УДК 343.1
DOI: https://doi.org/10.17721/1728-2195/2025/2.130-7

Олена КОСТЮЧЕНКО, канд. юрид. наук, доц.
ORCID ID: 0000-0002-2243-1173
e-mail: olena_kostiuchenko@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Андрій ШЕВЦОВ, асп.
ORCID ID: 0009-0006-2080-5561
e-mail: andriishevtsov@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

# ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ (OSINT) ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ ПРОТИ ЛЮДЯНОСТІ

**В с т у п .** *У сьогоденні, коли цифрові технології проникають у всі сфери життя, відкриті джерела інформації, відомі як OSINT (Open-Source Intelligence), стали невід'ємним складником сучасного розслідування злочинів проти людяності. Ці дані часто стають незамінними в процесі кримінального переслідування, особливо у випадках, коли інші джерела інформації недоступні або обмежені. Проте для того, щоб матеріали, отримані через OSINT, могли бути використані як докази, необхідно розв'язати низку складних проблем, які стосуються їх достовірності, автентичності та допустимості.*

**М е т о д и .** *У роботі використано такі методи, як-от: порівняльно-правовий (зіставлення стандартів допустимості доказів, сформованих у практиці Міжнародного трибуналу щодо колишньої Югославії, чи Міжнародного кримінального суду й української практики); нормативно-правовий аналіз (вивчення законів, міжнародних угод і інструкцій щодо OSINT); аналіз судової практики в Україні, яка перебуває на етапі формування підходів до використання OSINT у кримінальному процесі; інтерпретаційно-правовий (тлумачення процесуальних норм у контексті OSINT); системний юридичний підхід (інтеграція виявлених норм у рекомендації для українського кримінального процесу).*

**Р е з у л ь т а т и .** *У ході дослідження виявлено три ключові проблеми застосування OSINT у розслідуваннях злочинів проти людяності. По-перше, відсутність єдиних законодавчих стандартів і методик збирання цифрових доказів призводить до розбіжностей у процедурах різних юрисдикцій і ускладнює визнання таких доказів у суді. По-друге, без чітко визначених процедур верифікації (геолокація, аналіз метаданих, порівняння супутникових знімків) зібрані дані часто не витримують критики щодо автентичності. По-третє, у зонах активних бойових дій традиційні засоби документування є недостатніми, тоді як OSINT дає змогу відтворити хронологію подій і підтвердити місцезнаходження об'єктів злочину навіть за обмеженого доступу.*

**В и с н о в к и .** *Для підвищення ефективності OSINT у кримінальному провадженні необхідно розробити комплексні методики, які враховували б не лише технічні аспекти роботи з даними, але й етичні та правові обмеження. Наприклад, важливим є запровадження стандартів для документування процесу збирання інформації – від фіксації джерела до процедур перевірки. Без таких механізмів слідчі та прокурори залишаються у вразливому становищі, адже допустимість результатів процесуальних дій може бути оспорена на етапі судового розгляду. Лише міждисциплінарний підхід дасть змогу забезпечити належну якість розслідувань та ефективне притягнення до відповідальності осіб, які вчинили найтяжчі міжнародні злочини.*

**К л ю ч о в і  с л о в а :** *OSINT, злочини проти людяності, досудове розслідування, відкриті джерела, докази, електронні докази, документи.*

## Вступ

Сучасні міжнародні збройні конфлікти, які охоплюють окремі регіони світу, залишають за собою тяжкі наслідки у вигляді масових порушень норм міжнародного гуманітарного права та численних злочинів проти людяності. Ці злочини, серед яких умисні вбивства, депортація населення, катування та сексуальне насильство, вимагають негайного документування, розслідування і покарання винних. Однак реалії воєнного часу створюють значні перешкоди для традиційних методів збирання доказів. Допити свідків часто ускладнені через небезпеку для життя або відсутність доступу до постраждалих територій, а огляд місця події стає неможливим через активні бойові дії, мінування або окупацію. На цьому тлі використання OSINT (розвідки з відкритих джерел) набуває особливого значення. Завдяки даним із соціальних мереж, супутниковим знімкам, відеозаписам, публікаціям у ЗМІ та іншим доступним ресурсам можна відтворити картину подій навіть за відсутності прямого доступу до місця злочину. Однак OSINT як джерело доказів породжує нові виклики – як забезпечити автентичність таких даних? Як довести їхню достовірність і відповідність до вимог допустимості, закріплених у кримінальному процесуальному законодавстві? В Україні ці питання ще не знайшли належного правового врегулювання, що значно ускладнює використання відкритих джерел у судових провадженнях.

***Аналіз останніх досліджень і публікацій.*** Проблематика OSINT активно досліджується як науковцями, так і практиками. Зокрема, серед українських дослідників, що торкались цього питання, слід відзначити Калугіна В. Ю., Костюченко О. Ю., Сіфорова О. І., Ругала Ю., Косохатька Б. С., Торбаса О. О. Їхні роботи охоплюють аспекти збирання та аналізу інформації з відкритих джерел, зокрема в умовах гібридних війн і збройних конфліктів. На міжнародному рівні вагомий внесок у розвиток OSINT зробили експерти таких організацій, як Bellingcat, Human Rights Watch, Міжнародний кримінальний суд та ООН. Вони розробили методології збирання цифрових доказів, зокрема підтвердження їх автентичності через геолокацію, порівняння метаданих і аналіз супутникових зображень. Попри значні напрацювання, у працях як українських, так і зарубіжних дослідників залишаються нерозкритими питання правового регулювання використання OSINT у кримінальному процесі України.

***Метою статті є*** визначення ключових теоретичних і практичних аспектів використання OSINT під час розслідування злочинів проти людяності.



ISSN 1728-3817

Зокрема, увага зосереджується на аналізі міжнародних стандартів щодо збирання, перевірки й оцінювання цифрових доказів. Водночас автори мають намір запропонувати конкретні рекомендації для вдосконалення національної законодавчої бази. Це передбачає створення чітких правових механізмів, які б регулювали процесуальне використання інформації з відкритих джерел, забезпечуючи її допустимість як доказів у кримінальних справах. Зрештою, у статті робиться спроба знайти баланс між потребою у швидкому документуванні злочинів, вчинених у надзвичайно складних умовах, і дотриманням правових стандартів, необхідних для об'єктивного розгляду таких справ у суді.

**Методи**

Дослідження будується на поєднанні кількох взаємопов'язаних методів: порівняльно-правовому аналізі стандартів допустимості доказів у практиці Міжнародного трибуналу щодо колишньої Югославії та Міжнародного кримінального суду із зіставленням цих стандартів із поточною судовою практикою в Україні; аналітичному методі, що включає огляд і систематизацію підходів міжнародних організацій (Bellingcat, Human Rights Watch, ООН, МКС) до збирання та оцінювання цифрових доказів; документальному аналізі наукових публікацій і методичних рекомендацій із фіксації джерел і перевірки цифрових даних; системному підході до інтеграції технічних, правових і етичних аспектів у єдину методологічну систему.

**Результати**

Військові конфлікти XXI століття, серед яких особливе місце посідає повномасштабна агресія Російської Федерації проти України, підкреслили важливість використання новітніх технологій для аналізу, збирання та збереження інформації про події, що мають кримінальне значення. У таких умовах традиційні методи розслідування виявляються недостатніми, особливо коли йдеться про документування злочинів проти людяності. Саме тому у фокусі сучасних підходів опинилася розвідка з відкритих джерел (OSINT), яка стала невід'ємним складником розслідувань міжнародних злочинів. OSINT базується на аналізі даних, отриманих із численних джерел, таких як соціальні мережі, новинні ресурси, державні звіти, блоги, форуми, відеоплатформи й супутникові знімки. Ця технологія дає змогу об'єднати розрізнені фрагменти інформації у цілісну картину, що є надзвичайно важливим у контексті документування складних злочинів, які охоплюють велику кількість постраждалих, свідків і підозрюваних. Злочини проти людяності, за своєю природою, є багатоаспектними й часто мають масовий характер, що ускладнює процес їхнього розслідування. Питання виявлення винних, притягнення їх до відповідальності та забезпечення справедливості для жертв є не лише юридичною, але й моральною та соціальною проблемою. Саме тут OSINT виявляється незамінним інструментом. Його перевага полягає у здатності швидко реагувати на події, забезпечуючи майже миттєвий доступ до великого обсягу інформації. У контексті російсько-української війни OSINT активно застосовується для збирання доказів злочинів проти людяності. Цей метод дає змогу документувати воєнні злочини навіть у тих випадках, коли доступ до місця подій є неможливим через бойові дії або окупацію. Соціальні мережі, наприклад, стали важливим джерелом даних для ідентифікації осіб, які брали участь у злочинах, або для встановлення деталей подій. Фото- та відеоматеріали, які користувачі публікують у відкритому доступі, містять численні підказки: геолокацію, часові мітки, зображення конкретних осіб або об'єктів. У поєднанні з аналітичними інструментами OSINT дає змогу встановити не лише винуватців, а й їхню роль у подіях. Один із яскравих прикладів використання OSINT – це ідентифікація військових злочинців за допомогою аналізу їхніх профілів у соціальних мережах. Фотографії, на яких зафіксовано людей у формі, з озброєнням, на тлі певної місцевості, дають змогу визначити їхнє місцезнаходження, підрозділи, до яких вони належать, і навіть командирів. У деяких випадках ці дані стають відправною точкою для побудови доказової бази, яку можна використовувати в суді. Окрім того, OSINT відіграє ключову роль у встановленні ланцюгів командування, що є критично важливим для розслідування злочинів, вчинених на системному рівні. Наприклад, супутникові знімки дають змогу документувати пересування техніки чи концентрацію військових на певних територіях, а публічні заяви посадовців – аналізувати рівень їхньої поінформованості чи причетності до прийняття рішень. Метод OSINT також допомагає виявляти зв'язки між подіями, що на перший погляд здаються розрізненими. Наприклад, дані про артилерійські обстріли можуть бути підтверджені як супутниковими знімками пошкоджених об'єктів, так і відеозаписами місцевих жителів. Усе це сприяє створенню надійної доказової бази, яка здатна витримати ретельний аналіз у суді. Однак, незважаючи на значні досягнення у використанні OSINT, цей метод залишається викликом для українського правосуддя через відсутність чітких правових механізмів щодо його процесуального оформлення. Автентичність і допустимість отриманих даних потребують додаткових заходів, які гарантують, що інформація буде визнана доказом у суді. Використання OSINT у розслідуванні злочинів проти людяності відкриває нові горизонти для кримінальної юстиції в умовах збройних конфліктів, проте вимагає системного підходу, який включає розроблення законодавчих стандартів, удосконалення слідчих методик і активну міждисциплінарну співпрацю (Ругало, 2023).

Інформація, отримана за допомогою методик і засобів OSINT, за своєю природою є відкритою. Вона не підпадає під категорію даних з обмеженим доступом і, що особливо важливо, не здобувається незаконними методами. Це означає, що вона цілком відповідає вимогам чинного законодавства, зокрема статті 84 Кримінального процесуального кодексу України (далі за текстом КПК), яка визначає поняття доказів. Проте варто наголосити: хоча така інформація доступна у відкритому доступі, її ефективне використання у кримінальному процесі потребує чіткого розуміння юридичних аспектів. Особливістю даних, зібраних за допомогою OSINT, є те, що вони переважно зберігаються в електронному вигляді – на цифрових носіях або безпосередньо в мережі "Інтернет".

Міжнародне співтовариство докладає багато зусиль для реформування процедури отримання транснаціональних електронних доказів під час адаптації до сучасних вимог. Нові правила ЄС щодо надання та зберігання транснаціональних електронних доказів охоплюють категорії даних абонентів, доступу до транзакцій та контенту. Установлено, що проєкти SIRIUS і TREIO є важливими інструментами для підтримки правоохоронних органів ЄС у питаннях,

пов'язаних із транснаціональними електронними доказами. В Україні необхідно вдосконалити законодавство щодо порядку отримання транснаціональних електронних доказів з урахуванням міжнародної практики. Використання рекомендацій проєктів SIRIUS та TREIO в Україні може сприяти вдосконаленню процедури міжнародного співробітництва щодо доступу до транснаціональних електронних доказів у кримінальних розслідуваннях (Костюченко, Ахтирська, Середа та ін., 2023; Костюченко, & Ахтирська, 2022; Костюченко, Ахтирська, Виноградова та ін., 2024).

Саме це ставить перед українським правосуддям додаткові виклики. Нині у вітчизняному кримінальному процесуальному законодавстві йдеться про такий вид джерел доказів, як документ (частина 2 статті 84). Документом, згідно із частиною 1 статті 99 КПК, є спеціально створений із метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. До документів, за наявності в них відомостей, передбачених частиною 1 цієї статті, законодавець відносить: 1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у т. ч. комп'ютерні дані); 2) матеріали, отримані внаслідок здійснення під час кримінального провадження заходів, передбачених чинними міжнародними договорами, згоду на обов'язковість яких надано Верховною Радою України; 3) складені в порядку, передбаченому цим Кодексом, протоколи процесуальних дій і додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії. Матеріали, у яких зафіксовано фактичні дані про протиправні діяння окремих осіб і груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України "Про оперативно-розшукову діяльність", за умови відповідності до вимог цієї статті, є документами й можуть використовуватися в кримінальному провадженні як докази (частина 2 статті 99 КПК) (Верховна Рада, 2012). Відповідно, за наведеними ознаками частину із цих документів слід вважати "електронними доказами".

Разом із тим у КПК, на відміну від інших процесуальних кодексів, відсутнє чітке визначення терміна "електронний доказ". Це створює правову прогалину, яка значно ускладнює використання електронних даних у судових процесах саме в кримінальному провадженні. Водночас у науковій доктрині ця проблема вже знайшла своє відображення. Важливий внесок у дослідження поняття електронного доказу зробили такі українські науковці, як Ахтирська Н. М., Костюченко О. Ю., Коваленко А. М., Неділько Я. В., Сіренко О. В. Їхні праці не лише аналізують теоретичні аспекти цього явища, але й пропонують практичні рекомендації щодо використання електронних доказів у роботі суддів, слідчих і прокурорів. Незважаючи на це, реальність залишається складнішою, оскільки на практиці відсутність нормативного визначення поняття "електронний доказ" залишає простір для різночитань і суперечностей у правозастосуванні. Коли йдеться про дані з відкритих джерел, що можуть бути використані як електронні докази, то слід особливо зосередитися на аспектах їх отримання, оброблення та зберігання. З одного боку, збирання даних із відкритих джерел є доступним інструментом, що не потребує значних ресурсів. З іншого боку, воно потребує високого рівня відповідальності та професійної підготовки. Будь-яка недбалість під час збирання або зберігання таких даних може призвести до їх втрати або недопустимості в суді. Із цією метою в Україні діє низка нормативно-правових актів, які регулюють процедури фіксації та зберігання даних. Водночас ці акти не завжди враховують специфіку роботи з електронною інформацією. Тому органам досудового розслідування, що активно застосовують OSINT у своїй діяльності, доводиться шукати баланс між юридичними вимогами й технічними можливостями. Якщо інформація з відкритих джерел містить відомості, що вказують на наявність або відсутність обставин, які підлягають доказуванню у кримінальному провадженні, то вона може стати повноцінним доказом у справі. Проте, навіть попри активне використання OSINT у розслідуваннях злочинів проти людяності та інших міжнародних злочинів, зберігається значний дефіцит нормативно-правового регулювання цієї діяльності. Цей вакуум регулювання створює ризики для ефективного застосування даних, отриманих із відкритих джерел. По-перше, відсутність чітких процедур підвищує імовірність їхньої дискредитації в суді. По-друге, це ускладнює стандартизацію процесів збирання та оброблення електронних доказів, що, у свою чергу, позначається на їхній доказовій силі. Таким чином, використання OSINT як джерела електронних доказів має значний потенціал для вдосконалення досудового розслідування і судового розгляду щодо осіб, підозрюваних та обвинувачених у злочинах проти людяності. Водночас подальший розвиток цього напряму потребує розроблення комплексних нормативно-правових стандартів, які враховуватимуть як технічні особливості роботи з електронними даними, так і необхідність дотримання процесуальних гарантій.

Для забезпечення єдиних процедур і надання методичних рекомендацій слідчим, які використовують відкриті дані, був розроблений Протокол Берклі (United Nations, 2022). Цей документ став результатом співпраці між Центром прав людини Каліфорнійського університету в Берклі та представниками Управління ООН із прав людини. Його метою було формування міжнародних стандартів проведення онлайн-розслідувань, спрямованих на документування можливих порушень міжнародного права, прав людини, міжнародного гуманітарного та кримінального права. У Протоколі наводяться детальні рекомендації щодо процедур збирання, аналізу та збереження цифрової інформації. Хоча документ і не має обов'язкової юридичної сили, його стандарти стали важливим орієнтиром для правоохоронних органів різних країн. Дотримання цих рекомендацій значно підвищує надійність і точність зібраних доказів, а також зменшує ризик їхнього виключення з розгляду в судовому провадженні через процедурні порушення чи сумнівність автентичності. Однак Протокол Берклі – це лише один із багатьох інструментів, які можуть бути використані у процесі розслідування. Наприклад, слід ураховувати "Керівні принципи щодо електронних доказів", розроблені Радою Європи. Вони пропонують чіткі рекомендації для забезпечення належного документування та оброблення цифрових даних. Крім того, існує міжнародний стандарт ISO/IEC 27037:2017, який у своєму національному варіанті представлений як ДСТУ ISO/IEC 27037:2017. Ці стандарти, хоча й доволі об'ємні, зосереджуються на базових принципах

роботи з електронними доказами, таких як отримання, збереження та автентифікація зібраної інформації. Особливу увагу слід звернути на процес легалізації отриманих доказів, що є однією з найскладніших задач у контексті використання даних із відкритих джерел. Українське кримінальне процесуальне законодавство висуває суворі вимоги до порядку отримання, закріплення та використання доказів. Зокрема, кожен етап має чітко відповідати законодавчим нормам, щоб уникнути визнання доказів недопустимими. Легалізація таких доказів також потребує забезпечення їхньої автентичності. Це означає, що слідчий повинен мати можливість довести, що зібрана інформація не була змінена з моменту її отримання. Важливими інструментами в цьому процесі є фіксація метаданих, застосування технічних засобів для захисту від маніпуляцій, а також залучення експертів для перевірки походження і змісту доказів. Необхідність удосконалення нормативно-правової бази України в цій сфері є очевидною. Попри наявність міжнародних стандартів і рекомендацій, вони часто мають загальний характер і потребують адаптації до національних правових реалій. Розроблення чітких норм, які регулювали б використання відкритих даних у кримінальному провадженні, стала б вагомим кроком до підвищення ефективності розслідування злочинів, особливо тих, що стосуються порушень міжнародного права чи злочинів проти людяності. Протокол Берклі, "Керівні принципи щодо електронних доказів" і стандарти ISO/IEC є важливими елементами у створенні сучасної методології роботи з відкритими даними, проте їх практичне впровадження вимагає не лише технічних знань, а й законодавчого забезпечення, що гарантує дотримання прав учасників кримінального провадження та забезпечує допустимість зібраних доказів у суді.

Електронні докази, без сумніву, є важливим елементом сучасних кримінальних проваджень, їхня роль у розслідуваннях неухильно зростає, особливо у світі, де цифрові технології охоплюють практично всі сфери життя. Однак, щоб ці докази мали юридичну силу, вони мають відповідати чітким вимогам – належності, допустимості та достовірності, що визначаються не лише внутрішньою суттю доказу, а й процедурами його збирання і оброблення. Стаття 85 КПК чітко окреслює, що доказ є належним, якщо він має прямий чи опосередкований зв'язок із тими обставинами, що підлягають доказуванню в межах кримінальної справи, або з іншими фактами, що можуть вплинути на результат судового розгляду (Верховна Рада, 2012). Важливою частиною цього процесу є обов'язок обвинувачення довести, як саме конкретний електронний доказ пов'язаний із розслідуваними подіями. Ідеться не лише про фізичне існування доказу, а й про його роль у процесі – як він підтверджує або спростовує факти, що мають значення для справи. При цьому обвинувачення має також продемонструвати, що процедура збирання цього доказу була виконана в межах законодавчих норм, адже збирання доказів через відкриті джерела – це не простий одноетапний процес. Касаційний кримінальний суд Верховного Суду у постанові від 21 липня 2025 року у справі №201/11849/23 (Верховний Суд, Касаційний кримінальний суд, 2025) зазначив, що протоколи оглядів інтернет-сторінок і телеграм-каналів і додатки до протоколів, у яких зафіксовано за допомогою функцій скріншоту, друку й запису на технічні носії зміст відображеної на них інформації, що підтверджує існування обставин, які підлягають доказуванню, є допустимими доказами, якщо сторона захисту не спростувала відповідну інформацію і не аргументувала, що інформація, надана органом досудового розслідування, не відповідає дійсності, зокрема містить ознаки фальсифікації чи спотворення. Кожен крок, від аналізу джерела інформації до її фіксації, має бути документовано та виконано за всіма правилами, аби забезпечити автентичність і законність. За статтею 87 КПК недопустимими є докази, що були отримані внаслідок істотного порушення прав і свобод людини (Верховна Рада, 2012). Якщо на етапі збирання первинних доказів було допущено зазначене порушення, то суд має застосувати доктрину "плодів отруйного дерева" і визнати як первинні, так і похідні докази недопустимими. Ця доктрина передбачає, що недопустимий доказ, навіть якщо він має беззаперечне значення для справи, може "забруднити" всю іншу доказову базу, отриману у процесі розслідування. У зв'язку із цим слід підтримати позицію О. О. Торбаса, що потрібно чітко усвідомлювати, що робота із цифровими доказами – це не лише технічне завдання, а й складний юридичний процес, який вимагає не тільки професіоналізму, а й ретельності на кожному етапі. Кожен крок у збиранні, аналізі та зберіганні електронних доказів має бути продуманий і обґрунтований з погляду правового поля, аби не тільки забезпечити ефективність розслідування, а й гарантувати захист прав і свобод усіх учасників процесу (Торбас, 2024, с. 106–112).

У світі, де інформація стала найціннішим ресурсом, питання правильного збирання та оброблення доказів набувають особливого значення. У цьому контексті будь-які порушення встановлених алгоритмів збирання можуть не лише спотворити картину розслідування, а й призвести до визнання зібраних доказів недійсними. Це, у свою чергу, може фактично знищити значну частину роботи слідчого, що проводиться не один місяць чи навіть рік. Уявіть собі ситуацію, коли через технічну помилку або нехтування необхідними процедурами доказ, який міг би стати основою для доказування вини або невинуватості, буде відхилений судом. Це, безперечно, катастрофічно для всієї справи. Тому вимога до підвищення кваліфікації слідчих та аналітиків, які працюють із відкритими джерелами, стає нагальною. Ці фахівці мають не лише володіти техніками збирання інформації, а й бути здатними правильно застосовувати законодавчі норми, що регулюють ці процеси. Без належної юридичної обізнаності навіть найкращі технічні засоби збирання інформації можуть не дати бажаного результату в суді. З достовірністю доказів ситуація ще більш складна. Вона не обмежується лише питанням їхнього походження чи способу збирання; достовірність доказу стосується його відповідності до дійсності, тобто того, чи є він справжнім і точним відображенням фактів, що мали місце. Особливо в контексті електронних доказів ця проблема є дуже актуальною. Через свою цифрову природу такі докази набагато легші для маніпуляцій, ніж традиційні паперові. Змінити чи навіть підробити електронні дані не становить великих труднощів, особливо за допомогою сучасних інструментів редагування. Тому перевірка їх достовірності – це не просто важлива, а життєво необхідна процедура для забезпечення справедливості в судовому процесі.

Як правильно зазначає О. О. Торбас, одним із методів перевірки достовірності електронних доказів є перевірка хеш-суми. Це своєрідний цифровий підпис файлу, який гарантує його цілісність. Хеш-сума – це математичний алгоритм, що обчислює унікальне значення для кожного файлу або набору даних, яке залишається незмінним, поки самі дані не змінюються. Таким чином, якщо під час збирання доказів було створено точну копію файлу, то хеш-суми оригіналу та копії мають збігатися. Інакше, якщо дані були змінені хоча б на один символ, то хеш-сума вже не відповідатиме і вказуватиме на те, що файл був підданий редагуванню. Це дає змогу переконатися в достовірності доказів, зберігаючи їх незмінність протягом усього процесу розслідування і судового розгляду. Однак важливо також розуміти, що перевірка хеш-суми – це лише один з інструментів у всьому арсеналі методів для забезпечення достовірності електронних доказів. І для того, щоб система працювала без збоїв, усі етапи збирання, оброблення та зберігання електронних даних мають бути чітко регламентовані, з мінімальними можливими помилками. Отже, забезпечення достовірності доказів є процесом, який потребує ретельного підходу на всіх етапах і, як результат, має вирішальне значення для справедливого розгляду справи в суді (Торбас, 2024, с. 112–118).

Збираючи дані з відкритих джерел, важливо розуміти, що ці дані можуть бути неповними або неточними. Тому кожне джерело потребує ретельної перевірки, а також слід використовувати кілька методів для підтвердження отриманої інформації. Особливо це актуально в умовах конфліктів, коли сторони можуть навмисно поширювати неправдиві дані. Окрім того, використання відкритих джерел може викликати питання законності та етики. Важливо дотримуватися законів про конфіденційність та авторське право, а також професійних стандартів, щоб не зашкодити інформаторам і запобігти поширенню неправдивих даних. Це може передбачати використання анонімізаторів, шифрування та інших засобів безпеки. Коли говоримо про збереження та аналіз даних у сучасній журналістиці, неможливо обійти стороною співпрацю з міжнародними організаціями. Такі платформи, як International Fact-Checking Network (IFCN) та Bellingcat, відіграють ключову роль у цьому процесі. Вони надають доступ до глобальних баз даних, інструментів і методик для перевірки фактів і збирання інформації, підвищуючи якість розслідувань і гарантуючи досягнення соціуму достовірної інформації. Наприклад, співпраця з Bellingcat дає змогу використовувати найсучасніші методи OSINT для документування злочинів проти людяності в Україні. Bellingcat, будучи інтернет-ресурсом, заснованим на використанні матеріалів із відкритих джерел для розслідування різноманітних подій, включаючи воєнні конфлікти, використовує відео- та фотодокази, супутникові знімки, аналіз соціальних мереж та інші відкриті джерела для встановлення фактів, пов'язаних із конфліктами (Bellingcat, 2024; Бриж, 2022). Таким чином, слід погодитися з думкою О. О. Торбаса, що журналісти мають не лише ретельно перевіряти кожне джерело інформації, а й дотримуватися високих етичних стандартів і законів, щоб забезпечити безпеку своїх інформаторів і гарантувати поширення достовірних даних. У цьому процесі співпраця з міжнародними організаціями є надзвичайно важливою, оскільки вона надає доступ до ресурсів, які дають змогу проводити більш ґрунтовні та якісні розслідування (Торбас, 2024).

Застосування розвідки на основі відкритих джерел інформації (OSINT) у розслідуванні злочинів проти людяності є важливим елементом сучасного кримінального провадження. Рекомендовано впровадити на законодавчому рівні стандарти використання OSINT у кримінальних провадженнях, а також розробити спеціальні навчальні програми для слідчих, прокурорів, адвокатів і суддів щодо застосування OSINT у кримінальних справах. Окрім цього, важливо забезпечити міжнародну співпрацю для обміну досвідом і підвищення ефективності розслідувань, а також створити технічні протоколи збирання, зберігання й аналізу цифрових даних, які відповідатимуть міжнародним стандартам (Шевцов, 2025).

**Дискусія і висновки**

Застосування відкритих джерел розвідки (OSINT) у розслідуванні злочинів проти людяності є важливим елементом сучасного кримінального судочинства. Цей метод дає змогу збирати докази навіть за умов обмеженого доступу до місць скоєння злочинів. Висновки, зроблені у статті, підкреслюють, що ефективне використання OSINT можливе лише за умови належного правового регулювання, дотримання міжнародних стандартів і впровадження сучасних технічних засобів для верифікації доказів. Доцільно впровадити на законодавчому рівні стандарти використання OSINT у кримінальних провадженнях, а також розробити спеціальні навчальні програми для слідчих, прокурорів і суддів щодо застосування OSINT у кримінальних справах. Окрім цього, важливо забезпечити міжнародну співпрацю для обміну досвідом і підвищення ефективності розслідувань, а також створити технічні протоколи збирання, зберігання й аналізу цифрових даних, які відповідатимуть міжнародним стандартам. Отже, використання OSINT є перспективним напрямом удосконалення кримінальних розслідувань, особливо у справах про злочини проти людяності. Цей підхід сприятиме посиленню механізмів притягнення до відповідальності за найтяжчі міжнародні злочини, тим самим забезпечуючи справедливість правосуддя та відшкодування шкоди для постраждалих.

**Внесок авторів:** Олена Костюченко – сприяння в ідентифікації ключових правових проблем застосування OSINT, аналіз міжнародних та українських нормативних актів, формування рекомендацій щодо уніфікації процедур збирання цифрових доказів; Андрій Шевцов – проведення нормативно-правового аналізу законодавчих актів і процесуальних норм, збирання і систематизація судової практики з питань допустимості цифрових доказів, підготовка пропозицій із тлумачення та застосування процедур перевірки автентичності OSINT-даних.

**Джерела фінансування.** Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

**Список використаних джерел**

Бриж, Є. (2022, 27 листопада). *Важливо, щоб люди бачили війну в Україні очима українців*. Detector Media. https://detector.media/infospace/article/205355/2022-11-27-vazhlyvo-shchob-lyudy-bachyly-viynu-v-ukraini-ochyma-/ukraintsiv-predstavnyky-bellingcat-i-slidstva-rozpovily-pro-dokumentuvannya-/zlochyniv-rosiyan/

Верховна Рада України. (1992). *Про оперативно-розшукову діяльність*. Закон України № 2135-XII від 18.02.1992. https://zakon.rada.gov.ua/laws/show/2135-12#Text

Верховна Рада України. (2012). *Кримінальний процесуальний кодекс України.* Закон України № 4651-VI від 13.04.2012). https://zakon.rada.gov.ua/laws/show/4651-17/conv#n387

Верховний Суд, Касаційний кримінальний суд. (2025, 21 липня). Постанова у справі № 201/11849/23 (№ 51-584км25) https://reyestr.court.gov.ua/Review/129086893

Костюченко, О. (2022). Електронне подання до суду та цифровізація судового процесу як елементи впровадження ефективного судочинства та гарантія достовірності доказів. У Н. В. Глинська, Д. І. Клепка, А. А. Барабаш (Ред.). *Цифрова трансформація кримінального провадження в умовах воєнного стану. Право*, 78–81. https://doi.org/10.31359/9789669984395

Костюченко, О. Ю., & Ахтирська, Н. М. (2022). Процесуальні та організаційні аспекти збирання електронних доказів під час міжнародного співробітництва. *Науковий вісник Ужгородського національного університету. Серія ПРАВО,* 72(2), 192–198.

Костюченко, О., Ахтирська, Н., Виноградова, А., Павлиш, Т. Г., & Барган, С. (2024). Ефективність методу судової комп'ютерної симуляції злочинів у контексті військових операцій. *Lex Humana*, 16*(1), 156–172. https://seer.ucp.br/seer/index.php/LexHumana/article/view/2887/370

Костюченко, О., Ахтирська, Н., Середа, Ю., Виноградова, А., & Мірошников, І. (2023). Роль транснаціональних електронних доказів у розслідуванні злочинів. *Amazonia Investiga*, 12*(71), 293–303. https://doi.org/10.34069/AI/2023.71.11.26

Ругало, Ю. (2023). Злочини проти людяності в Україні з 2014 року і по сьогодні. *Юридичний науковий електронний журнал*, 6, 696–699. https://doi.org/10.32782/2524-0374/2023-6/164

Торбас, О. О. (2024). *OSINT при розслідуванні кримінальних правопорушень*. https://hdl.handle.net/11300/27740; https://doi.org/10.32837/11300.27740

Шевцов, А. (2025). Підвищення ефективності розслідування злочинів проти людяності за допомогою використання відкритих джерел інформації (OSINT). У М. О. Денисюк (Ред.). *Юридична наука та освіта: минуле, сучасне і майбутнє* (с. 370–371). Видавництво "Людмила".

Bellingcat. (2024). *How Bellingcat collects, verifies and archives digital evidence of war crimes in Ukraine*. https://reutersinstitute.politics.ox.ac.uk/how-bellingcat-collects-verifies-and-archives-digital-evidence-war-crimes-ukraine

United Nations. (2022). Berkeley Protocol on Digital Open-Source Investigations. https://doi.org/10.18356/9789210053433

**References**

Bellingcat. (2024). *How Bellingcat collects, verifies and archives digital evidence of war crimes in Ukraine*. https://reutersinstitute.politics.ox.ac.uk/how-bellingcat-collects-verifies-and-archives-digital-evidence-war-crimes-ukraine

Kostiuchenko, O. (2022). Electronic court submission and digitalization of judicial process as elements of effective justice and evidence reliability. In N. V. Hlynska, D. I. Klepka, A. A. Barabash (Eds.). *Digital transformation of criminal proceedings during martial law. Law*, 78–81 [in Ukrainian]. https://doi.org/10.31359/9789669984395

Kostiuchenko, O. Y., & Akhtyrska, N. M. (2022). Procedural and organizational aspects of electronic evidence collection during international cooperation. *Scientific Bulletin of Uzhhorod National University. Law Series*, 72(2), 192–198 [in Ukrainian].

Kostiuchenko, O., Akhtyrska, N., Sereda, Y., Vynohradova, A., & Miroshnykov, I. (2023). The role of transnational electronic evidence in the investigation of crimes. *Amazonia Investiga*, 12*(71), 293–303 [in Ukrainian]. https://doi.org/10.34069/AI/2023.71.11.26

Kostiuchenko, O., Akhtyrska, N., Vynohradova, A., Pavlysh, T. G., Barhan, S. (2024). Effectiveness of the method of forensic computer simulation of offences in the context of military operations. *Lex Humana*, 16*(1), 156–172 [in Ukrainian] https://seer.ucp.br/seer/index.php/LexHumana/article/view/2887/370.

Rugalo, Y. (2023). Crimes against humanity in Ukraine from 2014 to the present. *Legal Scientific Electronic Journal*, 6, 696–699 [in Ukrainian]. https://doi.org/10.32782/2524-0374/2023-6/164

Shevtsov, A. (2025). Enhancing the effectiveness of investigating crimes against humanity by using open-source intelligence (OSINT). In M.O. Denysiuk (Ed.). *Legal science and education: past, present, and future* (p. 370–371). "Lyudmyla" Edition [in Ukrainian].

Torbas, O. O. (2024). *OSINT in the investigation of criminal offenses* [in Ukrainian]. https://hdl.handle.net/11300/27740; https://doi.org/10.32837/11300.27740

United Nations. (2022). Berkeley Protocol on Digital Open-Source Investigations. https://doi.org/10.18356/9789210053433

Verkhovna Rada of Ukraine. (1992). *On Operative-Investigative Activities*. Law of Ukraine No. 2135-XII of 13.04.2012 [in Ukrainian]. https://zakon.rada.gov.ua/laws/show/2135-12#Text

Verkhovna Rada of Ukraine. (2012). *Criminal Procedure Code of Ukraine*. Law of Ukraine No. 4651-VI of 13.04.2012 [in Ukrainian]. https://zakon.rada.gov.ua/laws/show/4651-17/conv#n387

Bryzh, Y. (2022, November 27). *It is important for people to see the war in Ukraine through the eyes of Ukrainians*. Detector Media [in Ukrainian]. https://detector.media/infospace/article/205355/2022-11-27-vazhlyvo-shchob/-lyudy-bachyly-viynu-v-ukraini-ochyma-ukraintsiv-predstavnyky-bellingcat-i-/slidstva-rozpovily-pro-dokumentuvannya-zlochyniv-rosiyan/

Supreme Court of Ukraine, Criminal Cassation Court. (2025, July 21). Judgment in case No. 201/11849/23 (No. 51-584km25) [in Ukrainian]. https://reyestr.court.gov.ua/Review/129086893

**Отримано редакцією журналу / Received: 16.09.25**
**Прорецензовано / Revised: 21.09.25**
**Схвалено до друку / Accepted: 25.09.25**

**Olena KOSTYUCHENKO, PhD (Law), Assoc. Prof.**
**ORCID ID: 0000-0002-2243-1173**
**e-mail: olena_kostiuchenko@knu.ua**
**Taras Shevchenko National University of Kyiv, Kyiv, Ukraine**

**Andrii SHEVTSOV, PhD Student**
**ORCID ID: 0009-0006-2080-5561**
**e-mail: andriishevtsov@knu.ua**
**Taras Shevchenko National University of Kyiv, Kyiv, Ukraine**

## THE USE OF OPEN-SOURCE INTELLIGENCE (OSINT) IN THE INVESTIGATION OF CRIMES AGAINST HUMANITY

**Background.** ***In today's world, as digital technologies penetrate every sphere of life, open-source information, known as OSINT (Open-Source Intelligence), has become an integral component of contemporary investigations into crimes against humanity. These data often prove indispensable during criminal prosecution, especially in cases where other sources of information are unavailable or restricted. However, for materials obtained through OSINT to be used as evidence, several complex issues must be addressed regarding their reliability, authenticity, and admissibility.***

**Methods.** ***A comparative-legal method (juxtaposing evidence-admissibility standards developed in the practice of the International Criminal Tribunal for the former Yugoslavia and the International Criminal Court with Ukrainian practice); regulatory-legal analysis (examining laws, international agreements, and OSINT-related guidelines); analysis of Ukrainian case law, which is at a formative stage in developing approaches to the use of OSINT in criminal proceedings; interpretive-legal method (construing procedural norms in the context of OSINT); and a systemic legal approach (integrating the identified norms into recommendations for Ukrainian criminal procedure).***

**Results.** ***The study identified three key problems in applying OSINT in investigations of crimes against humanity. First, the absence of unified legislative standards and methodologies for collecting digital evidence leads to divergences in procedures across jurisdictions, complicating the recognition of such evidence in court. Second, without clearly defined verification procedures (geolocation, metadata analysis, comparison of satellite imagery), the collected data often fails to withstand scrutiny as to authenticity. Third, in areas of active hostilities, traditional means of documentation are often insufficient, whereas OSINT enables the reconstruction of event chronology and confirmation of crime-related object locations, even under conditions of limited access.***

**Conclusions.** ***To enhance the effectiveness of OSINT in criminal proceedings, it is necessary to develop comprehensive methodologies that consider not only the technical aspects of working with data but also ethical and legal constraints. For example, it is important to introduce standards for documenting the information-gathering process–from recording the source to verification procedures. Without such mechanisms, investigators and prosecutors remain vulnerable, as the admissibility of the results of procedural actions may be challenged at the trial stage. Only an interdisciplinary approach will ensure the proper quality of investigations and the effective prosecution of individuals who have committed the gravest international crimes.***

**Keywords:** ***OSINT, crimes against humanity, pre-trial investigation, open sources, evidence, electronic evidence, documents.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.