7. Кримінологія : навч.-метод. посібник / Л. І. Аркуша, Н. О. Федчун, В. Я. Цитряк, Л. В. Чорнозуб. НУ «ОЮА». Одеса : Бондаренко М. О., 2023. 68 с.
8. Кримінологія: навч.-метод. посібник / Г. З. Яремко, Н. І. Устрицька. Львів : ЛьвДУВС, 2018. 144 с.

DOI https://doi.org/10.30525/978-9934-26-645-4-68

OSINT AS A TOOL FOR PROVING WAR CRIMES

OSINT ЯК ІНСТРУМЕНТ ДОКАЗУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

Formanchuk Andrii
cadet of the 308th training platoon, faculty of training specialists for pre-trial investigation bodies of the National Police of UkraineНауковий керівник: Scientific advisor: Morozov Demyd Candidate of Law, Associate Professor, Professor of the Department of Operational and Investigative Activities, Odessa State University of Internal Affairs Odesa, Ukraine

Форманчук Андрій
курсант 308-го навчального взводу, факультет підготовки фахівців для органів досудового розслідування Національної поліції України Науковий керівник: Морозов Демид кандидат юридичних наук, доцент, професор кафедри оперативно-розшукової діяльності, Одеський державний університет внутрішніх справ м. Одеса, Україна

Сучасні збройні конфлікти супроводжуються численними порушеннями міжнародного гуманітарного права та воєнними злочинами, доказування яких є ключовим для притягнення винних до відповідальності. В умовах обмеженого доступу до традиційних джерел інформації важливу роль набуває OSINT (Open Source Intelligence) – розвідка з відкритих джерел – являє собою процес збору, аналізу та верифікації інформації з публічно доступних джерел, включаючи соціальні мережі, супутникові знімки, відеозаписи, фотографії, метадані та інші цифрові дані. У контексті розслідування воєнних злочинів, як один із гласних оперативно-розшукових заходів, OSINT стає потужним інструментом документування порушень міжнародного гуманітарного права,

дозволяючи фіксувати докази навіть у випадках, коли доступ до місця події обмежений або небезпечний.

Використання OSINT у правозахисній діяльності та кримінальному розслідуванні сприяє оперативному отриманню доказів, перевірці фактів та формуванню переконливих матеріалів для суду. Особливу актуальність цей інструмент набуває у воєнних конфліктах, де доступ до зони бойових дій часто обмежений, а традиційні методи збору доказів є небезпечними або неможливими.

Розслідування воєнних злочинів із застосуванням OSINT ґрунтується на широкому спектрі методів збору інформації. Сюди входить моніторинг соціальних мереж, таких як Facebook, Twitter, Telegram, ВКонтакте, Одноклассники, для виявлення відео та фотографій з місць подій, аналіз супутникових знімків руйнувань, зіставлення геолокацій та часових міток, а також пошук інформації про військових у відкритих реєстрах. Наприклад, міжнародні журналістські групи «Bellingcat» використовують відеозаписи з різних ракурсів та супутникові знімки для відтворення хронології атак і встановлення відповідальних осіб чи підрозділів [1, с. 115].

Цифрові докази можуть бути легко фальсифіковані або маніпульовані. Тому критично важливою є процедура верифікації, яка включає аналіз метаданих, геолокацію, перевірку часових міток, перехресну верифікацію з іншими джерелами. Берклійський протокол встановлює структурований шестиетапний цикл розслідування, що перетворює випадковий пошук у методологічно обґрунтований процес збору доказів [2].

З початку повномасштабного вторгнення рф у лютому 2022 року світ став свідком безпрецедентного використання OSINT для документування воєнних злочинів. Дослідження Королівського інституту об'єднаних служб (RUSI) показало, що мережа OSINT-практиків в Україні включає щонайменше 19 розслідувальних команд, 9 академічних центрів, 17 IT-проєктів і 39 організацій громадянського суспільства, які документують потенційні воєнні злочини [3]. Ця «мережа підзвітності», як її назвали на конференції United for Justice у Львові в березні 2023 року, створює комплексну систему збору доказів.

Збирання, перевірка та оцінка цифрових даних, які містять докази воєнних злочинів, скоєних під час збройної агресії на території України, є надзвичайно складним процесом. Цей процес включає технічні, етичні та правові аспекти, що потребують застосування різних стратегій для їх ефективного вирішення. Величезний обсяг цифрового контенту, що створюється під час війни в Україні, включно з відеозаписами, фотографіями та публікаціями у соціальних мережах, формує нові виклики щодо збору та фіксації інформації. Забезпечення

автентичності та збереження таких даних у умовах хаосу, що супроводжує неоголошену війну, є критично важливим і надзвичайно складним завданням. Виявлення справжніх доказів серед шахрайського чи фальшивого контенту стає все складнішим завданням. У сучасних умовах отримання достовірної інформації у найкоротший термін необхідне не лише для потреб Збройних сил України, але й для підрозділів Національної поліції, Служби безпеки України та інших органів, які здійснюють підслідність. Саме тому правоохоронні органи все частіше застосовують технологічні методи збору інформації, а також методи OSINT у своїй роботі.

Згідно зі статтею 1 Закону України «Про інформацію», інформація – це будь-які відомості та/або дані, які можуть зберігатися на матеріальних носіях або у електронній формі. Тобто законодавець відносить до сутності інформації саме дані або відомості, перероблені у певну форму подання, а не знання про факти чи події як такі [4, с. 24].

Використання OSINT дозволяє отримувати доступ до електронних даних, включно з листуванням, документами або іншими електронними записами, які можуть стати доказовою базою у кримінальних провадженнях щодо воєнних злочинів. За допомогою OSINT також можливо ідентифікувати осіб, причетних до злочинів, та притягнути їх до відповідальності.

Головною проблемою у використанні OSINT-матеріалів у досудовому провадженні та в суді є необхідність підтвердити їхню достовірність. Оскільки цифрові дані легко піддаються спотворенню, підробленню (зокрема через технології deepfake) чи навмисному поширенню неправдивої інформації, кожен такий матеріал має проходити детальну перевірку. Додатковою складністю є забезпечення належного «ланцюга безперервного володіння» (chain of custody). Слідству потрібно довести, що файл, поданий у суді, ідентичний тому, який був знайдений у відкритому джерелі, і що в нього не вносилися будь-які зміни. Для цього застосовують криптографічні інструменти, зокрема хеш-функції (наприклад, SHA-256), які дають змогу зафіксувати унікальний цифровий відбиток файлу на момент його отримання [5, с. 238].

У контексті українського кримінального процесу використання OSINT-матеріалів потребує особливої уваги. На відміну від Цивільного, Господарського процесуальних кодексів та Кодексу адміністративного судочинства України, Кримінальний процесуальний кодекс України не містить окремих положень щодо електронних доказів [6, с. 172]. Проте OSINT-матеріали можуть бути імплементовані в процесуальний простір через вже наявні інститути: речові докази (стаття 98 КПК України), документи (стаття 99 КПК України), висновки експертів (стаття 101 КПК України) та протоколи слідчих дій [7].

Підводячи підсумки, можемо зазначити, що OSINT як інструмент доказування воєнних злочинів має подвійне значення: він є джерелом нових доказів і водночас механізмом швидкого реагування на порушення міжнародного гуманітарного права. Використання OSINT вимагає суворого дотримання міжнародних стандартів, встановлених Берклійським протоколом, забезпечення належної верифікації даних та координації між національними і міжнародними органами правосуддя.

Література:

1. Колесников М. OSINT у розкритті воєнних злочинів. Роль OSINT-досліджень у підвищенні рівня національної безпеки України : матеріали круглого столу (м. Львів, 7 травня 2025 р.) / укладач І. О. Ревак. Львів : ЛьвДУВС, 2025. С. 114–116. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/8875/1/07_05_2025.pdf

2. Setting standards for digital investigations in the age of open source intelligence. *Andrea Fortuna*. 2024. URL: https://andreafortuna.org/2025/11/05/setting-standards-for-digital-investigations-in-the-age-of-open-source-intelligence

3. Puzzling Pieces: OSINT and War Crime Accountability in Ukraine. *Royal United Services Institute*. 2024. URL: https://www. rusi.org/explore-our-research/publications/commentary/puzzling-pieces-osint-and-war-crime-accountability-ukraine

4. Бакумов О. С., Марчук М. І., Гудзь Т. І., Венглінський О. О. Інформація: до питання про змістову еволюцію терміна. *Право і безпека – Law and Safety*. 2021. No 3 (82). С. 19–28. URL: https://pb.univd.edu.ua/index.php/PB/article/view/494/385

5. Лісніченко Д. В. Використання даних з медіа та відкритих джерел (OSINT) у процесі доказування у кримінальних провадженнях. *Право та державне управління*. 2025. № 1. С. 234–239. URL: https://doi.org/10.32782/pdu.2025.1.32 (дата звернення: 27.11.2025).

6. Музиченко О. В., Карандась, М. В. Електронні докази як джерела доказів у межах кримінального провадження: судова практика та нормативне регулювання інших процесуальних кодексів України. *Київський часопис права*. 2022. № 3. URL: https://kyivchasprava.kneu.in.ua/index.php/kyivchasprava/article/view/179

7. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 року № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 27.11.2025).