УДК 343.1
DOI https://doi.org/10.24144/2307-3322.2025.88.3.41

ПРОБЛЕМИ ВИКОРИСТАННЯ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ В РАМКАХ МІЖНАРОДНОГО ЗБРОЙНОГО КОНФЛІКТУ

Косохатько Б.С.,
аспірант кафедри кримінального процесу та криміналістики
Інституту права
Київського національного університету імені Тараса Шевченка
ORCID: 0009-0007-2168-6469

Косохатько Б.С. Проблеми використання інформації з відкритих джерел під час розслідування злочинів в рамках міжнародного збройного конфлікту.

У статті досліджуються актуальні проблеми, пов'язані з використанням інформації з відкритих джерел під час розслідування злочинів, скоєних в умовах міжнародного збройного конфлікту, зокрема в контексті воєнної агресії Російської Федерації проти України, що триває з 2014 року і значно загострилася після 24 лютого 2022 року. Увага автора зосереджена на викликах, що постали перед українською правоохоронною системою, яка зіштовхнулася з безпрецедентною кількістю воєнних злочинів, складністю їх документування, відсутністю фізичного доступу до місць вчинення злочинів та необхідністю інтегрувати новітні підходи до збору доказової інформації.

Одним із таких інноваційних напрямів є застосування OSINT (розвідки з відкритих джерел) як інструменту збору, аналізу та збереження цифрових доказів. Автор обґрунтовує, що в умовах обмеженого доступу до зони бойових дій саме OSINT стає критично важливим інструментом, здатним забезпечити об'єктивну доказову базу для кримінального переслідування. У дослідженні охоплено питання допустимості, достовірності та релевантності інформації, зібраної з відкритих джерел, а також відсутність чіткого правового регулювання щодо статусу такої інформації як доказу в національному кримінальному процесі.

Значну увагу приділено міжнародним стандартам та практикам, зокрема Протоколу Берклі, який регламентує процес фіксації, архівації та зберігання електронних доказів, зібраних з відкритих джерел, із забезпеченням автентичності та незмінності цифрового контенту. Прикладом успішного застосування OSINT є справа про збиття авіалайнера рейсу MH17, в якій докази, зібрані за допомогою відкритих джерел, стали підставою для притягнення винних осіб до міжнародної відповідальності.

Також автор висвітлює ключові проблеми, що виникають у контексті правового статусу спеціалістів та аналітиків OSINT, які залучаються до кримінального процесу в Україні. Виявлено колізію між фактичним значенням висновків таких спеціалістів та їх юридичною невизначеністю в Кримінальному процесуальному кодексі України, де не передбачено їхній висновок як повноцінне джерело доказів. Автор пропонує розширити процесуальні права спеціалістів та інтегрувати міжнародні рекомендації до національного законодавства з метою підвищення ефективності збору цифрових доказів.

Наукова новизна дослідження полягає в комплексному аналізі взаємодії між традиційними методами розслідування воєнних злочинів та новітніми цифровими інструментами, що використовують потенціал відкритих джерел інформації. Обґрунтовано потребу в законодавчих змінах, розробці навчально-методичних матеріалів та підготовці фахівців із практичними навичками роботи з OSINT.

У підсумку автор доходить висновку, що залучення відкритих джерел є не лише вимушеним кроком в умовах воєнного стану, але й перспективним напрямом, що дозволяє документувати злочини, ефективніше притягувати до відповідальності винних осіб та зміцнювати доказову базу в міжнародному правосудді. Практична значущість дослідження полягає у формуванні рекомендацій щодо вдосконалення методології роботи з відкритими джерелами у межах національного кримінального процесуального права.

Ключові слова: розвідка з відкритих джерел (OSINT), воєнні злочини, цифрові докази, міжнародний збройний конфлікт, кримінальне провадження, Протокол Берклі, електронні дані, міжнародне гуманітарне право, кримінальний процес, спеціаліст.

Kosokhatko B.S. Problems of using open-source intelligence in the investigation of crimes committed within the framework of an international armed conflict.

This article examines pressing issues related to the use of open-source intelligence (OSINT) in the investigation of crimes committed in the context of an international armed conflict, with a particular focus on the full-scale invasion of Ukraine by the Russian Federation beginning on February 24, 2022. The study emphasizes the unprecedented challenges faced by Ukraine's law enforcement system, which was forced to adapt rapidly to new types of criminal offenses, such as war crimes, often under dangerous and psychologically taxing conditions.

The research highlights how the complexity and geographical scale of the conflict have made access to physical crime scenes difficult or impossible in many cases. Consequently, investigators increasingly rely on open-source information, including satellite images, video footage, social media content, and digital communications. These sources are critically important for documenting events, identifying perpetrators, and verifying the authenticity of incidents. The study outlines the limitations of the current legal framework in Ukraine regarding the admissibility and handling of digital and open-source evidence, emphasizing the lack of a clear definition for "electronic evidence" in national criminal procedure legislation.

Special attention is given to international standards, such as the Berkeley Protocol on Digital Open Source Investigations, developed by the University of California, Berkeley Human Rights Center and the Office of the United Nations High Commissioner for Human Rights. These guidelines propose ethical and methodological principles for collecting, verifying, preserving, and presenting open-source information in a manner consistent with international human rights and criminal procedure standards. The article references successful implementation examples, particularly the MH17 case, where evidence collected by the Bellingcat investigative team played a key role in initiating legal proceedings against members of the Russian military.

Furthermore, the study identifies a legal gap concerning the procedural status of OSINT specialists in Ukrainian criminal investigations. Although their expertise is indispensable in collecting and analyzing open-source data, the current Criminal Procedure Code does not recognize the opinion of a "specialist" as a formal source of evidence – only expert opinions are formally included in the list. The article argues for legislative reforms to elevate the procedural role of OSINT practitioners and to equate or integrate their functions with those of certified experts.

The scientific contribution of the study lies in its interdisciplinary approach, bridging the fields of criminal procedure, international humanitarian law, digital forensics, and intelligence studies. The author underscores the need for comprehensive training programs, methodological guides, and legal instruments to equip investigators and prosecutors with the skills necessary for working effectively with open-source data. In addition, the paper advocates for legal and institutional adjustments that would allow Ukrainian authorities to make full use of OSINT as a reliable and lawful source of evidence in both national and international legal contexts.

In conclusion, the author asserts that OSINT has proven to be an essential investigative tool, not merely as a temporary solution during wartime conditions, but as a forward-looking strategy for criminal justice. When applied rigorously and ethically, open-source intelligence significantly enhances the capacity to identify perpetrators, build robust cases, and pursue accountability for war crimes, even in the absence of immediate access to crime scenes. The practical relevance of this research lies in its proposed roadmap for integrating OSINT into Ukraine's legal and institutional structures, thereby strengthening its role in achieving justice during and after armed conflict.

Key words: open-source intelligence (OSINT), war crimes, digital evidence, international armed conflict, criminal investigation, Berkeley Protocol, electronic data, international humanitarian law, criminal procedure, specialist witness.

Постановка проблеми. Сучасний глобалізований світ часто створює умови для нових геополітичних союзів, розробки надсучасних технологій та своєю чергою провокує появу нових викликів. Таким чином починаючи з 23 лютого 2022 року, не тільки суспільство зіткнулося з новими,

масштабними викликами від повномасштабного вторгнення Російської Федерації на територію України, а й правоохоронні органи мусили також адаптуватися під роботу в небезпечних для життя умовах й швидко навчитися працювати з тими злочинами, в яких раніше могли не мати достатньо досвіду та експертизи. Звісно що мова йде про злочини в умовах міжнародного збройного конфлікту. І хоча Україна так чи інакше стикається з ними вже починаючи з 2014 року, однак, їх масштабність та складність вразила всіх ще більше починаючи з 2022 року. Саме з цього періоду необхідність якісного їх розслідування стала ще вищою.

Станом на 31 січня 2025 року, за офіційною статистикою сайту Міністерства внутрішніх справ, всього правоохоронці відкрили 140 956 кримінальних справ. Однак, варто зауважити, що хоч і заголовок публікації "російські воєнні злочини: оновлені дані станом на 31 січня 2025 року", все ж МВС висвітлює їх наступний розподіл:

- Воєнні злочини – 125 079 випадків
- Порушення територіальної цілісності – 9320
- Колабораційна діяльність – 4268
- Державна зрада – 274 [1].

Трохи дивним виглядає такий заголовок, оскільки те що стосується статей 110 (порушення територіальної цілісності), 111-1 (колабораційна діяльність) та 111 (державна зрада), то загальноприйнято вважати, що ці злочини не вважаються "воєнними", хоч їх часто і асоціюють саме з збройним конфліктом. Однак, вони не підпадають під юрисдикцію МКС та не передбачені Римським статутом та звісно ж, не розслідуються іншими країнами, як найтяжчі злочини. До того ж, якщо слідувати такій логіці, то як воєнні варто розглядати й злочини, що стосуються пропаганди, а саме статті 436, 436-1 та 436-2. Окрім того, постає цілком логічне питання, чому в статистику не включені й інші статті з відповідного розділу. Ми можемо лише припускати чому було прийнято таке рішення, однак, для розуміння навантаження на правоохоронні органи будемо оперувати саме цими даними.

Що ж стосується тематики мого дослідження, то насправді нас цікавлять лише воєнні злочини. Однак, все ж, залишається незрозумілим, чи йде мова в статистиці саме про статтю 438 Кримінального кодексу України, чи також і про інші злочини передбачені ККУ (наприклад стаття "437. Злочин агресії"), яка взагалі не включена в статистику, але вона передбачена в Римському статуті, який Україна вже ратифікувала, однак досі не повністю імплементувала [2].

Ми також можемо побачити на вже зазначеному ресурсі не менш показову статистику щодо місць утримання та катувань, яка висвітлює нам значну кількість в Херсонській, Харківській та Запорізькій області: 23, 31 та 29 місць відповідно. Така ситуація насправді означає неабияку кількість потерпілих, підозрюваних та контекстуальної інформації, яку слідчим, оперативним працівникам та прокурорам необхідно встановити.

Звісно, ми розуміємо, що така кількість може означати, що правоохоронна система відчуває певне перевантаження. І насправді, якщо подивитися ширше, то мова звісно в першу чергу йде про державні інституції, як комплексне поняття, однак крім самої системи державної влади в цілому, мова може йти ще й про конкретних людей: слідчих, оперуповноважених, прокурорів та інших, які наразі займають відповідні позиції в органах правопорядку, судоустрою та виконують методичну та кропітку роботу з розслідування справ. Для них це також виклик і не аби яке навантаження, в тому числі психологічне, адже окрім фізичної спроможності, вони повинні мати відповідну компетенцію, чудово розумітися в правових та процесуальних питаннях, які перед ними постають, й до того ж залишатись об'єктивними та емоційно стабільними. Що ж стосується розслідування воєнних злочинів, то це питання часто нове не лише для окремої особи, але й певною мірою для цілих підрозділів чи інституцій.

Метою дослідження є всебічний аналіз правових, процесуальних та практичних аспектів використання інформації з відкритих джерел (OSINT) під час документування та розслідування злочинів, вчинених у контексті міжнародного збройного конфлікту, зокрема воєнних злочинів, що мають місце внаслідок збройної агресії Російської Федерації проти України. Дослідження спрямоване на:

- виявлення основних викликів, з якими стикаються органи досудового розслідування під час збору, фіксації, збереження інформації з відкритих цифрових джерел;
- оцінку нормативно-правового регулювання OSINT-діяльності в межах кримінального процесу України та міжнародного досвіду;

- аналіз можливостей імплементації міжнародних стандартів (зокрема Протоколу Берклі, ISO/IEC 27037:2017) у національне законодавство;
- визначення ролі та правового статусу фахівців OSINT у кримінальному провадженні;
- формулювання пропозицій щодо вдосконалення нормативної бази та розробки методичних рекомендацій для практиків.

Загальна мета полягає в обґрунтуванні доцільності системного впровадження OSINT як легітимного та ефективного інструмента кримінального переслідування в умовах сучасних збройних конфліктів, що дозволить підвищити ефективність боротьби з воєнними злочинами, забезпечити відповідальність винних осіб та захист прав потерпілих.

Стан опрацювання проблематики. Звісно, питання розслідування злочинів вчинених в умовах збройного конфлікту не є абсолютною новелою, адже країна стикається з ними вже понад 10 років. За період АТО (або ООС), ці питання безумовно досліджувалися в різних сферах, в тому числі як їх криміналістичні аспекти, так і аспекти національного та міжнародного права. Так чи інакше це розглядали такі науковці як Коваль Д.О., Гарасимів О.І., Марко С.І., Ряшко О.В, Торбас О.О, Тетерятник Г.К., Гловюк І.В. та багато інших. Окрім того, звісно ж, окремі науковці досліджували загальні питання кримінально-процесуального права і питання перехідного правосуддя, які є невід'ємною частиною системи досліджень права під час війни, –це, зокрема, Кучинська О.П., Хотинська-Нор О.З., Каліннікова О.В, Погорецький М.А., а також інші.

Виклад основного матеріалу. Звісно, повномасштабне вторгнення певною мірою продемонструвало, що практичне розслідування воєнних злочинів відрізняється від того, як це було втілено та висвітлено доктриною раніше, що власне зумовлює необхідність більш практичних наукових праць у цьому векторі. Можна вважати одними з перших та значущих викликів (які були відчутні ще в 2014 році) стали ті, що стосувалися методичних рекомендацій розслідування відмінних злочинів від воєнних. Адже насправді воєнні злочини значно різняться від інших видів злочинів. У зв'язку з цим, слідчим, прокурорам та оперативним працівникам знадобилося поглиблювати знання в абсолютно різних напрямках: в сфері балістики (як у випадку артилерійських чи ракетних обстрілів), хімії (як у випадку можливих злочинів на ЗАЕС), військової техніки та доктрини військового командування, збору інформації з відкритих джерел та інших сферах. Наприклад, після підриву Каховської ГЕС, для оцінки наслідків катастрофи, слідчим та прокурорам довелося заглибитися в сфери біологічних, екологічних та орнітологічних даних; досліджувати не лише прямі наслідки такої шкоди зараз, але й непрямі наслідки, що можуть стати в майбутньому, аби якомога краще довести злочинний намір ворога, в поєднанні з військовими цілями та наприклад, воєнною перевагою, які може нести та чи інша тактика на полі бою та впливати на цивільне населення. Звісно, можна заперечити, що слідчий не має бути експертом в хімічній, біологічній чи орнітологічній сфері, однак, так чи інакше, він має розумітися на загальних аспектах більше, ніж пересічний громадянин, особливо це стосується питань військової доктрини та використання зброї, що є вкрай важливим для якісного доведення злочинного наміру під час розслідування воєнних злочинів. До того ж, не менш важливим залишається аспект обміну досвіду з іншими країнами, зокрема континентів Африки та Азії, які так само переживало міжнародні збройні конфлікти, в тому числі проти Росії та в тому числі відчували (і досі відчувають) екологічні наслідки.

Іншим викликом стало те, що в більшості справ у слідчих немає можливості фактично потрапити на місце злочину. Часто це пов'язано або ж з прямою небезпекою для їх життя та здоров'я, або взагалі з відсутністю такої можливості. Звісно, це прямо впливає на можливість збору доказів чи огляду місця події, а також на необхідність діяти швидко та під психологічним тиском, що звісно впливає на прийняття тих чи інших рішень в розслідуванні кримінальних справ.

Фактично, це чи не найгостріші проблеми, на які варто звернути увагу та запропонувати шляхи їх вирішення. Звісно ж що комбінування практичних та теоретичних здобутків могли б дати в цьому аспекті найкращий результат, та могли б втілитися в різноманітних навчально-тренінгових матеріалах, посібниках, курсах, методичних рекомендаціях тощо.

Окремим блоком завжди постає питання кваліфікації злочинів, які вчиняються в умовах збройного конфлікту. Адже в умовах бойових дій ряд злочинів, включаючи вбивство або грабіж, за загальним правилом кваліфікується за ст. 438 КК України. Вони "не потребують додаткової кваліфікації за статтями про умисне вбивство, згвалтування, торгівлю людьми, насильницьке зникнення, катування, заподіяння тілесних ушкоджень, знищення майна тощо» [3]. Не менш важливим елементом під час розслідування воєнних злочинів та встановлення будь яких фактів

щодо збройного конфлікту є відкриті джерела. Масштабність конфлікту настільки всеосяжна географічно та відбувається з залученням такого кола осіб, що інформація щодо нього просто не може не потрапити у відкриту мережу – Інтернет. І тут варто розуміти, що це такий масив даних, який вже неможливо осягнути швидко, а в поєднанні з інформацією яка була доступна в мережі раніше – це вже обсяг який просто неможливо опрацювати фізично будь кому загалом. Знайти необхідну інформацію, яка може справді стати доказом, можливо лише в тому випадку, якщо слідчому чи оперативному співробітнику відомо точно де знаходиться та інформація яку він намагається знайти, або він володіє спеціальними техніками та програмним забезпеченням для сортування та пошуку. Однак, звісно є й позитивні елементи які стосуються збору інформації з відкритих джерел спричинені масштабністю конфлікту. Зокрема це пов'язано з тим, що під час збройного конфлікту, підрозділам що здійснюють військові операції, досить складно приховати власні переміщення чи перебування в тому чи іншому населеному пункті, особливо в щільній цивільній забудові, особливо під час такого стрімкого розвитку цифрових технологій та засилля камер, засобів стеження, розвідувальних супутників та інших технологій, що постійно фільмують чи фіксують певні дані, вже не кажучи про спеціальні військові технічні засоби та ті розробки що мають спеціалісти сил оборони України. Це в свою чергу означає, що так чи інакше, людство матиме в певному місці, під назвою "Інтернет" якусь важливу інформацію, яку так чи інакше хтось матиме змогу знайти чи опрацювати, а значить і злодій понесе справедливе покарання, а жертва отримає сатисфакцію.

Така велика кількість відкритих даних, що можуть бути знайдені у відкритих джерелах призвели до популяризації концепції або ж методології, під назвою: "розвідка у відкритих джерелах», або як її наразі називають – «OSINT». Фактично, це діяльність направлена на пошук будь якої інформації у відкритих джерелах (сайтах, базах, ресурсах тощо). Звісно що в нашому контексті мова буде йти не про будь-яку інформацію, а ту, яка надалі може бути використана як доказ в рамках певного кримінального провадження. Тобто, така інформація повинна містити допустимі та належні фактичні дані, зібрані у передбаченому порядку, як того вимагає глава четверта Кримінально-процесуального кодексу України та низка міжнародно-правових актів та стандартів міжнародних організацій та органів правосуддя.

При цьому, варто завжди пам'ятати, що в зборі навіть чутливої інформації з відкритих джерел часто немає нічого протизаконного, звісно, якщо ми говоримо лише про процес збору і користуємося лише відкритими джерелами, а в подальшому не використовуємо це в протизаконних цілях. Звісно за інших умов ми можемо дійти дещо іншого висновку. Варто також конкретизувати, що коли ми згадуємо термін OSINT, то мова йде про збір інформації з певною метою, яка також не буде суперечити нормам чинного законодавства чи певним морально-етичним правилам.

Найчастіше, інформація зібрана з відкритих джерел зберігається на електронних носіях чи в мережі Інтернет та існує в електронному вигляді (як файл чи веб-сторінка). При цьому, українське кримінально-процесуальне законодавство не має чітко визначеного поняття «електронного доказу». Однак, це поняття добре досліджене в науковій доктрині такими науковцями як Ахтирська Н.М., Неділько Я.В., Коваленко А.М., Сіренко О.В. Звісно, окремим блоком може стояти питання дослідження поняття електронного носія та інформації, яка на ньому зберігається, однак, це не є темою цього дослідження.

Звісно, робота з подібною інформацією вимагає її належного збирання та подальшого зберігання. Це питання не врегульоване жодним національним чи міждержавним нормативно-правовим актом прямої дії, однак існують документи "м'якого права". Один з таких, був представлений Центром прав людини Університету Берклі в Каліфорнії та Офісом Верховного комісара ООН з прав людини, під назвою «Протокол Берклі». В той же час, як може бути очевидним, він не є єдиним, оскільки існує також і інший документ, під назвою: «Керівні принципи щодо електронних доказів», представлений Радою Європи. Окрім того, існує також міжнародний стандарт ISO/IEC 27037:2017 та його національний (український) відповідник ДСТУ ISO/IEC 27037:2017. Варто відзначити, що ці документи не прийняті та не імплементовані жодним державним органом, хіба коли мова йде про ДСТУ, то прийнятий наказом ДП "УкрНДНЦ", однак яке це має практичне значення? Якщо в цей же час, як відомо з відкритих джерел, Офіс Генерального прокурора України розіслав усім регіональним підрозділам прокуратури лист-орієнтування [4], який містить інформацію про те, що слідчим під час розслідування кримінальних справ, які містять веб-дані як доказ, варто дотримуватись положень та рекомендацій Протоколу Берклі.

Насправді положення Протоколу Берклі що регулюють процес збирання інформації є доволі простими та зрозумілими для виконання. Перш за все, вони покликані полегшити роботу правоохоронних органів та забезпечити максимальну прозорість збору та зберігання, а також забезпечити існування доказу в його початковому вигляді, та в подальшому довести, що він не піддавався змінами та іншим маніпуляціям. Одним із успішних прикладів використання даних з відкритих джерел та їх належного зберігання може бути справа MH17, коли невелика команда онлайн-розслідувачів Bellingcat зібрала достатню доказову базу для видачі міжнародного ордеру на арешт офіцерського складу 53-ої зенітної ракетної бригади ППО РФ. Тієї самої що була звинувачена спільнотою в падінні літака авіарейсу MH17 на території Донецької області, в липні 2014 року. Після того як Белінгкет провели власне онлайн-розслідування – ця інформація була проаналізована та повторно зібрана спеціальною групою слідчих та експертів з різних країн та галузей. Вона більше відома як «JIT». Згодом, зібрані матеріали стали не лише доказом у справі, але й створили еталонний приклад для подібних справ, що базуються на OSINT-доказах.

Наразі Bellingcat можна приводити як приклад і в інших аспектах їх роботи, адже вони також неодноразово заявляли, що дотримуються вже згаданого міжнародного стандарту ISO 27037:2017 та протоколу Берклі. На практиці це означає наступне:

- вся зібрана інформація повинна мати чітко зафіксований час та дати архівування;
- веб сторінки мають зберігатися не як html-сторінка, а як ціла сукупність файлів та/або в форматі .pdf, в залежності від типу сторінки та цілей збору такої інформації;
- має відбуватися збереження метаданих та фіксація геш сум.

Звісно ми не знаємо напевне, яких саме стандартів дотримуються організації-лідери, однак припускаємо, що найвищих, адже їм вкрай необхідне використання таких матеріалів в подальшому, в міжнародних судах. Ця теза може також звучати логічною в контексті того, що протокол Берклі рекомендує слідувати правилам, де дії розслідувача мають відповідати ситуації. Саме тому протокол Берклі рекомендує виокремлювати лише важливу інформації під час розслідування та систематизувати її лише з основною метою: надати тільки цінні дані, а не усі, що можуть міститися в Інтернеті.

Такий успіх породив в рамках кримінальних проваджень вкрай сильну необхідність в окремих спеціалістах – OSINT-розслідувачах – професіоналах, що володіють OSINT інструментами, техніками збору, обробки та зберігання даних, які після збору та обробки/аналізу можуть бути доказами в рамках кримінального провадження. Насправді такі спеціалісти вже є, і часто вони навіть не є юристами за фахом (аби краще оцінювати результати власної роботу в рамках КП), проте, незважаючи на це, слідчі все одно гостро потребують їх залучення до справи, в якості спеціалістів. Адже відповідно до вже згаданого Протокол Берклі є надзвичайно важливий аспект, що в разі порушення алгоритму збору інформації слідчими, надалі знайдена інформація може не відповідати найвищим стандартам збору доказів. А отже, вся робота буде марною і не буде прийнятою національним чи міжнародними судовими інституціями. Це означає, що з одного боку, слідчі повинні підвищувати власні навички володіння відповідними техніками та методиками збору інформації з відкритих джерел, аби бути менш залежними від третіх осіб, однак, в той же час, OSINT-аналітики/розслідувачі мають підвищувати власний рівень юридичної обізнаності.

Таким чином OSINT вже зарекомендував себе як дієвий метод. Володіючи інструментами з переліку OSINT можна дістати певну чутливу та досить важливу інформацію для цілей кримінального переслідування. Наприклад: номер мобільного телефону, поштову скриньку чи навіть паспортні дані для винесення підозри. Особливо актуальними такі можливості можуть бути в рамках кримінальних проваджень, де коло підозрюваних є недоступними фізично для слідства. Це стає можливим завдяки всім ти даним, що люди залишають про себе в мережі Інтернет. При цьому в широкому сенсі, тобто в різноманітних застосунках, сервісах, соціальних мережах і не лише публічно. Також до роботи часто підключаються можливості штучного інтелекту, який є скоріше методом збору або методом прискорення такого збору для слідчого. Для наочності, ви можете проаналізувати тексти підозр Офісу генерального прокурора. Там ви побачите, наскільки чіткими та точними є вказані персональні дані, які стосуються як офіцерського, так і рядового складу підозрюваних. Там можна побачити номери паспортів, індивідуальні податкові номер чи навіть місце реєстрації або народження. Майже у 80% випадків такі дані отримуються саме завдяки відкритим джерелам, а не оперативним чи іншим можливостям правоохоронців.

На просторах різноманітних кібер спільнот часто ширится думка що, американська розвідка отримує від 35% до 95% розвідданих саме з відкритих джерел, витрачаючи на це лише 1% розвідувального бюджету США. Ми не будемо оцінювати наскільки ця теза правдива та достовірна в рамках цього дослідження. Однак, абсолютно очевидно, що на це варто звертати особливу увагу, як керівникам слідчих та розвідувальних управлінь різноманітних державних установ, так і законодавцю для правильного інкорпорування цих методик в українське законодавство, можливо навіть під грифом таємності. Адже саме законодавчі органи повинні створити сприятливі умови для розвитку подібних методик в умовах воєнного часу та їх правове використання повсякчас.

Повертаючись до питання можливості, доцільності та ефективності залучення осіб з окремими, спеціальними та особливими знаннями щодо OSINT, треба сказати, що насправді цей процес вже давно обговорюється науковцями та практиками. Фактично ж, ті самі слідчі вже певний час активно залучають окремих OSINT розслідувачів, правозахисників, приватних спеціалістів до відповідних процесуальних дій. Переважно в якості процесуального статусу "спеціаліста", особливо для отримання висновків щодо розслідування злочинів пов'язаних з порушенням законів та звичаїв ведення війни. Однак, тут також є певна юридична проблема, яка полягає в законодавчій прогалині, адже в частині 2, статті 84 КПК, в якій вказаний вичерпний перелік джерел доказів, немає висновку спеціаліста, водночас, є висновок експерта. Звісно це не означає, що дані отримані слідчим чи прокурором під час кримінального провадження від спеціаліста не будуть братись до уваги, однак, досить дивним виглядає така "інклюзія" законодавця по відношенню до спеціаліста, яку варто було б усунути або пояснити.

При цьому саме поняття "спеціаліст" законом передбачене. Вказано, що він є процесуальною особою, і несе відповідальність згідно з статтею 72 КПК України, аналогічно з іншою процесуальною особою, а саме, експертом, якому присвячено цілий розділ. Наразі ще одним важливим рішенням було б вирівняти подібну процесуальну нерівність. Це можливо зробити, якщо "вирівняти" спеціаліста та експерта в правах, або об'єднати ці два поняття в одного суб'єкта кримінального процесу, хоча, це звісно може викликати певні дискусії та потребувати додаткового врегулювання та обговорення. Таке рішення може залежати від волі законодавця та тої концепції реформування кримінально-правової політики, перевагу якій надає держава, що ж стосується самих концепцій, то їх напрацьовано чимало і кожна заслуговує на увагу, однак, не обов'язково прийняття.

Насамперед, саме слідчий та процесуальний керівник будуть нести відповідальність за кінцевий результат, а тому, доцільність залучення спеціаліста, експерта чи інших осіб, які можуть володіти спеціальними знаннями має бути саме їх рішенням. Ключовим в таких питаннях завжди є експертність особи, досвідченість, знання та інші переваги, а не лише її юридична можливість набувати процесуальний статус експерта.

Висновки. У результаті проведеного дослідження встановлено, що використання інформації з відкритих джерел стало важливою складовою розслідування воєнних злочинів в умовах обмеженого доступу до місць подій та великого обсягу цифрових даних. Водночас, наявні в українському кримінальному процесуальному законодавстві правові прогалини, зокрема щодо статусу електронних доказів і спеціалістів-OSINT-аналітиків, значно ускладнюють повноцінне використання такого типу інформації як належного доказу.

Автор дійшов висновку, що інтеграція міжнародних стандартів, таких як Протокол Берклі та ISO/IEC 27037:2017, у національну правову систему є необхідною умовою для забезпечення достовірності та допустимості цифрових доказів. Також доцільним є оновлення кримінального процесуального кодексу з метою офіційного визнання висновків спеціалістів-розслідувачів, які володіють інструментами OSINT. Це дозволить суттєво підвищити ефективність документування фактів збройної агресії, ідентифікації підозрюваних, збирання доказів та формування правових позицій у міжнародних судах.

Таким чином, мета дослідження – розробити рекомендації щодо правового врегулювання та методичного забезпечення роботи з відкритими джерелами – була досягнута. Результати мають як наукову, так і практичну цінність для органів досудового розслідування, прокуратури, суду, а також для наукової спільноти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Міністерство внутрішніх справ України. Російські воєнні злочини: оновлені дані станом на 31 січня 2025 року. URL: https://mvs.gov.ua/news/zlocini-vcineni-viiskovimi-rf-pid-cas-povnomasstabnogo-vtorgnennia-v-ukrayinu-stanom-na-31012025.
2. Верховна Рада України. Верховна Рада України ратифікувала Римський статут Міжнародного кримінального суду та поправки до нього. Прес-служба Апарату Верховної Ради України. URL: https://www.rada.gov.ua/news/razom/252711.html.
3. Тренінговий центр прокурорів України. Кваліфікація воєнних злочинів за Кримінальним кодексом України. URL: https://ptcu.gp.gov.ua/uk/czentr-znan/intervyu-z-treneramy/kvalifikacziya-voyennyh-zlochyniv-za-kryminalnym-kodeksom-ukrayiny.
4. Офіс Генерального прокурора. Лист-орієнтування від 28.08.2021 № 18/1-386 Керівникам обласних прокуратур «Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел». URL : https://zakononline.com.ua/documents/show/500229___686193.
5. Безпалько У. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання) . *Вісник Ужгородського національного університету*. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/289572/283146.