ISSN 2311-8040

УДК 343.985
DOI https://doi.org/10.32782/2311-8040/2025-3-14

**Кудінов Сергій Сергійович,**
доктор юридичних наук, професор,
головний науковий співробітник,
Державна наукова установа
«Інститут інформації, безпеки і права Національної академії правових наук України»;
експерт громадської організації «Safe Ukraine 2030»;
радник SK «Security»,
провулок Нестеровський, 4, Київ, 04053, Україна
ORCID: https://orcid.org/0000-0002-0582-1030

**Шехавцов Руслан Миколайович,**
кандидат юридичних наук, професор,
доцент кафедри кримінального процесу та криміналістики,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: https://orcid.org/0000-0002-4756-9849

# ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ OSINT ТА ЙОГО РЕЗУЛЬТАТІВ ПІД ЧАС ВСТАНОВЛЕННЯ ОБСТАВИН КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

***Анотація.*** *У статті на основі вивчення історії розвитку використання розвідки з відкритих джерел (OSINT) – від одержання даних про соціальні, економічні, управлінські процеси до даних про вчинення воєнних злочинів, на підставі узагальнення зарубіжних та вітчизняних літературних джерел, які містять дані про особливості здійснення OSINT та використання його результатів для встановлення обставин вчинення воєнних злочинів; нормативно-правових актів у сферах оперативно-розшукової діяльності та кримінальної юстиції; вітчизняної практики використання OSINT для встановлення обставин кримінальних правопорушень оперативними підрозділами та органами досудового розслідування Національної поліції України, СБУ, НАБУ, ДБР, БЕБ, а також судами у кримінальних провадженнях, з метою забезпечення принципу правової визначеності в оперативно-розшуковій та кримінальній процесуальній діяльності запропоновано: визначити у КПК України можливість здійснювати OSINT у процесі розслідування кримінальних правопорушень, зокрема: у ч. 2 ст. 264 КПК України здобувати під час зняття інформації з електронних інформаційних систем з використанням OSINT; включити у нормативні приписи ч. 1 ст. 273 КПК України можливість створення віртуальних засобів (особи) для зняття інформації з електронних інформаційних систем; унормувати практику використання OSINT для одержання даних, які мають значення для оперативно-розшукової діяльності, шляхом внесення відповідних змін до ч. 1 ст. 8 Закону України «Про оперативно-розшукову діяльність». Зазначено, що подальших наукових пошуків потребують питання організаційних, тактичних засад проведення OSINT-досліджень в інтересах вирішення завдань кримінального провадження; процесуального статусу осіб, уповноважених його здійснювати; оцінки його результатів та організаційно-правових засад їх використання у кримінальному провадженні тощо.*

***Ключові слова:*** розвідка з відкритих джерел (OSINT), оперативно-розшукова діяльність, кримінальне провадження, досудове розслідування, доказування, слідчий огляд, зняття інформації з електронних інформаційних систем.

**Kudinov Serhiy, Shekhavtsov Ruslan. Legal regulation of the use of OSINT and its results during the establishment of circumstances of criminal offenses**

***Abstract.*** *The article, based on the study of the history of the development of open source intelligence (OSINT) from obtaining data on social, economic, and managerial processes to data on the commission of war crimes, proposes: to determine in the Code of Criminal Procedure of Ukraine the possibility of conducting OSINT in the investigation of criminal offenses, in particular, in Part 2 of Art. 264 of the Code of Criminal Procedure of Ukraine to obtain information from electronic information systems using OSINT; to include in the regulatory provisions of Part 1 of Article 273 of the Code of Criminal Procedure of Ukraine the possibility of creating virtual means (personalities)*

*for removing information from electronic information systems; to regulate the practice of using OSINT to obtain data that is important for operational and investigative activities by making appropriate amendments to Part 1 of Article 8 of the Law of Ukraine "On Operational and Investigative Activities". It is noted that further scientific research is required on the issues of organizational and tactical principles of conducting OSINT research in the interests of solving the tasks of criminal proceedings, the procedural status of persons authorized to conduct it, the assessment of its results and the organizational and legal principles of their use in criminal proceedings, etc.*

***Key words:*** *open source intelligence (OSINT), operational and investigative activities, a criminal proceeding, pre-trial investigation, evidence, investigative examination, removal of information from electronic information systems.*

**Вступ.** Виникнення та розвиток методів та технологій збирання та дослідження інформації з відкритих джерел більшістю дослідників історії OSINT пов'язується із розповсюдженням у другій половині 19-го сторіччя газет як засобів масової інформації, вивчення яких дозволяло одержувати розвідувальні дані про соціально-політичне та економічне життя певної держави. У 40-х роках 20-го сторіччя розвідувальні спільноти Великої Британії, Сполучених Штатів Америки побачили у радіомовних засобах масової інформації потенціал одержання інформації про процеси, які відбуваються в суспільно-політичному, соціально-економічному житті різних держав [1, с. 95–99]. Моніторинг радіомовлення, який додався до відповідного вивчення та аналізу змісту періодичних видань, виступив основою для відпрацювання методів та технологій дослідження інформації з відкритих джерел. Однак, як справедливо зазначає К. Колкухаун, наприкінці другої половини 20-го сторіччя OSINT зайшов у глухий кут через обмеженість періодичними та систематичними (галузевими) виданнями, радіо – та телемовленням, а також через використання тільки у сфері діяльності розвідувальних органів [2].

Конвергенція цифрових та комунікаційних технологій у першому десятиріччі 21-го століття створила умови для переходу значної частини соціальних, економічних, управлінських процесів у середовище мережі Інтернет, яка стала одним із компонентів розбудови відкритого суспільства насамперед у державах, які позиціонують себе як правові та демократичні. Як наслідок, у відкритому доступі з'являються великі масиви даних, застосування до вивчення яких методології OSINT дозволило одержувати інформацію про життєдіяльність окремих осіб, соціальних груп, суб'єктів господарювання, державних інституцій тощо, і не тільки державним розвідувальним органам, а й правоохоронним органам, суб'єктам детективної, журналістської діяльності, забезпечення безпеки бізнесу.

Розвідка з відкритих джерел стала необхідним складником у багатьох сферах, надаючи можливість отримувати актуальну інформацію та розуміти контекст подій у світі, де доступ до даних є важливим ресурсом [3, с. 13].

Потужний поштовх запровадженню OSINT у розслідування кримінальних правопорушень був наданий у 2020 році ООН, за підтримки якої фахівцями Центру прав людини Університету Берклі був підготовлений практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, прав людини та гуманітарного права – загальновідомий зараз як Протокол Берклі [4].

**Матеріали та методи.** Для проведення дослідження використовувалися зарубіжні та вітчизняні літературні джерела, які містять дані про особливості здійснення OSINT та використання його результатів для встановлення обставин вчинення воєнних злочинів; нормативно-правові акти у сферах оперативно-розшукової діяльності та кримінальної юстиції. З метою вивчення вітчизняної практики використання OSINT для встановлення обставин кримінальних правопорушень проведено інтерв'ювання співробітників оперативних підрозділів, органів досудового розслідування Національної поліції України, СБУ, НАБУ, ДБР, БЕБ, а також пошук, вивчення та узагальнення відповідних судових рішень у кримінальних провадженнях.

**Результати.** З моменту початку збройної агресії росії 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.

Заслуговує 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 [5; 6; 7; 8; 9]. Позитивні результати такої практики сприяють розширенню категорій кримінальних правопорушень, для встановлення обставин яких може використовуватися пошук та дослідження викритих цифрових даних. Але таке масштабування сфери використання OSINT потребує відповідного законодавчого забезпечення, адміністрування та методичного супроводу з урахуванням особливостей відображення механізму вчинення певних різновидів кримінальних правопорушень у джерелах даних, які можуть бути досліджені за допомогою OSINT; вимог чинного оперативно-розшукового та кримінального процесуального законодавства та наявності відповідних заходів, засобів одержання даних про кримінальні правопорушення в процесі здійснення оперативно-розшукової та слідчої діяльності.

Характеризуючи OSINT, відомий вітчизняний дослідник Д. Ланде вказує, що базовими для його розуміння є два поняття:

– відкрите джерело – це джерело інформації, що надає її без вимоги збереження конфіденційності, тобто надає інформацію, не захищену від публічного розкриття. Відкриті джерела належать до середовища загальнодоступної інформації і не мають обмеження у доступі для фізичних осіб;

– загальнодоступна інформація – це інформація, опублікована або розміщена для широкого використання, доступна для громадськості [3, с. 13].

Протокол Берклі не містить визначення OSINT. Цей документ призначений для адаптації інструментів OSINT для потреб розслідування міжнародних злочинів, тому у Резюме Протоколу є лише визначення розслідування з використанням відкритих даних як розслідування, яке повністю або частково спирається на загально доступну інформацію для проведення офіційних та систематичних онлайн-розслідувань щодо передбачуваних правопорушень [4, с. 9]. Наведене визначення є похідним від розуміння OSINT як:

– несекретної інформації, яка була спеціально виявлена, розпізнана, перероблена і поширена серед визначеної аудиторії з метою з'ясування конкретного питання (NATO OSINT Handbook V 1.2.) [10, с. 6];

– розвідданих, які отримані із загальнодоступної інформації, зібрані, використані і своєчасно поширені серед відповідної аудиторії з метою задоволення конкретних розвідувальних потреб (Subtitle D – Intelligence-Related Matters SEC. 931. US PUBLIC LAW. 109-163-JAN. 6, 2006. National Defense Authorization Act for Fiscal Year 2006) [11].

Сучасне інформаційне суспільство є сприятливим середовищем для здійснення OSINT. Основні властивості такого суспільства – постійне зростання кількості людей, яким доступні інформаційно-комунікаційні технології мережі Інтернет, інтенсивний розвиток та проникнення інформаційних технологій та інформатизації у різні сфери суспільного життя, господарської діяльності, державного управління тощо. Однією з особливостей інтернет-технології є збереження на серверах даних про повсякденну активність користувачів цієї мережі, доступ до яких можуть одержати інші користувачі. Предметом OSINT за визначенням Протоколу Берклі є тільки загальнодоступна інформація, яка міститься в мережі Інтернет. У п. 14–16 цього документа описуються ознаки таких даних:

– для їх одержання користувачу не треба мати спеціальний правовий статус чи дозвіл;

– для доступу може вимагатися від користувачів реєстрація та одержання паролю. Але такий доступ вважається відкритим за умови загальності такої умови для всіх користувачів;

– доступ до даних може бути як безоплатним, так і платним;

– для одержання доступу до даних використовується відкрите програмне забезпечення [4, с. 24–26; 5, с. 19–20].

Слід зазначити, що нині ми маємо непоодинокі випадки, коли органи досудового розслідування (Національної поліції України, СБУ, НАБУ, ДБР, БЕБ), прокурори, суди у своїх рішеннях посилаються на матеріали OSINT як засоби отримання інформації, необхідної для розслідування злочинів. Крім того, станом на 09.08.2025 Єдиний державний реєстр судових рішень містить 139 ухвал та 21 вирок, де згадується OSINT. 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) [12], матеріалів OSINT-аналізу на фізичну особу [13], протоколів огляду комп'ютерних даних [14]. Причому у більшості таких рішень посилаються не на документ як джерело даних OSINT, а на результати чи джерела, зібрані в результаті OSINT [15]. Така практика існує через 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.

У контексті використання відкритих даних для потреб виявлення та встановлення обставин події кримінальних правопорушень важливе методологічне значення має визначення їхнього доказового потенціалу, яке укладачі Протоколу Берклі у п. 23 пов'язують із критеріями релевантності (відповідність події, яка виступає об'єктом розслідування), надійності (правдоподібність чи правдивість), достовірності (здатність забезпечувати доказування послідовно, відповідно до очікувань), справжності (точність, відповідність фактам). Наведені критерії в сукупності визначають допустимість використання даних із відкритих джерел для формулювання фактичних та юридичних висновків слідчим під час розслідування злочинів (п. 55–57, 148, 149 Протоколу Берклі) [4, с. 46–48, 85]. Наведені критерії частково збігаються з критеріями оцінки доказів, визначених у ст. 94 КПК України. Критерій релевантності в цілому відповідає належності доказів, а критерії надійності, достовірності та справжності даних із відкритих джерел – достовірності доказів. Але допустимість одержаних за результатами розслідування з використанням відкритих даних для доказування певних фактів пов'язується в Протоколі Берклі з фактичністю даних, а допустимість за ст. 86 КПК України – з дотриманням процедури одержання доказів. Зазначимо, що в Протоколі Берклі процедурі здійснення OSINT приділяється значна увага. Їй присвячені глави V «Підготовка», VI «Процес розслідування», VII «Звітування про висновки», але допустимість як критерій оцінки даних із відкритих джерел не охоплює аналіз порядку одержання цих даних. Укладачі Протоколу Берклі у п. 55 оперують кримінальною процесуальною категорією допустимості доказів у контексті стандартів доказування у національних судах, зазначаючи, що такі стандарти є більш суворими, ніж у міжнародних кримінальних трибуналах, хоча методи збору доказів впливають і в таких судових інстанціях на вагу, яку судді надають доказам [4, с. 47]. Формуючи Протокол Берклі, його автори свідомо уникнули інтеграції в систему методичних рекомендацій зі здійснення та використання результатів онлайн-досліджень вимог щодо обов'язкового дотримання певних процедур OSINT для визнання його результатів як доказів у кримінальному судочинстві з огляду на пріоритет визначення параметрів достовірності та ваги висновків через очевидну складність поєднати різні за ступенем суворості стандарти доказування, які є у міжнародному та національному кримінальному судочинстві. Єдиним ключовим постулатом для допустимості даних із відкритих джерел у доказуванні визначено забезпечення захисту прав обвинуваченого та справедливого судового розгляду (п. 55 Протоколу Берклі) [4, с. 47]. 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. У вітчизняному кримінальному процесуальному, а також оперативно-розшуко-

ISSN 2311-8040

вому законодавстві відсутня нормативно-правова регламентація використання таких інструментів для одержання даних про обставини готування та вчинення кримінальних правопорушень. Такий вакуум останні декілька років як науковці, так і практики намагаються заповнити навчальною літературою та тренінгами щодо використання OSINT та його результатів у сферах оперативно-розшукової та кримінально-процесуальної діяльності. З огляду на відсутність нормативно-правової основи використання OSINT, домінує обережний підхід, відповідно до якого основними суб'єктами його застосування є оперативні підрозділи й одержані в результаті дані можуть мати тільки орієнтуюче значення. У цьому зв'язку О. О. Торбас, спираючись на зарубіжний та вітчизняний досвід, зокрема на практичні кейси, слушно уточнює, що відомості, отримані з відкритих електронних джерел, можна розділити на три групи: 1) інформація, яка має орієнтуючий характер для пошуку джерел фактичних даних про обставини події кримінального правопорушення; 2) відомості, що характеризують особу; 3) відомості, які прямо стосуються предмета доказування. Щодо останньої групи даних зазначається, що для їх оцінки необхідно застосовувати параметри оцінки доказів, визначені КПК України [16, с. 247–248]. Одним із ключових критеріїв такої оцінки є одержання фактичних даних у визначений законом спосіб. Для виявлення та фіксування відкритих даних у мережі Інтернет у рамках OSINT для потреб кримінального провадження пропонується використовувати огляд, процесуальна форма якого передбачає одним із об'єктів комп'ютерні дані (ст. 237 КПК України) [17, с. 413–417; 5, с. 33]. Але огляд, незважаючи на гнучкість його процесуальної форми, не може включати повною мірою аналіз одержаних із відкритих джерел даних, результати якого і є продуктом OSINT. Такий аналіз може бути різного рівня складності. В одних випадках для висновку про наявність певного факту досить зафіксованих у протоколі огляду комп'ютерних даних та відповідному додатку до нього цифрових даних, які, наприклад, містять світлину певної особи у військовій формі росії зі зброєю [18], але в інших – необхідно здійснити комплекс дій з використанням різних програмно-технічних засобів (автоматизованого збору даних, візуального аналізу, документування та структурування результатів аналізу тощо). Такі дії не охоплюються процесуальною формою здійснення слідчого огляду, але, незважаючи на це, протокол огляду комп'ютерних даних на практиці може містити результати їх аналізу (дослідження). Альтернативою огляду комп'ютерних даних може виступати зняття інформації з електронних інформаційних систем, доступ до яких не обмежується їхнім власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту (ч. 2 ст. 264 КПК України). Порівняно з оглядом комп'ютерних даних використання цієї негласної слідчої (розшукової) дії для збирання відомостей із відкритих джерел ускладнене вимогами забезпечення дотримання державної таємниці. Ця обставина схиляє практиків до використання огляду комп'ютерних даних. Хоча, якщо зіставляти алгоритм здійснення розслідування з використанням відкритих даних, описаним у Протоколі Берклі, з процесуальною формою огляду комп'ютерних даних та зняття інформації з електронних інформаційних систем, доступ до яких не обмежується їхнім власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, остання процесуальна дія, за нашою оцінкою, більшою мірою забезпечує можливість не тільки виявлення даних із відкритих джерел, а й їх дослідження. Так, однією з вимог до здійснення розслідування з використанням відкритих даних за Протоколом Берклі є забезпечення безпеки в частині запобігання виявленню факту збирання даних третіми особами – з цією метою рекомендується створювати віртуальну особу (п. 68). Створення такої особи не може бути здійснене для проведення огляду комп'ютерних даних, а для негласної слідчої (розшукової) дії, передбаченої ч. 2 ст. 264 КПК України, це може бути реалізоване створенням несправжніх (імітаційних) засобів (ст. 273 КПК України). Аналіз даних із відкритих джерел, виявлених та зафіксованих під час зняття інформації з електронних інфор-

маційних систем, доступ до яких не обмежується їхнім власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, може бути здійснений, якщо немає питань, які стосуються комп'ютерно-технічної, портретної чи інших експертиз, дослідженням інформації, отриманої з використанням технічних засобів із залученням спеціаліста та відповідних програмно-технічних засобів, відповідно до ст. 266 КПК України. Застосуванню на практиці наведеного алгоритму здійснення розслідування з використанням відкритих даних за технологією OSINT перешкоджає недосконаліть кримінального процесуального законодавства. Не сприяє залученню у процес доказування результатів застосування інструментів OSINT оперативними підрозділами відсутність в оперативно-розшуковому законодавстві можливості їх застосування для одержання даних про обставини кримінального правопорушення.

**Висновки.** Потреби практики розкриття та розслідування воєнних злочинів та колабораційної діяльності зумовили активне використання інструментів OSINT як слідчими, так і оперативними підрозділами для встановлення обставин події кримінальних правопорушень, зокрема відомостей про осіб, які до них причетні, незважаючи на прогалини в оперативно-розшуковому та кримінальному процесуальному законодавстві. Використання результатів OSINT в умовах правової невизначеності вже призвело до різної практики як прийняття рішень про здійснення таких досліджень, так і оформлення їх результатів. Своєю чергою, правова невизначеність актуалізує питання про допустимість використання в доказуванні у кримінальному провадженні результатів OSINT.

Принцип правової визначеності зумовлює необхідність:

– по-перше, визначення можливості здійснювати OSINT у процесі розслідування кримінальних правопорушень. Інтегрувати таке визначення пропонується доповненням ст. 3 КПК України п. 29 такого змісту: «OSINT – це збір, аналіз та інтерпретація даних із відкритих джерел для виявлення фактів, які мають значення для кримінального провадження, що здійснюється з використанням спеціальних засобів та методів обробки інформації (в тому числі програмно-технічних засобів), відповідно до положень Протоколу Берклі»;

– по-друге, доповнити ч. 2 ст. 264 КПК України реченням такого змісту: «Здобуття такої інформації може здійснюватися з використанням OSINT.»;

– по-третє, включення у нормативні приписи ч. 1 ст. 273 КПК України можливості створення віртуальних засобів (особи) для зняття інформації з електронних інформаційних систем;

– по-четверте, визначення у ч. 1 ст. 266 КПК України: «Дослідження інформації, отриманої при застосуванні технічних засобів, у разі необхідності здійснюється за участю спеціаліста із застосуванням відповідних програмно-технічних засобів. Слідчий вивчає зміст отриманої інформації, про що складається протокол. У разі виявлення відомостей, що мають значення для досудового розслідування і судового розгляду, в протоколі відтворюється відповідна частина інформації, після чого прокурор вживає заходів для збереження отриманої інформації. До протоколу долучаються додатки, які містять результати застосування програмно-технічних засобів при дослідженні інформації, отриманої під час негласної (слідчої) розшукової дії»;

– по-п'яте, унормування практики використання OSINT для одержання даних, які мають значення для оперативно-розшукової діяльності. Це пропонується здійснити шляхом доповнення ч. 1 ст. 8 Закону України «Про оперативно-розшукову діяльність» п. 22 у такій редакції: «безпосередньо проводити або ініціювати проведення збирання та дослідження інформації з відкритих джерел з використанням OSINT».

Подальших наукових пошуків потребують питання організаційних, тактичних засад проведення OSINT-досліджень в інтересах вирішення завдань кримінального провадження; процесуального статусу осіб, уповноважених його здійснювати; оцінки його результатів та організаційно-правових засад їх використання у кримінальному провадженні тощо.

**Список використаних джерел:**

1. Ludo Block. The long history of OSINT. *JOURNAL OF INTELLIGENCE HISTORY*. 2024. Vol. 23, No. 2. С. 95–109. URL: https://www.tandfonline.com/doi/epdf/10.1080/16161262.2023.2224091?needAccess=true

2. Cameron Colquhoun. A Brief History of Open Source Intelligence. *Bellingcat.* July 14, 2016. URL: https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/

3. Ланде Д. В. OSINT у кібербезпеці : навчальний посібник. Київ : ТОВ «Інжинірінг», 2024. 552 с.

4. Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева : Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. 119 с. URL : https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

5. Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : науково-практичний порадник / Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін, А. В. Шевчишен та ін. ; за заг. ред. М. С. Цуцкірідзе. Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. 196 с.

6. Галузь OSINT в суспільній та державній діяльності / Institute of Post-Information Society. 2023. 140 с. URL : https://kr-labs.com.ua/books/galuz-osint-v-suspilnii-ta-derzhavnii-diialnosti-10032023.pdf

7. Зоренко Д. С., Кульчицька Л. О., Лех Р. В., Червяков О. І. Використання інструментів та методів OSINT для отримання пошукової інформації : практичний порадник. 5-те вид., переробл. та доповн. Харків : Видавець О. А. Мірошниченко, 2024. 80 с.

8. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Видавництво «Юридика», 2024. 180 с.

9. Пашковський М. Технології проти злочинів війни: виклики та можливості для правосуддя. *JustTalk.* 2025. 50 с. URL : https://drive.google.com/file/d/1iNqe4-l3kCOdt_RxLO7jykYHm7qlOU0Z/preview

10. NATO OSINT Handbook V 1.2. November 2001. 57 с. URL: NATO OSINT Handbook V 1.2 : Free Download, Borrow, and Streaming : Internet Archive

11. US PUBLIC LAW. 109-163-JAN. 6, 2006. National Defense Authorization Act for Fiscal Year 2006. URL: https://www.congress.gov/109/plaws/publ163/PLAW-109publ163.pdf

12. Вирок Тернопільського міськрайонного суду Тернопільської області у справі № 607/18729/23 за ч. 7 ст. 111-1 КК України. URL: https://reyestr.court.gov.ua/Review/121599242

13. Вирок Івано-Франківського міського суду Івано-Франківської області у справі № 344/19008/24 за ч. 7 ст. 111-1 КК України. URL: https://reyestr.court.gov.ua/Review/123535737

14. Ухвала Жовтневого районного суду м. Дніпропетровська у кримінальному провадженні № 12024052770000367 за ч. 3 ст. 111-1 КК України. URL: https://reyestr.court.gov.ua/Review/126668932

15. Вирок Соборного районного суду м. Дніпра у справі № 201/2452/24 за ч. 6 ст. 111-1 КК України. URL: https://reyestr.court.gov.ua/Review/129043850

16. Торбас О. О. Особливості доказування за допомогою OSINT у кримінальному процесі. *Актуальні проблеми держави і права.* 2025. № 105. С. 246–252. https://doi.org/10.32782/apdp.v105.2025.28

17. Коваленко А. В. Огляд комп'ютерних даних під час розслідування колабораційної діяльності: типові об'єкти та приклади з практики. *Війна в Україні: зроблені висновки та незасвоєні уроки :* збірник тез Міжнародної науково-практичної конференції (22–23 лютого 2024 року) / упор. У. О. Цмоць. Львів : Львів. держ. ун-т внутр. справ, 2024. С. 413–417.

18. Постанова Великої Палати Верховного Суду від 28.02.2024 у справі № 415/2182/20 (провадження № 13-15кс22). П. 125. URL: https://reyestr.court.gov.ua/Review/117555176

**References:**

1. Ludo Block. (2024). The long history of OSINT. Journal of intelligence history. Vol. 23, No. 2. Pp. 95–109. URL: https://www.tandfonline.com/doi/epdf/10.1080/16161262.2023.2224091?needAccess=true [in English].

2. Cameron Colquhoun. (2016). A Brief History of Open Source Intelligence. Bellingcat, July 14. URL: https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/ [in English].

3. Lande, D. V. (2024). *OSINT u kiberbezpetsi [OSINT in cybersecurity].* Kyiv : "Inzhynirinh" [in Ukrainian].

4. Protokol Berkli z vedennia rozsliduvannia z vykorystanniam vidkrytykh tsyfrovykh danykh. Praktychnyi posibnyk shchodo efektyvnoho vykorystannia tsyfrovoi informatsii u vidkrytomu dostupi dlia rozsliduvannia porushen mizhnarodnoho kryminalnoho prava, z prav liudyny ta humanitarnoho prava (2020) [Berkeley Protocol on Investigating with Open Digital Data. A practical guide to the effective use of publicly available digital information to investigate violations of international criminal law, human rights and humanitarian law] /

neofits. per. z anhl. O. V. Ziuz. Niu-York; Zheneva: Tsentr iz prav liudyny Kaliforn. un-tu, Berkli, Yuryd. shk., OON Upr. Verkhov. komisara z prav liudyny. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf [in Ukrainian].

5. Gavrilyuk, L.V., Basista, I.V., Afonin, D.S., Shevchishen, A.V., Khytra A.Ya., Lisnichenko D.V., et al. (2024). Vykorystannia elektronnykh dokaziv pid chas dosudovoho rozsliduvannia zlochyniv proty myru, bezpeky liudstva ta mizhnarodnoho pravoporiadku (Protokol Berkli) [Use of Electronic Evidence in Pre-Trial Investigations of Crimes against Peace, Human Security and the International Legal Order (Berkeley Protocol)] / edited by Tsutsikiridze, M.S. Kyiv: DNDI MVS Ukrainy; «Politekhnika» [in Ukrainian].

6. Haluz OSINT v suspilnii ta derzhavnii diialnosti [The field of OSINT in public and government activities]. (2023). Institute of Post-Information Society. URL: https://kr-labs.com.ua/books/galuz-osint-v-suspilnii-ta-derzhavnii-diialnosti-10032023.pdf [in Ukrainian].

7. Zorenko, D. S., Kulchitska, L. O., Lekh, R. V., & Chervyakov, O. I. (2024). *Vykorystannia instrumentiv ta metodiv OSINT dlia otrymannia poshukovoi informatsii [Use of OSINT tools and methods for obtaining search information].* Kharkiv : Vydavets Miroshnychenko, O. A. [in Ukrainian].

8. Pashkovsky, M. (2025). Tekhnolohii proty zlochyniv viiny: vyklyky ta mozhlyvosti dlia pravosuddia [Technologies against war crimes: challenges and opportunities for justice]. *JustTalk.* URL: https://drive.google.com/file/d/1iNqe4-l3kCOdt_RxLO7jykYHm7qlOU0Z/preview [in Ukrainian].

9. NATO OSINT Handbook V 1.2. (November 2001). URL: NATO OSINT Handbook V 1.2 : Free Download, Borrow, and Streaming : Internet Archive [in English].

10. US PUBLIC LAW. 109-163-JAN. 6, 2006. National Defense Authorization Act for Fiscal Year 2006. URL: https://www.congress.gov/109/plaws/publ163/PLAW-109publ163.pdf [in English].

11. Vyrok Ternopilskoho miskraionnoho sudu Ternopilskoi oblasti u spravi № 607/18729/23 za ch. 7 st. 111-1 KK Ukrainy [Judgment of the Ternopil City District Court of Ternopil Region in case No. 607/18729/23 under Part 7 of Article 111-1 of the Criminal Code of Ukraine]. URL: https://reyestr.court.gov.ua/Review/121599242 [in Ukrainian].

12. Vyrok Ivano-Frankivskoho miskoho sudu Ivano-Frankivskoi oblasti u spravi № 344/19008/24 za ch. 7 st. 111-1 KK Ukrainy [Judgment of the Ivano-Frankivsk City Court of Ivano-Frankivsk Region in case No. 344/19008/24 under Part 7 of Article 111-1 of the Criminal Code of Ukraine]. URL: https://reyestr.court.gov.ua/Review/123535737 [in Ukrainian].

13. Ukhvala Zhovtnevoho raionnoho sudu m. Dnipropetrovska u kryminalnomu provadzhenni № 12024052770000367 za ch. 3 st. 111-1 KK Ukrainy [Ruling of the Zhovtnevy District Court of Dnipropetrovsk in criminal proceedings No. 12024052770000367 under Part 3 of Article 111-1 of the Criminal Code of Ukraine]. URL: https://reyestr.court.gov.ua/Review/126668932 [in Ukrainian].

14. Vyrok Sobornoho raionnoho sudu m. Dnipra u spravi № 201/2452/24 za ch. 6 st. 111-1 KK Ukrainy [Judgment of the Soborny District Court of Dnipro in case No. 201/2452/24 under Part 6 of Article 111-1 of the Criminal Code of Ukraine]. URL: https://reyestr.court.gov.ua/Review/129043850 [in Ukrainian].

15. Torbas, O. O. (2025). Osoblyvosti dokazuvannia za dopomohoiu OSINT u kryminalnomu protsesi. *Aktualni problemy derzhavy i prava.* [Features of evidence using OSINT in criminal proceedings. *Current issues of state and law*]. Vol. 105. Pp. 246–252. https://doi.org/10.32782/apdp.v105.2025.28 [in Ukrainian].

16. Kovalenko, A. V. Ohliad kompiuternykh danykh pid chas rozsliduvannia kolaboratsiinoi diialnosti: typovi obiekty ta pryklady z praktyky. *Viina v Ukraini: zrobleni vysnovky ta nezasvoieni uroky* [Review of computer data during the investigation of collaboration activities: typical objects and practical examples. *War in Ukraine: conclusions drawn and lessons not learned*] *:* zbirnyk tez Mizhnarodnoi naukovo-praktychnoi konferentsii (22–23 liutoho 2024 roku) / upor. U. O. Tsmots. Lviv : Lviv. derzh. un-t vnutr. sprav. Pp. 413–417 [in Ukrainian].

17. Postanova Velykoi Palaty Verkhovnoho Sudu vid 28.02.2024 u spravi № 415/2182/20 (provadzhennia № 13-15ks22). [Resolution of the Grand Chamber of the Supreme Court of 28 February 2024 in case No. 415/2182/20 (proceedings No. 13-15кс22)]. P. 125. URL: https://reyestr.court.gov.ua/Review/117555176 [in Ukrainian].

*Дата надходження статті: 21.07.2025*
*Дата прийняття статті: 25.08.2025*
*Опубліковано: 27.10.2025*