

ІМПЛЕМЕНТАЦІЯ OSINT-ТЕХНОЛОГІЙ У ПРОЦЕСУАЛЬНУ ДІЯЛЬНІСТЬ ОРГАНІВ КРИМІНАЛЬНОЇ ЮСТИЦІЇ: ІННОВАЦІЙНИЙ ПОТЕНЦІАЛ, ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ТА НАПРЯМИ ЗАСТОСУВАННЯ В УМОВАХ ВІЙНИ В УКРАЇНІ

Негребецький В. В.

ВСТУП

Сучасні збройні конфлікти радикально трансформували не лише форми ведення бойових дій, а й способи їх документування та доведення у кримінальних провадженнях. Цифровізація комунікацій, масова доступність мобільних пристроїв із камерами, стрімів і геолокаційних сервісів, розвиток супутникового спостереження та поява нових платформ обміну даними створили безпрецедентно щільне інформаційне середовище. У такому середовищі відкриті джерела – соціальні мережі, відеохостинги, веб-архіви, супутникові платформи, державні реєстри та інші цифрові ресурси – стають повноцінним джерелом для формування доказової бази.

Від початку повномасштабної війни інтенсивність і різноманітність цифрових слідів воєнних злочинів різко зросли. Відео й фотоматеріали наслідків обстрілів, фрагменти трансляцій із місця подій, свідчення очевидців у соціальних мережах, телеграм-канали й масиви супутникових спостережень практично в реальному часі формували нову доказову базу для правоохоронних органів. Пошук достовірних інструментів ідентифікації осіб, причетних до воєнних злочинів, локалізації місць їх учинення, а також верифікація причинно-наслідкових зв'язків природно вивів вітчизняні правоохоронні органи на технологію OSINT як систематизований практикою підхід до роботи з відкритими цифровими даними.

Ключовою перевагою OSINT стала швидкість і масштабованість фіксації подій. Йдеться не лише про «перше сповіщення» із соцмереж, а про можливість будувати просторово-часові реконструкції: геолокувати кадри за характерними ознаками місцевості, зіставляти їх із супутниковими рядами «до/після», накладати на хроніки повітряних тривог чи системні часові мітки, звужуючи «вікно часу» до процесуально прийнятних меж. З огляду на обмежений доступ до місць злочинів у зоні бойових дій саме ці методики стали мостом між оперативним реагуванням і наступними «класичними» слідчими (розшуковими) і процесуальними діями.

OSINT став каталізатором міжвідомчої взаємодії й міжнародної кооперації. Спільні аналітичні проекти, консолідація верифікованих геолокацій у відкритих базах даних, обмін методиками та інструментарієм із громадянськими ініціативами і науковими центрами створили «екосистему довіри», де стандарти якості поступово уніфікуються¹. Таким чином, вихід на OSINT став не ситуативною

¹ OSINT-розвідка у роботі журналістів. URL: <https://youcontrol.com.ua/articles/osint-in-journalists-work/>

відповіддю на дефіцит доступу до місць подій, а елементом структурної модернізації правоохоронних органів в епоху цифровізації, що забезпечує і оперативність, і юридичну життєздатність доказів у воєнний і повоєнний періоди.

Питанням використання сучасних інформаційних технологій, в тому числі для збирання інформації з відкритих джерел, у кримінальному провадженні були присвячені наукові заходи та роботи таких вчених-юристів, як Г.К. Авдеева, В. С. Батиргареева, В. І. Борисов, Т. Я. Гнідець, Ю. І. Дмитрик, К.В. Дубонос, Н. М. Дяченко, В. А. Журавель, В. П. Захаров, А. О. Ігнатович, Р. С. Козьяков, С. С. Кудінов, В.О. Коновалова, Т. М. Лемеха, А.М. Лисенко, О. С. Мельник, А. О. Мороз, І. В. Олешко, Ю. В. Осадча, О. В. Рибальський, В. І. Рудешко, В. І. Соловйов, Л. І. Сопільник, І. О. Супрун, В. В. Топчій, А. О. Фесенко, В. Г. Хахановський, Л. М. Хмельничий, Р. Ю. Царьов, В. А. Швець, В.М. Шевчук, В.Ю. Шепітько, Р. М. Шехавцов й інших².

Необхідно відзначити, що в науковій і науково-практичній літературі OSINT-технології виявлення і збирання доказової інформації висвітлювались в різних аспектах. Разом із тим, з нашого погляду, вкрай важливо і актуально на цей час комплексно дослідити можливості імплементації OSINT-технологій у процесуальну діяльність органів кримінальної юстиції з огляду на інноваційний потенціал, функціональні можливості та напрями застосування саме в умовах війни в Україні. Тому питання дослідження тенденцій і потенціалу OSINT-технологій в прикладному аспекті щодо діяльності органів кримінальної юстиції і сектору безпеки і оборони України в діяльності, пов'язаної з розслідуванням і попередженням кримінальних правопорушень потребує подальшого розгляду. Також у зв'язку з війною в Україні вкрай актуальним становиться питання використання можливостей OSINT в діяльності слідчих підрозділів в контексті підвищення ефективності розслідування воєнних злочинів та злочинів агресії в Україні.

Отже, завдання вивчення міжнародного досвіду використання OSINT є актуальним, та враховуючи потреби вдосконалення нормативного регулювання у цій царині в Україні, є цілком обґрунтованим.

² *Трансформація завдань криміналістики в умовах воєнного стану та євроінтеграційних процесів* : зб. матеріалів наук.-практ. конф. присвяч. пам'яті д-ра юрид. наук, проф. В.О. Коновалої, м. Харків, 28 берез. 2024 р. Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків: Право, 2024; *Методологічні засади криміналістики: традиції та новачі* : зб. матеріалів Криміналістичних читань, присвяч.пам'яті акад. В. О. Коновалої, м. Харків, 28 берез. 2025 р. Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики; Нац. акад. прав. наук України; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків: Право, 2025; *Роль OSINT-досліджень у підвищенні рівня національної безпеки України* : матеріали круглого столу (м. Львів, 7 травня 2025 р.) Львів : ЛьВДУВС, 2025.

1. Нормативно-правове регулювання імплементації OSINT-технологій у процесуальну діяльність органів кримінальної юстиції

З моменту початку повномасштабної війни проти України пошук інструментів ідентифікації осіб, які вчинили воєнні злочини, місць вчинення таких злочинів, відомості про які потрапляли в мережу Інтернет, вивів вітчизняні правоохоронні органи на OSINT.

Заслугує на позитивну оцінку діяльність Офісу Генерального прокурора, СБУ, Національної поліції України, а також науковців та правозахисників, спрямована на впровадження OSINT у практику виявлення та розслідування воєнних злочинів. Так, 12–13 січня 2026 року у співпраці з Тренінговим центром прокурорів України та Національною школою суддів України, за підтримки проєкту Ради Європи CyberUA, відбувся спеціалізований тренінг, присвячений використанню відкритих джерел (OSINT) та електронних доказів у кримінальному процесі, з акцентом на кримінальні провадження щодо воєнних злочинів і грубих порушень прав людини³.

Перш за все, було обговорено вимоги до електронних доказів, закріплені у національному кримінальному процесуальному законодавстві та міжнародних стандартах, зокрема у Протоколі Берклі. Учасники розглянули типові категорії відкритих джерел, види електронних доказів, а також детально обговорили та проаналізували процедури забезпечення ланцюга зберігання (chain of custody) електронних доказів.

Офіс Верховного комісара ООН із прав людини та Центр з прав людини Каліфорнійського університету в Берклі у 2020 р. представили «практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права», який містить стандарти й методологічні підходи до «збору, збереження та аналізу інформації у відкритому доступі, яка може бути представлена як доказ у кримінальних процесах»⁴. Нажаль, норми Кримінального процесуального кодексу України не передбачають окремої категорії цифрових доказів. У КПК відсутнє визначення терміна «цифрові докази», не наведено докладного порядку їх вилучення, огляду, фіксування та зберігання. Однак у слідчих і суддів часто виникають труднощі у збиранні й оцінюванні цифрових доказів через відсутність у законодавстві України їх визначення, порядку фіксування й оцінки⁵. Це може спричинити помилки в роботі із цифровою інформацією й невизнання її допустимим і достовірним доказом у суді.

³ OSINT та електронні докази: юридичні вимоги та практика застосування у кримінальних провадженнях щодо воєнних злочинів в Україні. 14.01.2026. URL: <https://www.coe.int/uk/web/kyiv/-/osint-and-electronic-evidence-legal-requirements-and-practical-application-in-criminal-proceedings-on-war-crimes-in-ukraine>

⁴ Протокол Берклі. URL: <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf>.

⁵ Галина Авдєєва, Ельжбета Живуцька-Козловська. Проблеми використання цифрових доказів у кримінальному судочинстві України та США (2023). URL: <https://khrife-journal.org/index.php/journal/article/download/564/633>.

Отже необхідно використовувати досвід провідних європейських країн, із залученням профільних науково-дослідних установ та провідних фахівців в галузі права привести чинне кримінально-процесуальне законодавство до вимог ери цифрових технологій.

Учасники також обговорили роль спеціаліста в OSINT-розслідуваннях: від коректного вилучення та фіксації даних до пояснення суду технічних аспектів (метадані, хеш-значення, валідація файлів, встановлення ознак редагування тощо). У дискусіях підкреслювалося, що важливим є належне документування залучення спеціаліста до проведення огляду під час використання OSINT у кримінальному провадженні.

Особливу зацікавленість учасників викликав блок щодо невідкладного збереження даних передбаченого статтями 16–17 Будапештської конвенції про кіберзлочинність, який дозволяє зберегти електронні дані до отримання належного процесуального доступу. Також було обговорено роботу мережі контактних пунктів 24/7, підготовку запитів про невідкладне збереження даних (preservation requests) та використання механізмів міжнародної правової допомоги (MLA) для отримання електронних доказів.

Науково-практичні тренінги також проводились і в системі МВС. Так, в жовтні 2025 року працівники слідчих та оперативних підрозділів Національної поліції України пройшли навчання щодо опанування навичок застосування технології збору та використання інформації з публічно доступних джерел у процесі доказування воєнних злочинів⁶.

В рамках реалізації завдань та заходів, передбачених Імплементацийним планом з виконання Рамкової програми співробітництва між Урядом України та ООН щодо запобігання та протидії сексуальному насильству, пов'язаному з конфліктом, Управлінням моніторингу дотримання прав людини МВС організовано проведення двох дводенних офлайн тренінгів для слідчих та оперативних працівників на тему: «Використання OSINT у доказуванні командної відповідальності за міжнародні злочини: теорія і практика».

Застосування технології OSINT дозволяє не лише отримувати доказову інформацію в умовах обмеженого доступу, а й створює підґрунтя для її формування у справах про воєнні злочини та злочини проти людяності, що відповідає як національним, так і міжнародним стандартам розслідування.

Навчання організовані Управлінням моніторингу дотримання прав людини Міністерства внутрішніх справ України та Національною Поліцією України за підтримки Програми розвитку ООН (ПРООН) в межах проєкту ПРООН «Спільна програма для України з питань СНПК», яка фінансується Європейським союзом.

Під час війни арсенал традиційних криміналістичних засобів і форм збирання доказів вчинення воєнних злочинів в Україні доволі обмежений через небезпеку для всіх учасників слідчих (розшукових), негласних слідчих

⁶ Використання OSINT у доказуванні командної відповідальності за міжнародні злочини: навчання НПУ. 08.10.2025. URL: <https://npu.gov.ua/news/vykorystannia-osint-u-dokazuvanni-komandnoi-vidpovidalnosti-za-mizhnarodni-zlochyny-navchannia-npu>

(розшукових) дій та неможливість безпосереднього доступу до місця події⁷, тому виникає потреба у застосуванні технологій штучного інтелекту. Крім цього, про європейський вектор розвитку криміналістики та судової експертизи в Україні свідчить застосування європейських стандартів доказування під час кримінального провадження⁸.

Указом Президента України від 11 травня 2023 року № 273/2023 було схвалено Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки⁹. «Кожен елемент державної системи – органи правопорядку передусім – мають працювати так, щоб люди реально відчували безпеку й захищеність, щоб люди реально відчували справедливість, щоб гарантувалося на рівні інституцій, на рівні повсякденної роботи тих, по кому люди судять про державу. Довіра в державі, довіра до держави формуються з довіри до тих, хто діє від імені держави. Правоохоронці, система прокуратури – ключові в цьому. Звичайно, разом з усіма іншими, хто працює в державному апараті», – наголосив Президент Володимир Зеленський¹⁰.

Документ було спільно розроблено міжвідомчою групою, до складу якої входили очільники Офісу Генпрокурора, МВС, Міністерства юстиції, СБУ, ДБР, Національної поліції, Державної прикордонної служби, БЕБ, Державної митної служби, а також представники Офісу Президента України, Кабінету Міністрів України, міжнародні експерти від Офісу Ради Європи в Україні, КМЄС, проекту ЄС «PRAVO-JUSTICE», відділу з правоохоронних питань Посольства США в Україні, Міжнародної організації права розвитку (IDLO). Основною метою розробників Плану було поставити у центр уваги сектору правопорядку, сектору безпеки і оборони людину, її життя, здоров'я, честь і гідність, права і охоронювані законом інтереси. Кожен українець має бути впевнений, що живе у безпеці, має свободу і може розраховувати на механізми справедливості.

План визначає шість стратегічних пріоритетів, які дозволять модернізувати сектор безпеки й привести у відповідність до стандартів, яких має досягти Україна на шляху до членства у ЄС, до яких належать:

1. Дієвість і ефективність органів правопорядку та прокуратури як невід'ємної складової сектору безпеки і оборони, в межах якого вони забезпечують національну безпеку України, у тому числі громадські безпеку й порядок, протидіють злочинності з урахуванням стратегічних цілей та відповідно до стандартів прав людини і основоположних свобод, у тому числі із забезпеченням гендерної рівності.

⁷ Дуфенюк О. Розслідування воєнних злочинів: логістичні, криміналістичні та судово-медичні питання. *Юридичний науковий електронний журнал*. 2022. № 4. С. 369–374. DOI: 10.32782/2524-0374/2022-4/88

⁸ Шепітько В. Ю. Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору. *Право України*. 2022. № 2. С. 87.

⁹ Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 – 2027 роки: Указ президента України від 11.05.2023 № 273/2023. URL: <https://www.president.gov.ua/documents/2732023-46733>.

¹⁰ Президент України схвалив Комплексний стратегічний план реформування органів правопорядку (12.05.2023). URL: <https://www.gp.gov.ua/ua/posts/prezident-ukrayini-sxvaliv-kompleksnii-strategichni-plan-reformuvannya-organiv-pravoporyadku>.

2. Послідовна кримінальна політика, пріоритетом у якій є запобігання злочинності, невідворотність відповідальності, захист особи, суспільства та держави від кримінальних правопорушень, забезпечення інтересів потерпілого.

3. Оперативність кримінального провадження з дотриманням міжнародних стандартів та принципу верховенства права.

4. Система управління, орієнтована на результат відповідно до встановлених пріоритетів.

5. Комплексна цифрова трансформація.

6. Відкритість, прозорість, підзвітність і незалежність.

Планом передбачено комплексну цифрову трансформацію, зокрема:

1. Здійснення консолідованої поетапної цифрової трансформації органів правопорядку та прокуратури на основі інструментів стратегічного менеджменту, які відповідають найкращим практикам ЄС.

2. Подальше впровадження в діяльність органів правопорядку та прокуратури інноваційних технологічних досягнень, що забезпечують гнучкість операційних процесів, IT-рішення, цифрову спроможність оперативно реагувати на події та зміни й здобувати результат, орієнтований на інтереси суспільства.

3. Поетапне впровадження електронної системи управління кримінальними провадженнями шляхом комплексної заміни та модернізації обладнання, забезпечення сумісності IT-систем, безперервності роботи, доступу усіх учасників кримінального провадження та інтероперабельності.

4. Підвищення ефективності діяльності органів правопорядку та прокуратури через забезпечення більшої доступності й повноти інформації, розроблення і впровадження сервісів на Єдиному державному вебпорталі електронних послуг.

5. Впровадження заходів безпеки і захисту персональних даних відповідно до стандартів ЄС.

6. Удосконалення та впровадження більш безпечних, гнучких, спроможних і доступних систем зв'язку між усіма органами правопорядку та іншими екстреними службами (включаючи цифрове радіо: голосовий зв'язок і широко-смугове передавання даних).

7. Запровадження в усіх органах правопорядку та прокуратури уніфікованої системи особистої автентифікації та системи біометричного зіставлення із поступовим забезпеченням її сумісності з європейськими системами. Широке використання під час здійснення досудового розслідування, а також для обробки даних та аналітичної діяльності органів правопорядку і прокуратури штучного інтелекту, блокчейну, хмарних обчислень та інших інноваційних рішень.

8. Оновлення операційних процесів за допомогою IT-систем, придатних для обміну даними з інституціями ЄС відповідно до стандартів ЄС.

9. Надання органам правопорядку та прокуратури для забезпечення виконання покладених на них функцій права на безпосередній спільний доступ до автоматизованих інформаційних і довідкових систем, реєстрів і баз даних, держателем (адміністратором) яких є інші державні органи¹¹.

¹¹ Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 – 2027 роки: Указ президента України від 11.05.2023 № 273/2023. URL: <https://www.president.gov.ua/documents/2732023-46733>.

2. Інтеграція OSINT-технологій в документування та розслідування воєнних злочинів

В сучасних реаліях воєнних та глобальних загроз усі практики у сфері міжнародного кримінального правосуддя повинні покращувати своє технічне розуміння новітніх технологій штучного інтелекту і повинні культивувати глибше сучасне розуміння застосування того, як соціальні мережі, геолокації, розмови мобільного зв'язку, комп'ютерна інформація та інші цифрові сліди й комунікації використовуються в зонах проведення воєнних дій¹². Зважаючи на дії країни-агресора на території України та вчинення масових вбивств, гвалтувань, мародерства, сьогодні гостро постає проблема збирання доказів воєнних злочинів. Це потребує активізації та поширення застосування технологій штучного інтелекту при виявленні, документуванні та розслідуванні воєнних злочинів, злочинів проти людяності та геноциду.

Розслідування і документування воєнних злочинів в Україні – найважливіший напрямок у роботі органів кримінальної юстиції. Вирішальне значення має професійне, якісне, всебічне, допустиме, вчасне та належне документування всіх елементів воєнного злочину. Станом на 20 січня 2026 року Офісом Генеральної прокуратури в період повномасштабного вторгнення ворога зареєстровано понад 212 000 випадків воєнних злочинів агресії та воєнних злочинів проти України¹³. Задokumentовані чисельні випадки руйнувань житлової інфраструктури, вбивств мирних жителів, мародерства та насильства. Зібрані докази згодом дозволять не лише довести, що ці злочини було вчинено, а й пов'язати їх із конкретними особами (злочинцями), висунути їм обґрунтовані обвинувачення та притягнути до відповідальності. Задokumentовані та поширені особисті історії людей, що зазнали насильство, жорстоке та нелюдське поводження, приниження людської гідності привернуть увагу недотичної частини суспільства до нестерпного збройного конфлікту та дасть можливість створити нові рекомендації та механізми захисту прав людини.

Роль OSINT дуже велика у сфері документування грубих порушень прав людини та воєнних злочинів. Неурядові організації, такі як Bellingcat¹⁴, Amnesty International та Human Rights Watch, стали піонерами у використанні відкритих даних для розслідування подій у зонах конфліктів, куди доступ для офіційних слідчих є обмеженим або неможливим. Ці організації, аналізуючи супутникові знімки, відео з соцмереж та дані з публічних реєстрів, спростовують офіційні версії подій та надають докази для міжнародних судів.

Ключовим моментом, що легітимізував OSINT як доказовий інструмент, стало рішення Європейського суду з прав людини (ЄСПЛ) у справі «Україна та Нідерланди проти Росії» (2022 р.). У цьому рішенні ЄСПЛ уперше визнав дані, отримані з відкритих джерел (зокрема, розслідування Bellingcat щодо збиття

¹² Авдеева Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності*: мат-ли наук.-практ. онлайн-семинару (Харків, 05.11.2020). Харків, 2020. С. 6–10.

¹³ Злочини, вчинені в період повномасштабного вторгнення рф станом на 20.01.26. URL: <https://www.gp.gov.ua/>

¹⁴ Bellingcat. URL: <https://www.bellingcat.com/>

рейсу МН17), повноцінними та надійними доказами. Суд сформулював три ключові критерії для оцінки таких доказів:

– авторитетність та досвід джерела (дослідницька група має володіти визнаною компетенцією у відповідній сфері);

– прозорість методології (чіткий опис того, як інформація була зібрана, перевірена та збережена);

– узгодженість з іншими доказами (співпадиння OSINT-даних з офіційними результатами слідства, свідченнями очевидців чи іншими матеріалами)¹⁵.

Національні суди у своїх рішеннях вже неодноразово посилались на матеріали OSINT як засоби отримання інформації, необхідної для розслідування кримінальних правопорушень. Так, в Івано-Франківському міському суді OSINT був використаний для доведення вини у колабораційній діяльності (справа № 344/19008/24). Суд посилався на рапорт оперуповноваженого, де було вказано на аналіз інформації з відкритих джерел, зокрема соцмережі «Вконтакте», для встановлення факту співпраці особи з окупаційною владою. У вирокі зауважено: «...під час здійснення контррозвідувальної діяльності отримано відомості щодо неправомірних дій громадянки України ОСОБА_7... діючи на шкоду суверенітетові... перейшла на бік ворога в умовах воєнного стану... відповідно до OSINT-аналізу матеріалів про фізичну особу N 4/1-2350 від 29.09.2022, була курсанткою (Вирок від 05.12.2024 № 344/19008/24 Івано-Франківський міський суд) Луганського державного університету внутрішніх справ, працювала на посаді поліцейського сектору реагування патрульної поліції у АДПЕСА 2»¹⁶.

2. В Основ'янському районному суді м. Харкова термін OSINT був прямо використаний для позначення методу ідентифікації особи, яка передавала ворогу координати ЗСУ (справа № 643/6925/24). У вирокі засвідчено: «...який зареєстрований на номер українського оператора мобільного зв'язку НОМЕР_3 та належить громадянині України ОСОБА_5... особу якого встановлено за допомогою можливостей OSINT-аналітики»¹⁷.

Аналіз цих судових рішень свідчить, що результати OSINT представлені в матеріалах кримінальних проваджень у формі довідок OSINT-аналізу, витягів із розвідки на основі відкритих джерел (OSINT), матеріалів OSINT-аналізу на фізичну особу, протоколів огляду комп'ютерних даних. Причому у більшості таких рішень посилаються не на документ як джерело даних OSINT, а на результати чи джерела, зібрані в результаті OSINT¹⁸. Така практика існує через

¹⁵ Радейко Р. І. Інструментарії OSINT у юридичній методології: теоретичні основи та практичне застосування. *Наукові записки Львівського університету бізнесу та права. Серія юридична*. 2024. Вип. 43. С. 400–410. DOI: <https://doi.org/10.5281/zenodo.15648723>

¹⁶ Вирок Івано-Франківського міського суду Івано-Франківської області від 05 грудня 2024 року у справі № 344/19008/24. URL: <https://reyestr.court.gov.ua/Review/123535737>

¹⁷ Вирок Основ'янського районного суду міста Харкова від 10 червня 2025 року у справі № 643/6925/24. URL: <https://reyestr.court.gov.ua/Review/127999232>.

¹⁸ Кудінов С. С., Шехавцов Р. М. Правове регулювання використання osint та його результатів під час встановлення обставин кримінальних правопорушень. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. № 3. С. 126–133. URL: <https://doi.org/10.32782/2311-8040/2025-3-14>. <http://journals.lvduvs.lviv.ua/index.php/law/article/view/1013>

відсутність визначення OSINT як інструменту одержання інформації про обставини події кримінального правопорушення в чинному законодавстві. Зазначене, на нашу думку, суперечить принципу правової визначеності у кримінальній процесуальній діяльності та діяльності уповноважених органів з виявлення та розслідування кримінальних правопорушень.

В сучасних реаліях воєнних та глобальних загроз усі практики у сфері міжнародного кримінального правосуддя повинні покращувати своє технічне розуміння новітніх технологій штучного інтелекту і повинні культивувати глибше сучасне розуміння застосування того, як соціальні мережі, геолокації, розмови мобільного зв'язку, комп'ютерна інформація та інші цифрові сліди й комунікації використовуються в зонах проведення воєнних дій¹⁹. Зважаючи на воєнну агресію російськими військами на територію України та вчинення ними масових вбивств, гвалтувань, мародерства, сьогодні гостро постає проблема збирання доказів воєнних злочинів. Це потребує активізації та поширення застосування технологій штучного інтелекту при виявленні, документуванні та розслідуванні воєнних злочинів, злочинів проти людяності та геноциду.

Застосування OSINT технологій в розслідуванні воєнних злочинів в Україні може бути корисним в багатьох аспектах. Основними напрямками, в яких ця технологія може бути використана, є такі:

– *аналіз супутникових знімків*. Штучний інтелект може допомогти аналізувати великі обсяги супутникових знімків для виявлення змін у ландшафті, зокрема будівель, доріг, об'єктів інфраструктури, які можуть бути пов'язані з воєнними злочинами, а також допомогти в ідентифікації місць, де можуть бути поховані тіла жертв воєнних злочинів²⁰;

– *аналіз відео- та фотоматеріалів*. Штучний інтелект може бути використано для аналізу великого обсягу відео- та фотоматеріалів, які були зняті на місцях вчинення воєнних злочинів, що, у свою чергу, може допомогти в ідентифікації підозрюваних та свідків, а також встановити, чи були зображені на них об'єкти, які можуть містити криміналістично-значущу інформацію для розслідування таких злочинів²¹;

– *обробка аудіоматеріалів*. За записами телефонних розмов та під час обробки аудіоматеріалів щодо розслідування воєнних злочинів штучний інтелект може допомогти в ідентифікації голосів, які містяться на таких носіях, а також визначити місця, де були здійснені ці розмови;

¹⁹ Авдеева Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності*: мат-ли наук.-практ. онлайн-семинару (Харків, 05.11.2020). Харків, 2020. С. 6–10.

²⁰ Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? / New Voice. 08.06.2022. URL: <https://nv.ua/ukr/opinion/viyuna-v-ukrajini-yakcifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html>

²¹ Штучний інтелект Мінцифри викрив окупанта, який потрапив у госпіталь в Кривому Розі – новини України, – LIGA.net URL: <https://tech.liga.net/ua/ukraine/novosti/iskusstvennyy-intellekt-mintsifry-razoblachil-okkupanta-popavshego-v-gospitalv-krivom-roge>

– *аналіз соціальних мереж*²². Аналізуючи соціальні мережі, штучний інтелект може допомогти виявити зв'язки між підозрюваними, які можуть бути пов'язані з воєнними злочинами, та ідентифікувати осіб, які можуть бути свідками воєнних злочинів або мати інформацію про них²³;

– *аналіз даних з медичних закладів*. Штучний інтелект може допомогти в ідентифікації тіл жертв воєнних злочинів, встановленні причини смерті, ідентифікації військовополонених, військових злочинців та їх пошук за даними про хворобу та відомостями про їх ідентифікаційні ознаки, які допомагають встановленню конкретної особи²⁴;

– *розпізнавання облич*. Штучний інтелект може бути використаний для розпізнавання облич на фото та відео з місць вчинення воєнних злочинів. Це може допомогти в ідентифікації підозрюваних, причетних до вчинення таких злочинів, та встановленню свідків, які можуть повідомити важливу інформацію про розслідувану подію воєнного злочину;

– *аналіз текстової інформації*. Аналіз штучним інтелектом текстової інформації (наприклад, повідомлень у соціальних мережах та інших джерелах), пов'язаної з воєнними злочинами, сприятиме ідентифікації підозрюваних і свідків та з'ясуванню криміналістично значущої інформації про воєнні злочини, які розслідуються²⁵.

Сучасні підходи до розслідування воєнних злочинів дають змогу визначити джерела цифрової інформації, якими зумовлено напрями збирання й дослідження цифрових слідів для отримання інформації: із мобільних пристроїв, вилучених в учасників кримінального провадження телефонів; із персональних комп'ютерів фізичних і юридичних осіб; із серверів та інших накопичувачів інформації в організаціях та установах; із радіочастотних ідентифікаторів, *GPS*-трекерів, датчиків, стаціонарних і мобільних вимірювальних пристроїв із використанням систем геолокації, відеоспостереження та позиціонування; із мережевих сервісів, що забезпечують голосовий і відеозв'язок між комп'ютерами через інтернет (*ICQ*, *Skype*, *WhatsApp*, *Viber*, *Telegram* та ін.); із банківських систем на цифрових носіях (*HDD*, *SSD*, флешкартках тощо); від стільникових операторів зв'язку щодо деталізації абонентського зв'язку й визначення місця знаходження абонента що

²² Духенюк О. М. Використання соціальних мереж у протидії злочинності – нові виклики і нові можливості. *Кримінальне та кримінальне процесуальне законодавство у контексті реформи кримінальної юстиції*: матеріали науково-практичного семінару (22 травня 2020 р.). Львів: ЛьвДУВС, 2020. С. 56–61.

²³ Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідуванні кіберзлочинів: криміналістичні проблеми. *Кримінальні загрози в секторі безпеки: практики ефективного реагування*: матеріали панельної дискусії III Харків. міжнар. юридичного форуму (м. Харків, 26 вересня 2019 р.); Нац. юрид. університет ім. Ярослава Мудрого. Х.: Право, 2019. С.142–146.

²⁴ Під Ізюмом знайшли братську могилу українських військових та понад 460 нових поховань. URL.: <https://hromadske.ua/posts/pid-izyumom-znajshli-bratsku-mogiluukrayinskikh-vijskovih-ta-ponad-460-novih-mogil-foto>

²⁵ Шевчук В.М. Перспективні напрями використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень. *Іноваційні методи та цифрові технології в криміналістиці та судовій експертизі*: монографія / В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін. ; за заг. ред. В. Ю. Шепітька ; Нац. акад. прав. наук України, НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса. Харків : Право, 2024. 208 с. С. 89.

допомогою геолокації; із записів камер відеоспостереження комерційних і державних структур; із вилучених в учасників кримінального провадження фотоапаратів і відеокамер.

У сучасних реаліях за цим же алгоритмом OSINT розвінчує міфи про так звану «спеоперацію» з «невмирущими» солдатами. Такі технології розпізнають обличчя трупів окупантів та знаходять їх в соцмережах, а автодозвони повідомляють родичів про їхню смерть. Міноборони України також розпочало використовувати технологію розпізнавання обличчя «Clearview AI», щоб розпізнавати російських нападників, боротися з дезінформацією, ідентифікувати загиблих та воєнних злочинців-окупантів²⁶. У воєнних реаліях повномасштабної військової агресії РФ на території України інструменти цифрової криміналістики значно допомагають у виявленні, розкритті та розслідуванні воєнних злочинів.

Гео-OSINT – це підвид відкритої розвідки (OSINT), що спеціалізується на зборі, обробці, аналізі та інтерпретації геопросторових даних, отриманих з відкритих джерел інформації. У сучасній криміналістиці, безпеці, розвідувальній діяльності та журналістських розслідуваннях Гео-OSINT набуває стратегічного значення як інструмент для отримання доказів, верифікації інформації та побудови ситуаційної обізнаності. На відміну від класичного OSINT, який охоплює широкий спектр відкритої інформації (новини, форуми, соціальні мережі, офіційні бази даних тощо), Гео-OSINT фокусується на даних, що мають географічну прив'язку.

До таких джерел належать:

- супутникові знімки (наприклад, з сервісів Sentinel, Landsat, Maxar);
- цифрові карти (Google Maps, OpenStreetMap, Bing Maps);
- геотеги в зображеннях і відео (EXIF-дані);
- дані про маршрути (GPS-треки, AIS-сигнали, ADS-B для авіації);
- соціальні медіа з геолокацією (Twitter, Instagram, TikTok);
- краудсорсингові платформи (Mapillary, Wikimapia);
- відкриті бази даних геоінформаційних систем (ГІС)²⁷.

Гео-OSINT полягає у виявленні просторових зв'язків між об'єктами, подіями та діями на основі їхнього місцезнаходження, часу фіксації та контексту. Наприклад, поєднання супутникового знімка з геотегованим відео з соціальних мереж дозволяє підтвердити факт події або відстежити переміщення техніки, людей, озброєння. З наукової точки зору, Гео-OSINT поєднує елементи геоінформатики, криміналістики, цифрової форензики, інформаційної аналітики та права.

Завдяки Гео-OSINT у роботі детектива можливе:

- відстеження маршрутів підозрюваних та транспортних засобів;
- ідентифікація місць скоєння правопорушень;

²⁶ Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі ? / New Voice. 08.06.2022. URL: <https://nv.ua/ukr/opinion/viyuna-v-ukrajini-yakcifrova-kriminalistika-vikrivaye-zlochini-uf-ukrajini-novini-ukrajini-50248411.html>

²⁷ Баганов Є. А. Сучасні можливості технології «OSINT» у кримінальному аналізі в умовах воєнного стану : дис. ... канд. юрид. наук / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2023. С. 7.

- встановлення зв'язків між локаціями, подіями та об'єктами;
- відтворення хронології подій за геолокаційними даними;
- моніторинг змін на місцевості з використанням супутникових знімків у різні проміжки часу²⁸.

У криміналістиці Гео-OSINT може бути використаний для:

- верифікації свідчень (наприклад, підтвердження присутності особи в певному місці);
- відстеження злочинних угруповань шляхом вивчення цифрових слідів у публічному просторі;

- створення кримінальних карт для аналізу «гарячих точок» злочинності;
- моделювання сценаріїв правопорушень у просторі та часі²⁹.

Застосовування Гео-OSINT використовує в комплексі такі інструменти:

- сервіси супутникової візуалізації (Sentinel Hub, Google Earth Pro, Zoom Earth);

- геоаналітичні платформи (ArcGIS, QGIS, MapInfo);

- інструменти виявлення координат зображень (ExifTool, FotoForensics);

- системи моніторингу соцмереж з фільтрацією за геотегами (GeoSocial Footprint, Hootsuite, Maltego)³⁰.

Гео-OSINT став популярним в роботі військових аналітиків, слідчих і детективів, Державної прикордонної служби, і зокрема під час розслідування воєнних злочинів. Так, геолокаційний аналіз фотографій у соціальних мережах дозволив міжнародним розслідувачам з Bellingcat підтвердити переміщення військової техніки під час збройних конфліктів.

3. OSINT і права людини: забезпечення верховенства права та підвищення ефективності захисту

Правильна робота з доказовою базою, зокрема, виявлення, збирання, документування, розслідування воєнних кримінальних правопорушень, обов'язково має здійснюватися із врахуванням міжнародного досвіду та європейських стандартів доказування³¹. При цьому, однією із проблем використання технологій

²⁸ Кисельов А. О. Тактика спілкування поліцейського з особами. The Top Actual Researches in Modern Science: Proceedings of the IInd International Scientific and Practical Conference (Ajman, July 28- 29, 2016, UAE). International Scientific and Practical Conference «World Science». 2016. № 8 (12). P. 23.

²⁹ Горелік Д. С., Кисельов А. О. Міжнародне співробітництво Національної поліції у сфері оперативно-розшукової діяльності. Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики: матеріали Всеукр. наук.-практ. конф. : у 2-х ч. (Дніпро, 19 жовт 2018 р.). Дніпро: Дніпроп.держ. ун-т внутр. справ, 2018. Ч. 1. С. 139–141.

³⁰ Москаленко Я., Кривошея Д., Дейкун О, Кисельов А. Гео-OSINT в кримінальному аналізі. Collection of Scientific Papers «SCIENTIA», (May 30, 2025; Glasgow, Scotland, UK). С. 89.

³¹ Шевчук В. М. Цифрові технології та європейський вектор розвитку криміналістики під час війни. Використання цифрових технологій у криміналістиці та судовій експертизі : матеріали міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р.: електрон. наук. вид. / [редкол.: В. Ю. Шепітько, Г. К. Авдєєва] ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. С та шиса НАПрН України. Харків: Право, 2024. С. 133–136.

OSINT під час досудового розслідування може бути порушення прав людини (щодо захисту конфіденційності особистих даних, втручання у приватне життя). Тому важливо не перебільшувати потенціал і переваги цих технологій, необхідно звернути увагу на можливі недоліки. Вбачаємо, що застосовувати OSINT у правоохоронній діяльності і судочинстві допустимо тільки за умови неухильного дотримання основних прав людини, принципів верховенства права і поваги до її честі й гідності, рівності перед законом і судом, змагальності сторін, прозорості, пропорційності, справедливості та неупередженості тощо.

Використання відкритих джерел інформації у розслідуванні воєнних злочинів супроводжується складним комплексом етичних, юридичних та процесуальних викликів, які вимагають особливо зваженого підходу. На відміну від традиційних слідчих методів, OSINT спирається на дані, що були створені, поширені або зібрані поза процесуальним контролем держави, нерідко приватними особами, журналістами, волонтерами або навіть органами, що переслідують пропагандистські цілі. Це підвищує доказовий потенціал, але одночасно створює ризики порушення прав людини, втручання у приватність, викриття свідків, поширення травматичного контенту та появи неперевіраних, неповних або маніпулятивних матеріалів. Саме тому Протокол Берклі наголошує на необхідності дотримання професійних, методологічних і етичних принципів під час роботи з відкритими джерелами, особливо у контексті міжнародних злочинів.

Єдиним ключовим постулатом для допустимості даних із відкритих джерел у доказуванні визначено забезпечення захисту прав обвинуваченого та справедливого судового розгляду (п. 55 Протоколу Берклі)³². Протокол Берклі (The Berkeley Protocol on Digital Open Source Investigations) – це практичний посібник з ефективного використання цифрової інформації з відкритим вихідним кодом при розслідуванні порушень міжнародного кримінального права, міжнародного права прав людини та міжнародного гуманітарного права, розроблений школою права Університету Каліфорнії в Берклі разом з представниками ООН. Протокол Берклі був розроблений за допомогою внесків осіб з різними професійними перспективами, юридичним та культурним походженням, статтю та національністю, та для його розробки було проведено понад 150 консультацій з експертами та отримано внесок від ключових зацікавлених сторін, включаючи слідчих ООН з прав людини. Спираючись на цей підхід до співпраці, Протокол Берклі включає міжнародні стандарти для проведення онлайн-досліджень щодо ймовірних порушень міжнародного права в області прав людини, міжнародного гуманітарного та кримінального права. Він також містить вказівки щодо методологій та процедур збору, аналізу та збереження цифрової інформації у професійному, юридичному та етичному порядку.

У цьому контексті для формування нормативно-правового забезпечення використання інструментів OSINT у кримінальному провадженні основоположне значення мають приписи ч. 2 ст. 6 та ст. 8 Конвенції про захист прав людини й основоположних свобод. Одним із ключових етичних вимірів є

³² Протокол Берклі. URL: <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf>.

питання *приватності* та *пропорційності*. OSINT-дослідник мимоволі має справу з даними, які можуть містити персональну інформацію: обличчя, голоси, локації, побутові деталі, поведінку людей, їхні соціальні зв'язки. Використання таких матеріалів повинно бути необхідним для досягнення конкретної процесуальної мети, а втручання – пропорційним. Якщо ідентифікація особи не є критично важливою для доведення події, доречно обмежитися групувою або рольовою атрибуцією; якщо контент містить дані, що можуть поставити людину під загрозу, необхідно вдаватися до деперсоналізації, розмиття деталей або часткового затемнення зображення. Ці підходи прямо відображені у положеннях Протоколу Берклі де підкреслюється, що захист цифрової, фізичної та психологічної безпеки всіх залучених осіб має превалювати над дослідницькими інтересами.

Не менш вагомим є аспект *вразливості жертв та свідків*. Матеріали, які з'являються у відкритому доступі, часто містять сцени насильства, наслідки атак, загиблих або поранених. Такий контент здатний спричинити ре-травматизацію не лише для родичів постраждалих, але й для самих аналітиків, які працюють з великою кількістю зображень. Тому протокол передбачає застосування етичних фільтрів: обмеження кола осіб, які мають доступ до графічних матеріалів, створення умов психологічної підтримки, маркування контенту та використання процедур, що мінімізують шкоду. Зокрема, наголошується на тому, що дослідник повинен відмовитися від копіювання та зберігання зайвих файлів, що не мають доказової цінності, щоб зменшити ризики витоку та неправомірного доступу.

Юридичні аспекти використання OSINT зумовлені необхідністю забезпечити *автентичність, цілісність і допустимість цифрових матеріалів*. Згідно з міжнародними стандартами та вимогами кримінального процесу, докази мають мати встановлене походження, бути зібраними належним суб'єктом або у спосіб, що не суперечить закону, а також зберігати незмінний стан від моменту виявлення до моменту подання у суд. У цьому контексті особливого значення набуває документування ланцюга збереження (chain of custody): фіксація часу отримання матеріалу, джерела, технічних параметрів, версій програмного забезпечення та будь-яких перетворень, яких зазнав файл. Протокол Берклі пропонує структуру таких процедур і підкреслює, що прозорість технічного процесу – одна з умов судової прийнятності цифрових доказів.

Питання *авторського контексту та намірів* також має юридичне значення. Матеріали з соціальних мереж можуть бути створені цивільними свідками, військовими, журналістами чи ворожими інформаційними структурами. Важливо оцінити, чи мав автор доступ до місця події, чи не порушені права третіх осіб, чи не є контент частиною пропагандистської операції. Водночас сам факт того, що матеріал був оприлюднений приватною особою, не усуває можливості його використання в процесі – за умови, що він належним чином верифікований, а його обробка відповідає міжнародним стандартам. Однак суди часто оцінюють не лише зміст, а й спосіб отримання доказів – отже, процесуальна дисципліна стає не менш важливою, ніж сам зміст матеріалу.

Окремий юридичний виклик становить проблема *маніпуляцій та дезінформації*. Цифровий простір насичений фейками, відредагованими відео,

підробленими метаданими та контентом, вивраним з контексту. Саме тому триангуляція незалежних джерел, аналіз історії появи контенту, реверсивний пошук зображень, встановлення раннях копій та робота з первинними файлами є обов'язковими складовими OSINT-розслідування. Протокол Берклі визначає ці процедури як базові методологічні стандарти, що забезпечують відтворюваність і незалежну перевірку надійності матеріалів.

Етичні дилеми виникають також у сфері публічної комунікації результатів. OSINT-розслідування часто проводяться в режимі, коли проміжні результати активно поширюються у медіа або соціальних мережах. Проте передчасне розкриття матеріалів може перешкодити офіційному розслідуванню, створити ризики для свідків або поставити під загрозу майбутні процесуальні дії. Тому дослідник зобов'язаний зважувати інтерес громади до доступу до інформації з інтересом правосуддя, а також дотримуватися принципу мінімальної достатності – публікувати лише те, що не зашкодить провадженню або особам, залученим до події. Ці вимоги перегукуються з етичними принципами безпечного використання цифрових джерел, які містяться у Протоколі Берклі.

Правова оцінка OSINT-матеріалів відбувається у контексті міжнародного гуманітарного та міжнародного кримінального права. Зокрема, для кваліфікації певної події як воєнного злочину необхідно не лише встановити факт нападу або руйнувань, але й підтвердити статус об'єкта (цивільний чи військовий), пропорційність застосованої сили, наявність умислу або грубої недбалості, а також зв'язок між дією і наслідками. У цьому сенсі цифрові докази можуть бути необхідними, але недостатніми – вони потребують узгодження з іншими видами доказів: показаннями свідків, результатами експертиз, огляду місця події та матеріалами офіційних джерел. Проте належно зібрані та верифіковані OSINT-матеріали здатні надати унікальні можливості для відтворення події, особливо якщо безпосередній доступ до місця злочину обмежений або небезпечний.

У підсумку підкреслимо, що юридичні та етичні аспекти використання OSINT не обмежуються технічною якістю файлів. Вони охоплюють питання приватності, безпеки, достовірності, правового статусу матеріалу, збалансованості втручання, відповідальності за наслідки публікації та методологічної прозорості. Саме дотримання цих принципів, сформульованих у *Berkeley Protocol on Digital Open Source Investigations*, дозволяє перетворити цифрові відкриті джерела на повноцінну доказову базу у розслідуванні воєнних злочинів і забезпечити сумісність результатів із міжнародними стандартами правосуддя.

ВИСНОВКИ

Системне впровадження OSINT у розслідування воєнних злочинів засвідчило здатність відкритих цифрових джерел забезпечувати швидке виявлення подій, побудову просторово-часової канви та формування переконливих аналітичних висновків, сумісних із процесуальними стандартами. Ретельно організовані процедури збору, збереження та верифікації матеріалів – від фіксації URL і часу доступу до обчислення хеш-значень і документування кожного перетворення файлу – перетворюють

«сирий» контент на доказовий ресурс, придатний до судового контролю. Ключовим каталізатором якості виступають уніфіковані професійні, методологічні та етичні принципи, що вимагають відтворюваності кроків, прозорості логіки та чіткого розмежування спостережуваних фактів і аналітичних інтерпретацій із позначенням рівнів впевненості.

Практика підтвердила, що саме комбінація різних OSINT-модальностей дає найвищу доказову віддачу: зображувальні матеріали, супутникові знімки, геопросторові шари та контент соціальних мереж взаємно підсилюють один одного, дозволяючи звузити «вікна часу», підвищити точність геолокації, ідентифікувати типи озброєння, підрозділи і навіть окремі одиниці техніки за унікальними ознаками. При цьому методична дисципліна – триангуляція джерел, робота з первинними копіями, опис інструментів і версій ПЗ, ведення «доріжки аудиту» – є безальтернативною умовою допустимості та достовірності цифрових доказів.

Разом із тим OSINT ставить перед правозастосуванням вимоги до етичної обачності: захист приватності, мінімізація шкоди для жертв і свідків, уважна робота з травматичним контентом, відповідальна публічна комунікація проміжних результатів. З огляду на чутливість цифрових даних саме баланс між доказовою цінністю і безпекою людей має визначати межі опрацювання та розкриття інформації. В юридичній площині вирішальними залишаються належний суб'єкт і спосіб збирання, неперервність ланцюга збереження, можливість незалежної реплікації методики перевірки та узгодженість з національними нормами і міжнародними стандартами.

З позиції стратегічного розвитку кримінальної юстиції пріоритетами є інституціоналізація єдиних національних протоколів роботи з цифровими відкритими джерелами, розбудова міжвідомчої OSINT -скосистеми, підготовка слідчих, прокурорів та суддів до роботи з цифровими доказами, а також інтеграція сумісних із міжнародною практикою інструментів і процедур. У такій конфігурації OSINT перестає бути «допоміжним» інструментом і стає повноцінною опорою доказування, здатною істотно підвищити ефективність розслідування воєнних злочинів у воєнний і повоєнний періоди та зміцнити довіру суспільства до правосуддя.

АНОТАЦІЯ

Стаття присвячена дослідженню можливостей використання OSINT технологій у діяльності органів кримінальної юстиції з розслідування воєнних злочинів у сучасних умовах збройних конфліктів в діяльності органів кримінальної юстиції. Акцент зроблено на інноваційних можливостях відкритих цифрових джерел і методиках їх практичного використання у процесуальному доведенні фактів порушення міжнародного гуманітарного права. Розкрито теоретико-правові засади застосування OSINT та наведено алгоритми роботи зі зображувальними матеріалами, супутниковими знімками, геопросторовими даними, соціальними мережами й іншими публічними цифровими ресурсами. Значну увагу приділено питанням автентичності та цілісності цифрових доказів, документуванню ланцюга збереження, використанню професійних підходів до геолокації та хронологізації подій, а

також методикам ідентифікації причетних осіб та військової техніки. Особливо висвітлено етичні та юридичні аспекти роботи з відкритими даними, включно із захистом приватності, мінімізацією ризиків ретравматизації, протидією маніпуляціям та забезпеченням відповідності міжнародним стандартам, зокрема Berkeley Protocol on Digital Open Source Investigations. Насамперед, такі технології поширюють можливість своєчасного повідомлення про правопорушення, розшуку і ідентифікації злочинців. На основі аналізу світових тенденцій цифрової трансформації діяльності органів кримінальної юстиції запропоновано системний підхід до впровадження використання OSINT технологій за даним напрямом. В роботі приділяється увага питанню узгодженості процесу тенденціям Євроінтеграції. Автор дійшов висновку, що системна імплементація OSINT у розслідування воєнних злочинів сприяє підвищенню ефективності кримінальної юстиції, розширює доказові можливості та забезпечує більш повне документування обставин кримінальних правопорушень у воєнний і повоєнний періоди.

Ключові слова OSINT; технологізація; інновації; воєнні злочини; кримінальна юстиція; цифрові докази; відкриті джерела інформації; супутникові знімки; геолокація; хронологізація; верифікація; ланцюг збереження; Berkeley Protocol; пропаганда; процесуальне доказування.

Література

1. OSINT-розвідка у роботі журналістів. URL: <https://youcontrol.com.ua/articles/osint-in-journalists-work/>.
2. Трансформація завдань криміналістики в умовах воєнного стану та євроінтеграційних процесів : зб. матеріалів наук.-практ. конф. присвяч. пам'яті д-ра юрид. наук, проф. В.О. Коновалової, м. Харків, 28 берез. 2024 р. / [редкол.: А. П. Гетьман, В. М. Шевчук, Є. Є. Демидова] ; Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків: Право, 2024. 148 с. URL: <https://ivpz.kh.ua/wp-content/uploads/2024/09/Трансформація-завдань-криміналістики-28.06.2024.pdf>
3. Методологічні засади криміналістики: традиції та новації : зб. матеріалів Криміналістичних читань, присвяч.пам'яті акад. В. О. Коновалової, м. Харків, 28 берез. 2025 р. Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики; Нац. акад. прав. наук України; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків: Право, 2025. 276 с. URL: https://ivpz.kh.ua/wp-content/uploads/2025/04/Kryminalistychni_chytannia_Konovalova_28.03.2025.pdf.
4. 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. 249 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/8875/1/07_05_2025.pdf.
5. OSINT та електронні докази: юридичні вимоги та практика застосування у кримінальних провадженнях щодо воєнних злочинів в Україні. 14.01.2026. URL:

<https://www.coe.int/uk/web/kyiv/-/osint-and-electronic-evidence-legal-requirements-and-practical-application-in-criminal-proceedings-on-war-crimes-in-ukraine>.

6. Протокол Берклі. URL: <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf>.

7. Галина Авдєєва, Ельжбета Живуцька-Козловська. Проблеми використання цифрових доказів у кримінальному судочинстві України та США (2023). URL: <https://khrife-journal.org/index.php/journal/article/download/564/633>.

8. Використання OSINT у доказуванні командної відповідальності за міжнародні злочини: навчання НПУ. 08.10.2025. URL: <https://npu.gov.ua/news/vykorystannia-osint-u-dokazuvanni-komandnoi-vidpovidalnosti-za-mizhnarodni-zlochyny-navchannia-npu>.

9. Дуфенюк О. Розслідування воєнних злочинів: логістичні, криміналістичні та судово-медичні питання. *Юридичний науковий електронний журнал*. 2022. № 4. С. 369–374. DOI: 10.32782/2524–0374/2022–4/88.

10. Шепітько В. Ю. Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору. *Право України*. 2022. № 2. С. 87-90.

11. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки: Указ президента України від 11.05.2023 № 273/2023. URL: <https://www.president.gov.ua/documents/2732023-46733>.

12. Президент України схвалив Комплексний стратегічний план реформування органів правопорядку (12.05.2023). URL: <https://www.gp.gov.ua/ua/posts/prezident-ukrayini-sxvaliv-kompleksnii-strategicnii-plan-reformuvannya-organiv-pravoporyadku>.

13. Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності: мат-ли наук.-практ. онлайн-семінару* (Харків, 05.11.2020). Харків, 2020. С. 6–10.

14. Злочини, вчинені в період повномасштабного вторгнення рф станом на 22.12.23. URL: <https://www.gp.gov.ua>.

15. Bellingcat. URL: <https://www.bellingcat.com/>

16. Радейко Р. І. Інструментарій OSINT у юридичній методології: теоретичні основи та практичне застосування. *Наукові записки Львівського університету бізнесу та права. Серія юридична*. 2024. Вип. 43. С. 400–410. DOI: <https://doi.org/10.5281/zenodo.15648723>.

17. Вирок Івано-Франківського міського суду Івано-Франківської області від 05 грудня 2024 року у справі № 344/19008/24. URL: <https://reyestr.court.gov.ua/Review/123535737>.

18. Вирок Основ'янського районного суду міста Харкова від 10 червня 2025 року у справі № 643/6925/24. URL: <https://reyestr.court.gov.ua/Review/127999232>.

19. Кудінов С. С., Шехавцов Р. М. Правове регулювання використання osint та його результатів під час встановлення обставин кримінальних правопорушень. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. № 3. С. 126–133. DOI: <https://doi.org/10.32782/2311-8040/2025-3-14>

20. Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? / New Voice. 08.06.2022. URL: <https://nv.ua/ukr/opinion/viyna-v-ukrajini-yakcifrova-kriminalistika-vikrivayev-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html>

21. Штучний інтелект Мінцифри викрив окупанта, який потрапив у госпіталь в Кривому Розі – новини України, – LIGA.net URL: <https://tech.liga.net/ua/ukraine/novosti/iskusstvennyu-intellekt-mintsifry-razoblachil-okkupanta-poravshego-v-gospitalv-krivom-roge>.

22. Дуфенюк О. М. Використання соціальних мереж у протидії злочинності – нові виклики і нові можливості. *Кримінальне та кримінальне процесуальне законодавство у контексті реформи кримінальної юстиції*: матеріали науково-практичного семінару (22 травня 2020 р.). Львів: ЛьвДУВС, 2020. С. 56–61.

23. Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідуванні кіберзлочинів: криміналістичні проблеми. *Кримінальні загрози в секторі безпеки: практики ефективного реагування*: матеріали панельної дискусії III Харків. міжнар. юридичного форуму (м. Харків, 26 вересня 2019 р.); Нац. юрид. університет ім. Ярослава Мудрого. Х.: Право, 2019. С.142–146.

24. Шевчук В. М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. *Military offences and war crimes: background, theory and practice*: Scientific monograph. Riga, Latvia: «Baltija Publishing», 2023. С. 795-823. URL: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/322/8791/18392-1>.

25. Під Ізюмом знайшли братську могилу українських військових та понад 460 нових поховань. URL: <https://hromadske.ua/posts/pid-izyumom-znajshli-bratsku-mogiluukrayinskih-vijskovih-ta-ponad-460-novih-mogil-foto>.

26. *Інноваційні методи та цифрові технології в криміналістиці та судовій експертизі*: монографія / В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін. ; за заг. ред. В. Ю. Шепітька ; Нац. акад. прав. наук України, НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса. Харків : Право, 2024. 208 с. С. 89.

27. Батанов Є. А. Сучасні можливості технології «OSINT» у кримінальному аналізі в умовах воєнного стану: дис. ... канд. юрид. наук / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2023. 205 с.

28. Кисельов А. О. Тактика спілкування поліцейського з особами. The Top Actual Researches in Modern Science: Proceedings of the IInd International Scientific and Practical Conference (Ajman, July 28- 29, 2016, UAE). International Scientific and Practical Conference «World Science». 2016. № 8 (12). P. 25–28.

29. Горелік Д. С., Кисельов А. О. Міжнародне співробітництво Національної поліції у сфері оперативно-розшукової діяльності. Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики : матеріали Всеукр. наук.-практ. конф.: у 2-х ч. (Дніпро, 19 жовт 2018 р.). Дніпро: Дніпроп.держ. ун-т внутр. справ, 2018. Ч. 1. С. 139–141.

30. Москаленко Я. , Кривошея Д. , Дейкун О, Кисельов А. Гео-OSINT в кримінальному аналізі. Collection of Scientific Papers «SCIENTIA», (May 30, 2025; Glasgow, Scotland, UK). С. 85–91.

31. Шевчук В. М. Цифрові технології та європейський вектор розвитку криміналістики під час війни. *Використання цифрових технологій у криміналістиці та судовій експертизі*: матеріали міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р.: електрон. наук.-практ. вид. / [редкол.: В. Ю. Шепітько, Г. К. Авдєєва]; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. С ташиса НАПРН України. Харків: Право, 2024. С.133–136.

22. Shevchuk, V., Morozova, T., Chorny, H., Nehrebetskyi, V., and Slobodeniuk, I. Artificial Intelligence in Criminal Proceedings: Criminalistics, Criminal Procedure and Psychology Issues / V. Shevchuk та ін. *International Annals of Criminology*. 2025. С. 1–19. URL: <https://doi.org/10.1017/cri.2025.10090>.

23. Shevchuk, V., Dunaev, O., Tyshchenko, O., Biletska, G., and Nehrebetskyi, V. Innovative Methods in the Identification of Deceased Persons during Armed Conflicts and Disasters: Criminalistic and Forensic Medical Issues / V. Shevchuk et al. *International Annals of Criminology*. 2025. С. 1–20. URL: <https://doi.org/10.1017/cri.2025.10094>.

Information about the author:

Nehrebetskyi Vladyslav Valerevych,

Ph. D. in Law,

Associate Professor at the Department of Criminalistics

Yaroslav Mudryi National Law University

77, Pushkinska str., Kharkiv, 61024, Ukraine,

Researcher at Academician Stashis Scientific Research Institute

for the Study of Crime Problems

National Academy of Law Sciences of Ukraine

49, Pushkinska str., Kharkiv, 61002, Ukraine