УДК:343.983
DOI.ORG/10.32703/2663-6352/2024-1-15-105-111
Ліхтанська Анна Петрівна
студентка 2013 групи
юридичного факультету
Інституту управління та технологій
Державного університету інфраструктури та технологій,
м. Київ Україна

ORCID.ORG/0000-0002-0892-1694
Михайлов Володимир Олександрович
старший викладач кафедри правосуддя
юридичного факультету
Інституту управління та технологій
Державного університету інфраструктури та технологій,
м. Київ Україна

ВИКОРИСТАННЯ OSINT В КРИМІНАЛЬНОМУ ПРАВІ УКРАЇНИ

Анотація. *Стаття присвячена дослідженню окремих питань використання OSINT у кримінальному праві України. Автор звертає увагу навелику кількість воєнних злочинів та необхідність їх ефективного розслідування. Зазначається, що розвиток інформаційно-комп'ютерних технологій виводить слідчі процеси на якісно новий рівень: отримання криміналістична значущої інформації, в чому важливу роль відіграє OSINT.*

Проаналізовано поняття OSINT та інформацію з відкритих джерел, а також алгоритм роботи з ними. Звертається увага як на позитивні моменти, так і на труднощі, які можуть виникнути при роботі з інформацією з відкритих джерел. Зазначається, що з міркувань ефективності, виконання завдань кримінального процесу, захисту персональних даних відповідно до законодавства, можливості процесуальної фіксації та використання в процесі доказування в національних судах необхідно передбачити відповідні гарантії функціонування OSINT.

Використання комп'ютерних технологій стало невід'ємною частиною сучасного світу, а глобальна мережа Інтернет – невід'ємною частиною життя людини. При цьому кожен користувач інтернет-гаджетів, так чи інакше, залишає свій «інтернет-слід», фотографуючись з друзями, роблячи «чек-ін» або оцінюючи якість обслуговування персоналом рекламного та сервісного центру. Крім того, такі елементарні заходи щодо громадян правоохоронці можуть застосовувати для запобігання чи розкриття злочинів.

OSINT безпосередньо розглядається як метод збору інформації для запобігання та розкриття злочинів. Вперше технічні прийоми OSINT (Open Sources Intelligence) були застосовані під час Другої світової війни американською розвідкою, а саме Службою моніторингу іноземного мовлення (FBMS). Але сьогодні OSINT використовують не лише державні спецслужби, а й журналісти, приватні детективи, IT-компанії, фінансові групи тощо.

Ключові слова: OSINT, інформація, докази, доказування, відриті джерела, дані, фіксування, розслідування.

Annotation. *The article is devoted to the study of certain issues of the use of OSINT in the criminal law of Ukraine. The author draws attention to the large 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 concepts of OSINT and information from open sources, as well as the algorithm for working with them, were analyzed. Attention is drawn to both positive points and difficulties that may arise when working with information from open sources. It is noted that for reasons of efficiency, performance of tasks of the criminal process, protection of personal data in accordance with the law, the possibility of procedural fixation and use in the process of proof in national courts, it is necessary to provide for appropriate guarantees of the operation of OSINT. Attention is drawn to the need to ensure a proper process of collecting, verifying and evaluating information from open sources, as well as to the importance of metadata in the process of proof.

The use of computer technologies has become an integral part of the modern world, and the global Internet has become an integral part of human life. At the same time, every user of Internet gadgets, in one way or another, leaves his "Internet footprint" by taking pictures with friends, checking in, or evaluating the quality of service provided by advertising and service center personnel. In addition, such elementary measures against citizens can be used by law enforcement officers to prevent or solve crimes.

OSINT is directly considered as a method of collecting information for the prevention and detection of crimes. OSINT (Open Sources Intelligence) technical techniques were first used during World War II by American intelligence, namely the Foreign Broadcast Monitoring Service (FBMS). But today OSINT is used not only by state intelligence services, but also by journalists, private detectives, IT companies, financial groups, etc.

Keywords: OSINT, information, evidence, proof, open sources, data, capture, investigation.

Постановка проблеми. У часи розвитку цифрових технологій є необхідність дослідити можливості забезпечення належного процесу збору, перевірки та оцінки інформації з відкритих джерел, а також на важливість метаданих у процесі доказування.

Огляд останніх досліджень і публікацій. Проблематику штучного інтелекту вивчали наступні вчені: Дуфенюк О., Демура М.І., Ржевська Н.Ф.., Серватовський А. В., Онищенко Ю.М., Макаренко П.В., Шевчук Т.А. та інші.

Формулювання завдання дослідження. Метою статті є отримання наукового результату у вигляді теоретично обґрунтованих положень щодо окремих питань використання OSINT в кримінальному процесі України.

Виклад основного матеріалу. Вчені по-різному визначають сутність OSINT. Перша група обмежується отриманням інформації виключно з віртуального простору [9, с. 205]

Другий – більш комплексний підхід до інтерпретації, який зазначає, що це одна з форм процесу організації та управління збором розвідувальних даних (Intelligence Collection Management), що включає їх пошук та відбір із загальнодоступних джерел, закупівлю та аналіз інформації, яка формує розвідувальний документ для прийняття відповідного рішення.

Третя пропозиція пропонує вважати «...OSINT є такою формою роботи з розвідувальними даними, яка включає їх пошук і відбір із відкритих, загальнодоступних джерел, подальшу класифікацію та аналіз інформації, а також формування висновків щодо управління і може служити основою для прийняття управлінських рішень».

А з посиланням на американські джерела зазначають, що існують такі категорії відкритих джерел інформації: 1. широко розповсюджені дані та інформація; 2. цільові комерційні дані; 3. звіт; 4. “сіра” література.

Водночас експерти зазначають, що пошук значущої інформації в Інтернеті пов’язаний із необхідністю подолання низки викликів, пов’язаних із великими обсягами даних, складною динамікою інформаційних потоків, багаторазовим дублюванням інформації, викликані наявністю «шумової інформації», відсутністю індексації значних обсягів інформації в

пошукових системах (навіть такій потужній пошуковій системі Google, за деякими підрахунками, потрібно 300 років, щоб індексувати всю інформацію, обсяг якої становить 300 років, далі рости) [7]. Конкретний механізм обробки цієї інформації, тобто на подальшу можливість їх використання як доказів, зокрема у кримінальному провадженні, з урахуванням перспективи подальшого подання до Міжнародного кримінального суду.

Дослідження В.Д.Щербаня щодо системи забезпечення функціональності OSINT є актуальним. І хоча теми представлені в контексті антикорупційної діяльності правоохоронних органів, деякі з них також є орієнтиром для використання OSINT у сфері розслідування:

- гарантія права правоохоронних органів вільно збирати, зберігати і використовувати інформацію, якщо це не порушує таємниці листів, телефонних розмов, телеграфної та іншої кореспонденції і не полягає у збиранні, зберіганні та використанні конфіденційної інформації;
- гарантія створення механізмів реалізації правоохоронними органами права на інформацію при проведенні розвідувальної інформації 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 одержання необхідної інформації від усіх органів державної влади, підприємств, організацій та установ тощо;
- гарантія отримання інформації від її розпорядників – передбачає на нормативному рівні визначення видів інформації, передбаченої законодавством для розпорядників, яка не є конфіденційною та має надаватися правоохоронним органам, які здійснюють правоохоронні дії на їх запит;
- гарантія максимального спрощення процедури отримання публічної інформації – ця гарантія забезпечує швидкість та оперативність отримання інформації за умови, що вона не порушує таємниці листів, телефонних розмов, телеграфної та іншої кореспонденції та не полягає у збиранні, зберіганні, використанні конфіденційної інформації [6].

Як слушно підкреслюють ІТ-фахівці: «OSINT не включає несанкціонований доступ до інформації шляхом шахрайства, хакерства, маніпуляцій і кібератак». Цифрові сліди, залишені користувачами на відкритих платформах, аналізуються.

Натомість, незважаючи на певні труднощі, OSINT зарекомендував себе у військовій, політичній сферах, у роботі поліції та приватних детективів, а також у проведенні журналістських розслідувань.

Натомість слід мати на увазі, що OSINT – це не просто процес пошуку інформації, а процес її збереження, відповідної обробки та порівняння з іншою інформацією з метою досягнення певного результату щодо встановлення обставин, що мають значення для кримінального провадження, створення криміналістичних версій, планування процесу розслідування. Окремі спеціалісти спрощено виділяють наступні елементи: збір інформації, очищення даних та аналіз «чистих» даних.

Інші виділяють: ідентифікацію джерела, збір даних, обробку даних і звітність [8]. Як зазначають науковці, можливість збирати інформацію з відкритих джерел є вручну або автоматично за допомогою відповідних інструментів і алгоритмів. Наприклад, доцільно використовувати програмні інструменти або сценарії під час пошуку відповідної інформації, наприклад, для веб-скрейпінгу – перетворення інформації з веб-сторінок у структуровані дані: Snscrape Скрипт Python для служб соціальних мереж (SNS), який сканує профілі користувачів, хештеги або пошукові запити, групи Facebook, Instagram, Telegram, Twitter, ВКонтакте, Weibo, канали Mastodon і Reddit і повертає розпізнані елементи, такі як відповідні публікації Hunchly.

Залежно від сценарію, завдань і кінцевої мети можливий аналіз як фактичного інформаційного охоплення (наприклад, що і хто зображений на відео та/або фото, відеозапис, знімки з даних геолокації), так і метаданих і в кінці - проведення комплексної оцінки. Метадані — це інформація, створена видавцями електронних ресурсів як обов’язковий інформаційний мінімум, що дає можливість каталогізатору використовувати її при систематизації в чітко

регламентованому середовищі електронного каталогу з відповідними правилами та стандартами.

У спрощеному сенсі це дані про дату, час, місце створення, «цифровий відбиток» відповідної 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 вмісту. «Суди повинні знати про потенційну доказову силу метаданих, якщо протилежна сторона оскаржує автентичність доказів (авторство, цілісність, автентичність) Метадані можуть бути використані для ідентифікації джерела та одержувача повідомлення, даних про пристрій, який відправив електронний для відстеження та ідентифікації дати, часу, тривалості та типу створених доказів. Метадані можуть бути релевантними як непрямі докази (наприклад, вказувати на найбільш релевантну версію документа) або як прямі докази (наприклад, якщо дані файлу були підроблені). Ця політика актуальна також у разі втрати метаданих» [5].

Тому правильний збір інформації з відкритих джерел відіграє дуже важливу роль під час розслідування. Методичним посібником сьогодні є Берклійський протокол, практичний посібник із використання цифрової інформації з відкритим джерелом у розслідуванні порушень міжнародного кримінального права, прав людини та гуманітарного права, розроблений Університетом Каліфорнії, Школою права Берклі спільно з представниками згідно з Берклійським протоколом Організації Об'єднаних Націй щодо цифрових досліджень із відкритим кодом. У ньому містяться вказівки щодо міжнародних стандартів проведення онлайн-розслідувань підозрюваних порушень, а також вказівки щодо методів і процедур збору, аналізу та зберігання цифрової інформації професійним, законним та етичним способом.

Відповідно, даний алгоритм забезпечує:

- процес виявлення інформації (онлайн-запити, моніторинг);
- процес попередньої оцінки даних;
- процес збору даних;
- процес збереження даних, тобто збір і вилучення цифрової інформації з Інтернету таким чином, щоб можна було підтвердити певні факти, навіть якщо інформацію було видалено з вихідного джерела (резервне копіювання даних, завантаження вмісту, створення скріншотів тощо);
- процес верифікації (перевірка надійності джерел даних і правдивості їх змісту);
- процес слідчого аналізу, тобто інтерпретація даних, формулювання висновків, виявлення прогалин, з'ясування значущості отриманих даних для процесу розслідування [1, с. 38]

Таким чином OSINT зарекомендував себе як ефективний інструмент для роботи з інформацією з відкритих джерел в Україні. Серед науковців і спеціалістів продовжуються дискусії щодо поняття інформації з відкритих джерел, гарантій законності її отримання з деяких із них, різних видів програмного забезпечення та способів його використання, а також роботи з отриманою інформацією. Водночас слід зазначити, що важливою складовою використання даних, отриманих за допомогою OSINT, є перспектива їх подальшого використання в судах, у тому числі в Міжнародному кримінальному суді, і хоча вже розроблено ряд стандартів для цього, виходячи з міжнародного досвіду та вже набутого досвіду вітчизняних спеціалістів, перспективним напрямом дослідження такої інформації залишаються питання процесуалізації: збір, перевірка та оцінка отриманих фактичних даних.

До переваг OSINT можна віднести доступність джерел інформації, обсяг інформаційних ресурсів, простоту повторного використання, а також мінімальні витрати на отримання цієї інформації. У цьому контексті використання елементів і методів OSINT в сфері кримінального права можна розглядати в поєднанні з іншими елементами в рамках конкретних моделей запобігання злочинності.

Слід враховувати, що збір інформації з відкритих джерел може розглядатися як вторгнення в приватне життя. У цьому випадку систематичний збір інформації вважається втручанням у приватне життя, оскільки особа, яка публікує цю інформацію, розраховує на збереження цих даних і відсутність моніторингу свого профілю. Збір даних дозволяється лише в рамках положень законодавства та з метою боротьби зі злочинністю. Враховуючи вимоги європейського законодавства щодо захисту прав і свобод людини, необхідно також наголосити, що правоохоронні органи мають право збирати будь-яку інформацію за умови, що законодавством країни передбачено зберігання загальнодоступної інформації, отриманої через правові засоби.

Відповідні органи мають право збирати інформацію про осіб лише в рамках окремого оперативно-розшукового провадження або відкритого кримінального провадження. Щодо цих випадків у ч. 3 ст.214 Кримінально-процесуального кодексу України законодавець передбачає, що проведення досудового розслідування (розшукових заходів) до порушення кримінального провадження не допускається і тягне за собою відповідну відповідальність (щодо досудового розслідування).

Для об'єктивності використання OSINT у кримінальному праві необхідно розрізняти принципи отримання інформації з відкритих джерел, зокрема:

- загальне право - законність;
- повага і дотримання прав і свобод людини і громадянина;
- верховенство права та презумпція невинуватості. Ця група принципів стосується не лише розвідувальної та правоохоронної діяльності, а насамперед усіх сфер суспільних відносин.
- відомчий - характерний виключно для підрозділів, які здійснюють діяльність виключно в рамках кримінального провадження. До них належать принципи безперервності, відкритості та негласності слідчих дій, справедливості та неупередженості.

На сьогоднішній день OSINT активно та успішно використовується інформаційно-аналітичними підрозділами провідних країн світу. Дані щодо відсоткового співвідношення продуктивності відкритих джерел інформації підтверджують необхідність і актуальність використання досвіду США та європейських країн у вирішенні оперативних, тактичних і стратегічних завдань силових структур [3].

Варто зазначити, що використання OSINT-методів є невід'ємною частиною кримінально-правової діяльності багатьох європейських країн, особливо при криміналістичному та експертному супроводі розслідування кримінальних проваджень з метою пошуку достовірної інформації.

Виходячи з вищесказаного, OSINT – це сукупність способів і методів пошуку інформації у загальнодоступних джерелах, таких як: соціальні мережі та відкриті бази даних в Інтернеті.

Основними перевагами OSINT є доступність джерел та мізерність матеріальних витрат для отримання такої інформації. Використовуючи методи OSINT, можливим є:

- встановити особу, яка вчинила злочин, за фотографією;
- встановити місцезнаходження особи, яка перебуває в розшуку, за допомогою соціальних мереж, зокрема особистих сторінок як розшукуваної особи, так і кола її знайомих;
- встановити коло знайомств та інтересів особи тощо.

Важливим є не лише оперативний доступ до необхідних ресурсів, але фіксація їх стану та змісту, пошук та належне збереження вилученої з них інформації. Таким чином, постає завдання в забезпеченні оперативного та постійного моніторингу значного обсягу повідомлень в індивідуальних профілях, групах, каналах соціальних мереж та клауд-месенджерів з метою аналізу, виявлення та фіксації (збереження) відомостей, що можуть бути використані як докази злочинної діяльності або цілеспрямованого відшукання певного повідомлення.

Завдання ускладнює та обставина, що цифрова інформація, що знаходиться у відкритому доступі, вразлива до змін та видалення (знищення), а отже адекватність інструментів та методів її збереження є вирішальними факторами (під адекватністю розуміється сукупність

властивостей цифрового елемента, які необхідно охороняти та зберігати з плином часу, включають його автентичність, доступність, ідентичність, стійкість, можливість відображення та зрозумілість [5]).

Нерідкими є випадки, коли інформація, що знаходиться у відкритому доступі, про колаборaційну діяльність збирається приватними особами (волонтерами) для її наступного надання до правоохоронних органів.

Оскільки цифрова інформація, що знаходиться у відкритому доступі (далі – інформація з відкритих джерел), збирається для використання як доказ у кримінальному провадженні, а сам процес збереження, як правило, полягає в отриманні цифрової копії (відбитку) такої інформації, важливим є забезпечення встановлення справжності цифрових даних. Тому протоколом Берклі рекомендовано зберігати цифрові дані у тому ж (рідному) форматі або "в стані, максимально наближеному до його вихідного формату. Будь- які зміни, перетворення або конвертації, спричинені процесом збору, повинні бути задокументовані".

Очевидно, що за належної підготовки таке збирання може здійснюватися і без участі спеціаліста. Щодо інформації з відкритих джерел протоколом Берклі рекомендовано фіксувати щонайменше такі дані: цільова вебадреса; вихідний код; захоплення всієї вебсторінки або зображення повідомлення крауд-месенджера в застосунку; вбудовані мультимедійні файли; вбудовані метадані; контекстуальні дані; хеш-значення; дані про процес збирання інформації [2].

В процесі роботи з інформацією з відкритих джерел важлива роль відводиться ланцюгу забезпечення збереження – "хронологічній документації послідовності зберігачів інформації чи доказів, а також документація контролю, дати та часу, передачі, аналізу та розпорядження такими доказами", у зв’язку з чим значно підвищуються вимоги до рівня деталізації відповідних протоколів слідчих (розшукових) дій, в межах яких здійснюється збереження інформації з відкритих джерел. У випадку, коли відповідна інформація фіксувалася приватними особами та на момент проведення розслідування вже відсутня у відкритому доступі, потрібно орієнтувати таких приватних осіб щодо надання відповідних хронологічних протоколів документування, допитувати таких осіб як свідків про обставини виявлення та збереження відповідної інформації. Такі протоколи волонтерів є документами (ст. 99 КПК України), вони мають значення для оцінки допустимості та достовірності як доказу відповідної інформації, збереженою волонтером з відкритих джерел.

Збирання інформації з відкритих джерел може здійснюватися вручну за стандартизованою процедурою або бути автоматизованим за допомогою різноманітних інструментів або сценаріїв. В останньому випадку ланцюг забезпечення збереження може створюватися також автоматично (програмно). Особливо актуальним є використання програмних інструментів або сценаріїв в процесі відшукання належної інформації, наприклад для вебскрапінгу (від англ. scraping) – перетворення у структуровані дані інформації з вебсторінок [4, с.152]).

Одним з таких достатньо простих для використання інструментів є 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. Самостійним програмним інструментом вебзахоплення, призначеним для онлайн-розслідувань, є, наприклад, Hunchly. Обидва інструменти використовуються у своїй діяльності Центром з прав людини Юридичної школи Каліфорнійського університету в Берклі.

Висновок. Викладене дозволяє зробити висновки про те, що цифрова інформація, що знаходиться у відкритому доступі, може мати важливе значення для розслідування кримінальних правопорушень, передбачених ст. 111-1 КК України. Цю інформацію можуть збирати також приватні особи та надавати органам досудового розслідування, прокуратури. Під час пошуку, збирання та подальшого використання такої інформації слід керуватися як методичним документом Протоколом Берклі. Така інформація може збиратися

як вручну, так і з використанням програмних інструментів. Важливим елементом забезпечення можливості перевірки та оцінки допустимості та достовірності як доказу вказаної інформації є ланцюг забезпечення збереження. Наразі КПК України не містить будь-яких застережень щодо збирання та використання в кримінальному провадженні цифрової інформації, що знаходиться у відкритому доступі Протоколу Берклі та інших подібних методичних посібників і має бути включено в програму підготовки правознавців та правоохоронців, в курси підвищення кваліфікації адвокатів, слідчих, прокурорів.

Підсумовуючи, варто зауважити, що з урахуванням дії правового режиму воєнного стану в Україні правоохоронним органам нашої країни необхідно опановувати метод OSINT та вдосконалювати навички його використання.

ЛІТЕРАТУРА

1. 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.
2. Єдиний звіт про кримінальні правопорушення по державі за листопад 2022 року. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yihdosudovogo-rozsliduvannya-2.
3. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI (із змін.) // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text
4. 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.
5. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права (перекл. з англ.). Вид. офіц. Нью-Йорк, Женева, 2020. 119 с.
6. 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.
7. Серватовський А. В., Онищенко Ю.М., Макаренко П.В. Міжнародний досвід використання OSINT. Актуальні питання протидії кіберзлочинності та торгівлі людьми: збірник матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2018. С. 379-382.
8.Щербань В. Д. Система гарантій функціонування OSINT у сфері антикорупційної діяльності в правоохоронних органах. Часопис Київського університету права. 2019. №4. С. 137 – 141.
9. 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.