Україні сьогодні з інформацією з відритих джерел, яка може бути використана у розслідуванні, працюють не тільки представники правоохоронних органів, а й фахівці у сфері ІТ, громадські організації, журналісти, волонтерські групи та ін.

Звертається увага на необхідності забезпечення відповідної процедури збирання, перевірки та оцінки інформації з відкритих джерел, важливості метаданих у процесі доказування. Акцентується увага на особливому значенні відповідного фіксування такої інформації для можливості використання її як доказів у національних судах та у Міжнародному кримінальному суді. Як один із апробованих методів наводиться Протокол Берклі.

Ключові слова: OSINT, інформація, докази, доказування, відриті джерела, дані, воєнні злочини, Міжнародний кримінальний суд, фіксування, Протокол Берклі, розслідування, військова агресія, воєнний стан.

Vykhodets Yu.O., Teteriatnyk H.K. Some issues of the use of osint in the investigation of crimes in the conditions of military aggression of the russian federation

Summary

The article is devoted to the study of certain issues of the use of OSINT in the investigation of crimes in the conditions of military aggression of the russian federation.

It is noted that in the conditions of temporary occupation of certain territories, active hostilities, the possibility of conducting investigative (search) actions, covert investigative (search) actions, obtaining information upon requests and other traditional procedural methods is impossible or complicated. The authors draw attention to the significant number of war crimes and the need for their effective investigation. It is noted that the development of information and computer technologies brings investigative processes to a qualitatively new level: obtaining forensically significant information, in which OSINT plays an important role.

The authors analyze the concept of OSINT and information from open sources, the algorithm for working with them. Attention is drawn to both the positive aspects and difficulties that may arise when working with information from open sources. It is indicated the need to provide appropriate guarantees of OSINT functioning for efficiency, performance of tasks of criminal proceedings, protection of personal data in accordance with legislation, possibility of procedural fixation and use in the process of proof in national courts and the International Criminal Court.

It is indicated that in Ukraine today, not only representatives of law enforcement agencies, but also specialists in the field of IT, public organizations, journalists, volunteer groups, etc. work with information from open sources that can be used in the investigation.

Attention is drawn to the need to ensure an appropriate procedure for collecting, checking and evaluating information from open sources, the importance of metadata in the process of proof. Attention is focused on the special importance of appropriate recording of such information for the possibility of using it as evidence in national courts and the International Criminal Court. The Berkeley Protocol is cited as one of the proven methods.

Key words: OSINT, information, evidence, proof, open sources, data, war crimes, International Criminal Court, recording, Berkeley Protocol, investigation, military aggression, martial law.

Список використаних джерел:

1. Єдиний звіт про кримінальні правопорушення по державі за листопад 2022 року. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.
2. Одерій О.В., Кожевніков О.А. отримання криміналістично значущої інформації шляхом аналізу відкритих інтернет-джерел. Правовий часопис Донбасу. 2020. № 4 (73) 2020. С. 144 – 155.
3. Яровий Т. С. OSINT, як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. *Експерт: парадигми юридичних наук і державного управління*. 2019. № 4(6). С. 201 – 208.
4. Ржевська Н.Ф. Розвідка відкритих джерел (OPEN SOURCE INTELLIGENCE) Ржевська Н. Ф., Кожушко О. О. Розвідка відкритих джерел. URL: http://ena. lp.edu.ua/bitstream/ntb/19232/1/53– Rzhevska-257-261.pdf.
5. Heather J. Williams, Ilana Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise https://www.rand.org/pubs/ research_reports/RR1964.html
6. Open Source Intelligence (OSINT): Issues for Congress, December 5, 2007. (n.d.). fas.org. Retrieved from www.fas.org/sgp/crs/ intel/RL34270.pdf
7. Гавловський В. Д. Окремі питання отримання інформації з відкритих джерел для правоохоронних органів. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2010. Вип. 23. С. 308−315.
8. Дуфенюк О. Використання відкритих джерел цифрової інформації під час розслідування злочинів. Інформація та документ у сучасному науковому дискурсі: матеріали VII Всеукраїнської дистанційної науково-практичної конференції. (Івано-Франківськ, 20 травня 2022 р.). Івано-Франківськ: ІФНТУНГ, 2022. С. 36-41.
9. Війна та правосуддя: як слідчим ефективно використовувати Osint та що робити із рішеннями «судів» на непідконтрольних територіях. URL: https://helsinki.org.ua/articles/viyna-ta-pravosuddia-iak-slidchym-efektyvno-vykorystovuvaty-osint-ta-shcho-robyty-iz-rishenniamy-sudiv-na-nepidkontrolnykh-terytoriiakh/.
10. Щербань В. Д. Система гарантій функціонування OSINT у сфері антикорупційної діяльності в правоохоронних органах. Часопис Київського університету права. 2019. №4. С. 137 – 141.
11. Що таке OSINT і як він допоміг викрити вбивства у Бучі. URL: https://explainer.ua/shho-take-osint-i-yak-vin-dopomig-vikriti-vbivstva-u-buchi/.
12. InformNapalm. URL: https://informnapalm.org/ua/category/for-ato-fighter/osint-info/page/3/.
13. Сайт «Миротворець». URL: https://myrotvorets.center/about/.

14. InformNapalm. URL: https://informnapalm.rocks/.
15. В Україні зібрали базу майже 150 тисяч російських військових-злочинців. Львівський портал. URL: https://portal.lviv.ua/news/2022/08/31/v-ukraini-zibraly-bazu-majzhe-150-tysiach-rosijskykh-vijskovykh-zlochyntsiv.
16. Пашковський М.І. Особливості використання OSINT при документуванні та розслідуванні колаборaційної діяльності. Актуальні питання кримінально-правової кваліфікації, документування та розслідування колаборaціонізму : матеріали Всеукр. науково-практ. конф., м. Одеса, 21 лип. 2022 р. Одеса, 2022. С. 82–86.
17. Шаховська Н. Б., Пасічник В. В. Сховища та простори даних. Львів, 2009. 230 с.
18. Яновська О. Докази та доказування у кримінальному провадженні в умовах воєнного стану: практика Верховного Суду. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2022_prezent/2022_09_28_Ianovska_.pdf
19. Berkeley Protocol on Digital Open Source Investigations. URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf.