Яцур Павло Олександрович,
здобувач вищої освіти Навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ
Науковий керівник:
Патик Леся Леонідівна,
доцент кафедри криміналістики та судової медицини Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ВИКОРИСТАННЯ ЦИФРОВИХ ДОКАЗІВ І ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ В КРИМІНАЛІСТИЧНОМУ ЗАБЕЗПЕЧЕННІ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

Використання цифрових доказів та відкритих джерел інформації (OSINT – Open Source Intelligence, тобто розвідки на основі відкритих джерел) стало одним із найважливіших інструментів криміналістичного забезпечення розслідування воєнних злочинів, вчинених у ході збройної агресії Російської Федерації проти України. Особливість сучасних злочинів полягає в тому, що значна частина слідів подій фіксується не лише традиційними методами (огляд місця події, вилучення речових доказів тощо), а й у цифровому середовищі – на відео з камер спостереження, у записах камер спостереження на об'єктах інфраструктури, у публікаціях у соціальних мережах, на супутникових знімках, у даних геолокації мобільних пристроїв. Ці матеріали дають змогу встановлювати точний час, місце та обставини вчинення злочину, ідентифікувати причетних осіб та збройні підрозділи, а також підтверджувати характер завданих пошкоджень. У поєднанні з класичними криміналістичними методами цифрові та OSINT-дані формують комплексну доказову базу, яка має вагоме значення не лише для національного кримінального провадження, але й для міжнародного правосуддя.

Практика Верховного Суду вже закріпила допустимість використання цифрових доказів та матеріалів з відкритих джерел інформації за умови дотримання процесуальних вимог їх отримання. Так, у касаційній скарзі захисник стверджував про недостовірність і недопустимість таких доказів, як скриншоти

інтернет-сторінок, відеофайли, завантажені з мережі «Інтернет». В свою чергу Касаційний кримінальний суд у складі Верховного Суду в постанові від 12 червня 2024 року у справі № 569/1908/23 (провадження № 51-1430км24) прямо зазначив, що електронні (цифрові) докази з відкритих джерел – інтернет-ресурсів, засобів масової інформації, соціальних мереж – можуть бути основними доказами у кримінальних провадженнях щодо злочинів проти основ національної безпеки, якщо їх отримано процесуально належним чином. У цьому рішенні як докази було прийнято скріншоти та відеофайли з мережі, долучені як додатки до протоколів огляду, складених на виконання доручення слідчого відповідно до статті 40 Кримінального процесуального кодексу України [1]. У мотивувальній частині рішення детально описано, що було здійснено огляд інтернет-сторінок, зняття скріншотів, завантаження відео та долучення цих матеріалів до протоколів огляду, що забезпечило їх процесуальну належність та доказову силу. Така позиція Верховного Суду фактично закріплює можливість повноцінного використання даних з відкритих джерел у кримінальному провадженні, якщо вони оформлені відповідно до передбачених процедур[2].

На практиці одним із найважливіших джерел цифрових доказів стали публікації у відкритих джерелах, зокрема соціальних мережах, месенджерах та незалежних медіа. OSINT-дані – це інформація, яка знаходиться у вільному доступі і може бути перевірена, систематизована та використана як допоміжний доказовий матеріал. Супутникові знімки високої роздільної здатності дозволяють встановити час та масштаби руйнувань цивільних об’єктів, фото- та відеоматеріали очевидців дають змогу ідентифікувати конкретні одиниці техніки, форми ураження будівель, типи боєприпасів, а також присутність військових підрозділів у певному районі. Цінність таких даних полягає в їхній часовій прив’язці та об’єктивності: супутникові знімки мають фіксовані метадані, а публікації в соціальних мережах часто містять автоматично збережену геолокацію та часові мітки [4]. Саме завдяки OSINT-розслідуванням у низці випадків вдалося встановити траєкторії ракет, місця пуску та конкретні військові підрозділи, причетні до обстрілів цивільних об’єктів.

Ще одним важливим орієнтиром у судовій практиці щодо використання цифрових доказів та OSINT-даних є підхід Верховного Суду до оцінки матеріалів, зібраних аналітичними та оперативними підрозділами. У своїх узагальненнях за червень

2024 року Суд окремо звернув увагу на те, що матеріали з відкритих і закритих інформаційних мереж, зібрані уповноваженими підрозділами з дотриманням процесуальних вимог, є документами у розумінні статті 99 КПК України [1]. Такі матеріали можуть містити результати аналітичної обробки, у тому числі дані супутникової зйомки, скріншоти вебсторінок, відеозаписи з мережі, зведені в єдиний аналітичний звіт. Верховний Суд підтвердив, що ці звіти, якщо вони складені на підставі належно зафіксованих джерел та містять відомості, які можна перевірити, мають повноцінну доказову силу в кримінальному провадженні [2]. Це безпосередньо стосується роботи аналітичних підрозділів Національної поліції, зокрема Департаменту кримінального аналізу, який системно збирає й опрацьовує цифрові та відкриті джерела, формуючи офіційні аналітичні звіти для долучення до матеріалів кримінальних проваджень. Судова практика фактично закріпила цей формат як процесуально допустимий та доказово значимий елемент, що забезпечує інтеграцію цифрових та OSINT-даних у структуру доказової бази у кримінальних провадженнях про воєнні злочини.

Важливим аспектом роботи з цифровими та OSINT-доказами є перевірка достовірності та верифікація джерел. У сучасних умовах поширення великої кількості дезінформації особливого значення набуває встановлення автентичності фото- і відеоматеріалів. Для цього використовуються методи аналізу метаданих, співставлення з іншими незалежними джерелами, геолокаційна верифікація, порівняння архітектурних та природних об’єктів на зображеннях, визначення погодних умов на момент фіксації [4]. Наприклад, за допомогою зіставлення форми дахів, тіней та елементів ландшафту можна точно визначити місце зйомки. Такі методи вже широко застосовуються міжнародними слідчими органами та журналістськими розслідувальними групами, а українські аналітики поступово інтегрують їх у свою щоденну роботу.

Використання цифрових та OSINT-доказів особливо важливе у випадках, коли фізичний доступ до місця події обмежений або неможливий. Наприклад, під час активних бойових дій слідчі не завжди можуть оперативно прибути на місце ракетного удару чи окуповану територію для проведення огляду. У таких ситуаціях цифрові матеріали стають єдиним способом задокументувати події та зберегти інформацію, необхідну для подальших експертних досліджень і судового

розгляду [3]. Ці докази дозволяють формувати хронологію подій, встановлювати відповідальних осіб та доводити системний характер атак на цивільні об'єкти, що має ключове значення для кваліфікації злочинів як воєнних.

Разом із тим існують і проблеми, які потребують поступового вирішення. Серед основних – необхідність уніфікації стандартів збору та оформлення цифрових доказів, підвищення кваліфікації слідчих та аналітиків у сфері цифрової криміналістики, а також технічне забезпечення для збереження великих обсягів даних із гарантією їх автентичності. Перспективи розвитку полягають у подальшому розвитку роботи аналітичних підрозділів, розбудові партнерства з міжнародними структурами, впровадженні єдиних стандартів збирання та перевірки цифрових матеріалів, а також інтеграції інноваційних інструментів штучного інтелекту та автоматизованих систем пошуку.

Таким чином, використання цифрових доказів та даних з відкритих джерел є сьогодні невід'ємною складовою криміналістичного забезпечення розслідування воєнних злочинів. Поєднання класичних слідчих (розшукових) дій з аналітичними можливостями цифрової епохи забезпечує побудову повної та надійної доказової бази, яка має значення не лише для національного правосуддя, але й для міжнародних судових процесів.

Список використаних джерел

1. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. *Відомості Верховної Ради України.* 2013. № 9–13. Ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 10.10.2025).

2. Огляд судової практики Касаційного кримінального суду у складі Верховного Суду: Вип. 06/2024. Київ : Верховний Суд України, 2024. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/ogliady/Oglyad_KKS_06_2024.pdf (дата звернення: 10.10.2025).

3. Прокопенко Н. М. Методи та криміналістичний аналіз цифрових доказів: виклики та інновації. *Правові новели*. 2023. № 12. URL: http://www.legalnovels.in.ua/journal/21-2_2023/21-2_2023.pdf#page=12 (дата звернення: 10.10.2025).

4. OSINT як доказ у розслідуванні воєнних злочинів: представники ВС взяли участь у тематичному семінарі. *Прес-реліз Верховного Суду України.* URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1883443?utm_source (дата звернення: 23.09.2025).