УДК 343.97"363"

ГУЦАЛЮК М.В., *кандидат юридичних наук, доцент, старший науковий співробітник*, провідний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України
ORCID: https://orcid.org/0000-0003-4496-5173
СЕМЕНОВ В.В., *кандидат юридичних наук, доцент*, Національна академія внутрішніх справ
ORCID: https://orcid.org/0000-0003-2036-3450
ЧУПРИНА О.В., *Ph.D. доцент*, Національний університет оборони України
ORCID: https://orcid.org/0000-0001-6349-9361

OSINT У ГІБРИДНИХ КОНФЛІКТАХ: ІНСТРУМЕНТ ДОКУМЕНТУВАННЯ ЗЛОЧИНІВ ТА ВИКЛИКИ ПРАВОВОГО ВИЗНАННЯ

DOI: https://doi.org/10.37750/2616-6798.2025.4(55).346497

Анотація. *У статті проаналізовано роль OSINT (розвідки/розслідування з відкритих джерел) у виявленні та документуванні злочинної діяльності у контексті гібридних конфліктів XXI століття. Розглянуто приклади ефективного застосування OSINT у розслідуваннях воєнних злочинів, кібератак і порушень міжнародного гуманітарного права. Проаналізовано стандарти цифрової доказової бази, зокрема Berkeley Protocol, та інтеграцію OSINT у роботу міжнародних правозастосовних органів. Запропоновано висновки щодо нормативного регулювання та перспектив удосконалення використання OSINT в умовах сучасних загроз.*

Ключові слова*: OSINT, гібридний конфлікт, електронні докази, кібератаки, воєнні злочини, Berkeley Protocol, Bellingcat.*

Summary. *The article analyses the role of OSINT (Open Source Intelligence/Investigations) in detecting and documenting criminal activity in the context of 21st-century hybrid conflicts. It examines case studies of effective OSINT application in the investigation of war crimes, cyberattacks, and violations of international humanitarian law. Particular attention is paid to standards for digital evidence, notably the Berkeley Protocol, and the integration of OSINT into the work of international law enforcement bodies. The article offers conclusions regarding legal regulation and the prospects for improving the use of OSINT in response to contemporary threats.*

Keywords: *OSINT, hybrid conflict, electronic evidence, cyberattacks, war crimes, Berkeley Protocol, Bellingcat.*

Постановка проблеми. Гібридні конфлікти XXI століття радикально змінили природу сучасних збройних протистоянь, об’єднуючи елементи традиційної війни з кіберопераціями, інформаційно-психологічними впливами, кампаніями дезінформації, підривною економічною діяльністю та втручанням у внутрішні справи суверенних держав. Такий комплексний характер гібридних загроз створює суттєві виклики для виявлення, документування та доказування злочинів, зокрема порушень міжнародного гуманітарного права, актів агресії та масових воєнних злочинів.

У цих умовах особливої актуальності набуває використання відкритих джерел інформації (OSINT — Open Source Intelligence) як альтернативного або додаткового інструмента збирання доказів. OSINT дозволяє оперативно фіксувати події у майже реальному часі, аналізувати цифрові сліди, ідентифікувати причетних осіб, навіть у

випадках відсутності контролю над відповідною територією або фізичного доступу до об’єкта злочину.

Попри високу ефективність OSINT у практичному застосуванні - від журналістських розслідувань до дій національних та міжнародних правоохоронних органів - в українському правовому полі все ще відсутнє належне нормативне закріплення цього підходу. Зокрема, Кримінальний процесуальний кодекс України не містить визначення ні поняття OSINT, ні терміну “електронні докази”, що створює прогалини в процесуальному забезпеченні доказування в умовах гібридної війни.

Результати аналізу наукових публікацій. Аналіз наукових публікацій засвідчує зростаючий інтерес до тематики OSINT у контексті гібридних конфліктів, зокрема щодо його застосування для документування воєнних злочинів, протидії кіберзагрозам, моніторингу порушень прав людини та інформаційної безпеки. Дослідники розглядають OSINT не лише як технічний інструмент збору інформації, а як повноцінну методологію аналізу, яка поєднує краудсорсинг, цифрову криміналістику, машинне навчання, верифікацію джерел і правовий супровід зібраних матеріалів.

Зокрема, у працях Пучкова, Ланде та Субача (КПІ) [1] досліджується роль OSINT у запобіганні кіберінцидентам і виявленні технічних індикаторів атак, включаючи IP-адреси, домени та фішингову активність. Жмур і Землянікіна (НАУ) [2] здійснили ретроспективний огляд становлення технології OSINT, виокремивши її етапи розвитку в контексті інформаційної війни. Івкова та Опірський (Львівська політехніка) аналізують сучасні автоматизовані інструменти OSINT, а також проблеми їхньої адаптації до українських реалій [3].

У міжнародній науковій літературі значна увага приділяється використанню OSINT у контексті збройного конфлікту між Росією та Україною. Наприклад, дослідження E. Dincelli та ін. присвячене етичному хакінгу для гуманітарних цілей - розшуку зниклих осіб за допомогою OSINT [4]. J. Hauter запропонував концепцію "forensic conflict studies", де OSINT слугує основним джерелом реконструкції подій у зонах конфліктів у цифрову епоху [5].

Водночас низка публікацій наголошує на ризиках, пов’язаних із неналежною верифікацією даних, правовим статусом цифрових доказів, етичною відповідальністю дослідників, а також відсутністю нормативної бази для легітимного використання результатів OSINT у судовому процесі. Ці виклики актуалізують потребу в гармонізації національного законодавства з міжнародними стандартами, зокрема положеннями Berkeley Protocol on Digital Open Source Investigations, який встановлює правила автентифікації, збереження метаданих, дотримання етики і забезпечення ланцюга зберігання цифрових доказів (chain of custody).

Таким чином, науковий дискурс підтверджує важливість OSINT як ключового інструменту документування злочинів у гібридних конфліктах, водночас вказуючи на необхідність подальшої правової, технологічної та методологічної інституціоналізації цього підходу.

Метою статті є комплексний аналіз потенціалу та практичного застосування OSINT (розвідки/розслідування з відкритих джерел) як інструменту виявлення, документування та доказування злочинів у контексті гібридних конфліктів, зокрема воєнних злочинів, кібератак та порушень міжнародного гуманітарного права. Стаття також спрямована на дослідження нормативно-правових, методологічних і етичних аспектів інтеграції OSINT у національні та міжнародні правозастосовні практики, а також на визначення перспектив його подальшого впровадження в українську систему

кримінального правосуддя з урахуванням міжнародних стандартів, зокрема Berkeley Protocol.

Виклад основного матеріалу. Одним із найбільш ефективних та динамічних інструментів сучасного інформаційного аналізу є розвідка з відкритих джерел - OSINT (Open Source Intelligence). У практиці журналістики, криміналістики та правозахисної діяльності нерідко використовується термін "розслідування з відкритих джерел", що акцентує увагу на фактичному встановленні подій або обставин. Водночас у військовій, аналітичній та розвідувальній сфері переважає термін "розвідка", який відображає системну обробку, оцінку та інтерпретацію даних з відкритих джерел з метою формування аналітичного продукту. Незважаючи на термінологічні розбіжності, обидва підходи відображають одну методологічну основу - використання доступної публічної інформації для виявлення, підтвердження або пояснення фактів, подій та явищ.

У контексті гібридних загроз OSINT трансформувався з допоміжного інструмента у повноцінний метод збору доказів, який активно використовується як журналістськими ініціативами, так і правоохоронними та судовими органами на національному та міжнародному рівнях. OSINT передбачає систематичний збір, аналіз, верифікацію та збереження інформації з відкритих джерел, зокрема:

- соціальних мереж (Twitter/X, Telegram, Facebook, TikTok);
- відеохостингів (YouTube, Vimeo);
- супутникових знімків (Maxar, Planet Labs);
- цифрових медіа та інформаційних порталів;
- урядових і корпоративних вебресурсів;
- відкритих баз даних, реєстрів та метаданих;
- тематичних форумів, зокрема в Даркнеті;
- друкованої преси;
- радіо;
- телебачення тощо.

Особливістю OSINT у гібридних конфліктах є можливість виявляти, документувати й підтверджувати факти злочинів у режимі майже реального часу, а також встановлювати цифрові сліди причетних осіб або угруповань. Застосування OSINT охоплює декілька ключових напрямів: геолокаційний аналіз (наприклад, визначення місць ударів чи пересування техніки), хронологічна реконструкція подій, ідентифікація підозрюваних за допомогою розпізнавання облич або профілів у соцмережах, а також технічна атрибуція кібератак.

Яскравим прикладом ефективного застосування OSINT став кейс розслідування авіакатастрофи рейсу MH17. Незалежне дослідницьке об'єднання Bellingcat на основі відкритих даних (фото, відео, супутникових зображень, геолокацій) зуміло довести переміщення ЗРК "Бук" із території Російської Федерації до тимчасово окупованої частини Донбасу, його участь у знищенні літака, а також ідентифікувати конкретних військовослужбовців РФ, що були до цього причетні [6].

З початком повномасштабного вторгнення рф в Україну у 2022 році OSINT почав масово використовуватися неурядовими організаціями, волонтерами та слідчими органами для документування злочинів проти цивільного населення. Так, відео з Telegram, фото із соціальних мереж, супутникові знімки стали доказовою базою у кримінальних провадженнях щодо обстрілів населених пунктів, руйнування житлових будинків, шкіл, лікарень та інших об'єктів цивільної інфраструктури. Зібрані дані стали основою для створення детальних звітів, аналітичних досліджень та матеріалів, які передаються до національних і міжнародних правових інституцій. Висока точність

геолокаційних даних, хронологічна конкретність відомостей та можливість верифікації матеріалів зробили OSINT важливим інструментом для фіксації злочинів, підвищення рівня транспарентності розслідувань та забезпечення невідворотності покарання для винних.

У кіберпросторі OSINT забезпечує аналіз та атрибуцію кібератак, моніторинг деструктивної діяльності угруповань типу KillNet, збір технічних індикаторів (IP-адрес, доменів, фішингових кампаній), а також виявлення загроз у даркнеті. Інформація, здобута за допомогою OSINT, дозволяє CERT-групам, правоохоронцям та міжнародним структурам (наприклад, Europol чи ENISA) своєчасно реагувати на кіберзагрози.

У зв'язку зі зростанням значущості електронних доказів, міжнародна спільнота почала напрацьовувати відповідні нормативно-етичні стандарти використання OSINT у кримінальному правосудді. Визначальною подією стало ухвалення у 2020 році Berkeley Protocol on Digital Open Source Investigations, розробленого спільно UC Berkeley Human Rights Centre та Управлінням Верховного комісара ООН з прав людини (OHCHR) [7]. Цей Протокол регламентує ключові принципи:

- забезпечення автентичності джерел та неперервності ланцюга зберігання доказів (chain of custody);
- збереження метаданих;
- верифікація інформації та джерел;
- дотримання етичних стандартів, зокрема недопущення шкоди свідкам та потерпілим.

Сьогодні OSINT дедалі активніше інтегрується у роботу міжнародних інституцій: Міжнародного кримінального суду, Організації Об'єднаних Націй, Human Rights Watch, Europol (через платформу SIRIUS), INTERPOL, а також спеціалізованих трибуналів.

Таким чином, OSINT стає не лише технічним інструментом, а й новою парадигмою доказування у міжнародному кримінальному праві, що дозволяє документувати злочини навіть у недосяжних фізично регіонах, з високою точністю, оперативністю та доказовою якістю.

Разом з цим у чинному Кримінальному процесуальному кодексі України відсутнє поняття OSINT. Більше того, відсутнє і поняття електронних доказів, відносно чого тривають гострі наукові дискусії [8].

Проте сучасна ситуація вимагає прийняття нових методів реагування на новітні виклики та загрози [9]. Адже зловмисники, особливо у випадку воєнних злочинів, цілеспрямовано знищують докази або маніпулюють ними. Наприклад, масові поховання часто приховуються, об'єкти цивільної інфраструктури - добудовуються або реконструюються.

Також у гібридних конфліктах часто діють незареєстровані, "анонімні" формування, які не мають офіційного статусу армії. У кібервійні — злочини часто вчиняються через ботнети, VPN, інфраструктуру в інших юрисдикціях, що ускладнює ідентифікацію виконавців і встановлення їхньої відповідальності.

Для традиційного кримінального переслідування необхідно:

- мати контроль над територією, де вчинено злочин;
- зібрати допустимі з правової точки зору докази;
- забезпечити безпеку свідків;
- отримати міжнародну правову допомогу, яка часто є тривалою та забюрократизованою.

У випадках кібератак або вчинення воєнних злочинів в умовах гібридної війни класичні методи розвідки та збирання доказової інформації часто виявляються

малоефективними або зовсім непридатними. Відсутність фізичного доступу до зони бойових дій, сувора контрольованість інформаційного простору агресором, а також високі ризики для агентурного апарату зумовлюють необхідність використання альтернативних інструментів, серед яких відкриті джерела інформації (OSINT) відіграють дедалі важливішу роль.

Яскравим прикладом ефективного застосування OSINT є безпрецедентна операція, проведена незалежною данською журналістською організацією Danwatch у співпраці з низкою європейських медіа. У межах цієї журналістської ініціативи було отримано та оприлюднено понад 2 мільйони документів, що містили вкрай чутливу інформацію щодо модернізації інфраструктури російського ядерного арсеналу.

Проаналізовані матеріали включали докладні креслення, інженерні плани та логістичну документацію ядерних баз, зокрема: системи багаторівневих фізичних бар'єрів (потрійні заземлені паркани), засоби виявлення радіаційного забруднення, укріплені входи, дистанційно керовані кулеметні й гранатометні установки, а також опис розміщення й готовності ядерних боєголовок, що можуть бути застосовані з різних платформ – наземних, морських та авіаційних. У документах також фіксувалася активність військового персоналу, що обслуговує ці комплекси. Витік автентичних креслень і логістичної інформації засвідчив вразливість систем безпеки російських ядерних об'єктів до кібератак, інформаційних вторгнень та внутрішніх техногенних загроз [10].

Зазначені дані, за своєю природою, не могли бути отримані за допомогою традиційних засобів супутникової розвідки, агентурної мережі чи технічного прослуховування. Їхній збір і верифікація стали можливими виключно завдяки методам OSINT, що передбачають аналітичне опрацювання масивів відкритої або напіввідкритої цифрової інформації, зокрема витоків, метаданих і цифрових слідів.

В Україні після початку повномасштабної агресії рф OSINT став не просто допоміжним, а ключовим інструментом у розслідуванні злочинів у гібридних конфліктах. При цьому важливо дотримуватися допустимості доказів, адже суди не завжди визнають OSINT, якщо порушено процедуру автентифікації.

Ефективність OSINT залежить від:

- стандартизації процедур збору та обробки даних;
- навчання фахівців (слідчих, прокурорів, суддів);
- розвитку міжнародного співробітництва.

У сучасних умовах цифровізації доказового процесу OSINT постає не лише як інструмент оперативного збору інформації, а як феномен нової доказової парадигми, що поєднує елементи інформаційної безпеки, цифрової криміналістики та правового аналізу. У контексті теорії доказового права OSINT змінює уявлення про джерела, допустимість і достовірність доказів: дані з відкритих джерел дедалі частіше слугують основою для формування судових рішень, навіть за відсутності класичних речових чи письмових доказів. А у сфері цифрової криміналістики, OSINT інтегрується як метод виявлення, фіксації, аналізу та збереження цифрових слідів, що часто є єдиними доказами у випадках воєнних злочинів або кібератак. Таким чином, OSINT перетворюється на міждисциплінарну категорію, яка вимагає оновлення правових підходів до визначення, допустимості та легітимності цифрових доказів у кримінальному процесі.

Окремої уваги потребують ризики зловживань у сфері OSINT, зумовлені як технічними, так і етичними чинниками. Зокрема, з розвитком технологій штучного інтелекту зростає загроза використання DeepFake-контенту, здатного імітувати голос,

обличчя або дії конкретних осіб з високим ступенем достовірності. Водночас фальсифікація метаданих (дати, геолокації, авторства) або навмисне викривлення джерела інформації може призвести до хибної атрибуції злочинців, коли невинні особи помилково ідентифікуються як винні. Така ситуація не лише нівелює доказову цінність матеріалів, а й підриває довіру до OSINT у судовому процесі. У зв'язку з цим постає потреба у суворих стандартах верифікації цифрових джерел - перевірки автентичності, ланцюга зберігання збереження первинних даних, а також залучення кваліфікованих експертів до процесу аналізу. Без належної процедурної легалізації та незалежної експертизи використання OSINT у кримінальному правосудді може не лише виявитися неефективним, а й становити загрозу для прав людини та верховенства права.

Україна має потенціал стати прикладом для інших держав у впровадженні OSINT-підходів до документування злочинів, скоєних у зоні збройного конфлікту, у кіберпросторі, а також у сфері транснаціональної злочинності та порушень міжнародного гуманітарного права.

Важливу роль у впровадженні OSINT у практичну діяльність правоохоронних органів відіграє Національний координаційний центр кібербезпеки РНБО України. Діяльність НКЦК у цьому напрямі суттєво активізувалась після військової агресії рф [11].

Комплексне використання відкритих джерел – відео та фотоматеріалів із соціальних мереж, супутникових знімків, метаданих, геолокаційної інформації, записів із публічних камер спостереження – дозволяє створювати достовірну доказову базу, що може бути використана у національних та міжнародних судових провадженнях, зокрема Міжнародним кримінальним судом та спеціалізованими трибуналами.

Систематичний розвиток OSINT-практик в Україні в умовах повномасштабної війни сприяє формуванню нової парадигми документування воєнних злочинів, яка поєднує цифрові технології, краудсорсинг (збір фото, відео, повідомлень від очевидців подій через соціальні мережі, чат-боти, спеціальні платформи) та аналітичну експертизу. У цьому контексті Україна може не лише адаптувати найкращі міжнародні стандарти, а й стати джерелом інновацій для формування глобальної нормативної та методологічної бази у сфері застосування OSINT у правозастосовній діяльності та міжнародному правосудді.

Висновки.

OSINT утвердився як один із ключових інструментів документування злочинної діяльності у контексті гібридних конфліктів XXI століття. Його переваги - оперативність, доступність, цифрова масштабованість і здатність функціонувати в умовах обмеженого або відсутнього фізичного доступу до місця події.

Ефективність OSINT доведено на практиці у численних кейсах - від міжнародних журналістських розслідувань (Bellingcat, Danwatch) до кримінальних проваджень в Україні щодо воєнних злочинів, скоєних під час збройної агресії РФ. Такі приклади засвідчують потенціал OSINT як джерела доказів, здатного доповнювати або заміщувати традиційні методи розвідки та слідства.

Водночас залишається низка викликів щодо правового статусу OSINT-даних як доказів у судовому процесі. Зокрема, українське законодавство не містить чіткого визначення OSINT, а відсутність стандартизованих процедур автентифікації, збереження метаданих і забезпечення безперервного ланцюга зберігання (chain of custody) обмежує можливості повноцінного використання таких матеріалів у кримінальному провадженні.

Важливу роль як етичний і процедурний орієнтир для забезпечення достовірності, правомірності та захищеності даних, отриманих із відкритих джерел відіграє Berkeley Protocol on Digital Open Source Investigations (протокол Берклі). Інтеграція його положень у національне законодавство та практику правоохоронних органів України є необхідною умовою підвищення якості розслідувань і довіри до цифрових доказів.

Україна має унікальний досвід та потенціал для формування сучасної моделі застосування OSINT у сфері протидії злочинам у гібридних конфліктах. У довгостроковій перспективі OSINT може стати основою нової парадигми кримінального правосуддя у цифрову епоху, що поєднує технологічні можливості, етичні стандарти та міжнародне співробітництво.

На основі отриманого досвіду в умовах гібридної війни перспективним напрямом є уніфікація та експорт напрацювань як прикладу ефективного реагування на злочинну діяльність. Подальші дослідження потребують розробки методики процесуальної легалізації цифрових доказів, здобутих за допомогою OSINT, створення національного стандарту верифікації відкритих джерел, а також вивчення OSINT як інструменту не лише розслідування, але й попередження кібер- та воєнних злочинів.

Використана література

1. Puchkov O., Lande D., Subach I. OSINT investigation to detect and prevent cyber attacks and cyber security incidents URL: https://ela.kpi.ua/items/a9d6917b-42b2-4f08-8ceb-64e27248e367

2. Жмур Н., Землянікіна М. Історія становлення та сучасний стан технології пошуку інформації OSINT URL: https://jrnl.nau.edu.ua/index.php/UV/article/view/16895

3. Ivkova V., Opirskyy I. Research of Existing Osint Tools and Approaches in the Context of Personal and State Information Security URL: https://science.lpnu.ua/csn/all-volumes-and-issues/volume-7-number-1-2025/research-of-existing-osint-tools-and-approaches-in-the-context-of-personal-and-state-information-security

4. Dincelli E., Van Slyke C., Yayla A. Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and OSINT Tools URL: https://aisel.aisnet.org/cais/vol53/iss1/49/

5. Jakob Hauter Forensic conflict studies: Making sense of war in the social media age URL: https://journals.sagepub.com/doi/full/10.1177/17506352211037325

6. Ludo Block Solving the MH17 and the Skripal Case: How Bellingcat Demonstrates the Power of OSINT URL: https://www.leidensecurityandglobalaffairs.nl/articles/solving-the-mh17-and-the-skripal-case-how-bellingcat-demonstrates-the-power?utm_source=chatgpt.com; Yuliya Ilyuk Journalistic Investigations in the Digital Age of Post-Truth Politics: the Analysis of Bellingcat's Research Approaches Used for the (Re)construction of the MH17 case URL: https://journals.ehu.lt/index.php/perekrestki/article/view/977?utm_source=chatgpt.com

7. United Nations Office of the High Commissioner for Human Rights. (2020). Berkeley Protocol on Digital Open Source Investigations. URL: https://www.ohchr.org

8. Гуцалюк М.В. Антонюк П.Є. Проблемні аспекти процесуальної спроможності використання електронної (цифрової) інформації як доказів в кримінальному провадженні // Інформація і право. – № 2(41)/2022. – С.116-122. https://doi.org/10.37750/2616-6798.2022.2(41).270373

9. Гуцалюк М. В. Кіберзагрози під час гібридної війни та протидія організованій кіберзлочинності // Інформація і право. - № 1(52)/2025. – С. 123-131. DOI: https://doi.org/10.37750/2616-6798.2025.1(52).324708 http://il.ippi.org.ua/article/view/324708

10. Massive security breach: Russian nuclear facilities exposed online URL: https://danwatch.dk/en/serious-security-breach-russian-nuclear-facilities-exposed/

11. За сприяння НКЦК представники органів сектору безпеки і оборони розпочали навчання з імплементації інструментарію OSINT URL: https://www.rnbo.gov.ua/ua/Diialnist/5850.html?utm_source=chatgpt.com