УДК 343.132:004.75
DOI https://doi.org/10.24144/2788-6018.2026.02.3.12

ВИКОРИСТАННЯ МЕТОДИК OSINT У МЕЖАХ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ: УСПІШНІ КЕЙСИ У ПРАКТИЦІ ІНОЗЕМНИХ ПРАВООХОРОННИХ ОРГАНІВ ТА ІНСТИТУТІВ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Каландирець Я.М.,
аспірант
Національного юридичного університету імені Ярослава Мудрого
ORCID: 0009-0009-2238-8337

Тітко І.А.,
доктор юридичних наук, професор,
завідувач кафедри кримінального права та кримінально-правових дисциплін
Полтавського юридичного інституту
Національного юридичного університету імені Ярослава Мудрого
ORCID: 0000-0003-4126-6967

Каландирець Я.М., Тітко І.А. Використання методик OSINT у межах розслідування кримінальних правопорушень: успішні кейси у практиці іноземних правоохоронних органів та інститутів громадянського суспільства.

У статті здійснюється комплексний науковий аналіз використання методик розвідки на основі відкритих джерел (OSINT) як надефективного інструменту протидії злочинності в умовах сучасного входження людства в епоху тотальної цифровізації та домінування інформаційних потоків. Відзначається, що представники кримінальної сфери активно використовують переваги кіберпростору для узгодження своїх планів, проте неминуче залишають специфічний «цифровий слід». Авторами докладно розглядається сутність концепції OSINT, яка полягає у легальному зборі, обробці та інтерпретації публічно доступної інформації. Особлива увага у публікації приділяється детальному розбору конкретних успішних іноземних кейсів застосування OSINT. Зокрема, проаналізовано процес розкриття серійних вбивств «Gilgo Beach Murders» у США, де ключову роль відіграв симбіоз традиційних доказових методик (аналіз ДНК на залишках піци) та інструментів цифрової розвідки: систем розпізнавання авто на базі штучного інтелекту, геопросторових даних Google та Bing Maps, а також аналізу цифрових слідів анонімної електронної пошти обвинуваченого. Досліджено досвід різних штатів США у боротьбі з браконьєрством, де слідчі встановлюють факти незаконного полювання, використання забороненого корму та проникнення на ферми шляхом профілювання соціальних мереж, моніторингу геотегів та аналізу публікацій позначених друзів зловмисників. Надзвичайно важливим є описаний досвід протидії організованій злочинності у сфері торгівлі людьми за допомогою розробленої DARPA програми Memex. Крім того, авторами статті висвітлено потужний превентивний потенціал OSINT щодо прогнозування соціальних заворушень на прикладі подій біля Капітолія США у 2021 році, де автоматизований пошук за хештегами допоміг ідентифікувати координаторів-інфлюенсерів та плани екстремістів, після чого ФБР успішно залучило громадськість до збору цифрових медіафайлів. Окремо підкреслюється значення OSINT для митних адміністрацій з метою виявлення закономірностей контрабанди, створення профілів високого ризику та порівняння задекларованої вартості товарів. Не залишено без уваги таке досягнення незалежної розвідки з відкритих джерел як кейс організації Bellingcat щодо розслідування збиття рейсу MH17: ретельний аналіз фото та відео з соцмереж дозволив відстежити маршрут ЗРК «Бук», що згодом було верифіковано офіційним міжнародним слідством. Досліджено правові межі застосування методик, з акцентом на тому, що збір інформації визнається законним лише за умови використання публічних даних без порушення конституційних прав та з обов'язковим дотриманням рекомендацій протоколу Берклі для гарантування достовірності цифрових доказів у суді. Серед іншого, звертається увага, що тоді як у міжнародній практиці OSINT є стандартизованим інструментом, в Україні його потенціал розкрито недостатньо. В статті обґрунтовано критичну необхідність впровадження передового досвіду OSINT та технологій машинного навчання у вітчизняну практику для протидії злочинності та належної фіксації воєнних злочинів в умовах сьогодення.

Ключові слова: OSINT, кримінальне провадження, кримінальне процесуальне доказування, цифрові (електроні) докази, кримінальний процес іноземних держав, розслідування воєнних злочинів, належна правова процедура.

Kalandyrets Y.M., Titko I.A. The application of OSINT methodologies in criminal investigations: successful case studies from the practice of foreign law enforcement agencies and civil society institutions.

The article provides a comprehensive scientific analysis of the use of open-source intelligence (OSINT) methodologies as a highly effective tool for combating crime in the context of humanity's modern transition into the era of total digitalization and the dominance of information flows. It is noted that representatives of the criminal sphere actively use the advantages of cyberspace to coordinate their plans but inevitably leave a specific "digital footprint". The authors examine in detail the essence of the OSINT concept, which consists of the legal collection, processing, and interpretation of publicly available information. Special attention in the publication is paid to a detailed analysis of specific successful foreign cases of OSINT application. In particular, the process of solving the "Gilgo Beach Murders" serial killings in the USA is analyzed, where a key role was played by a symbiosis of traditional evidentiary techniques (DNA analysis on pizza remnants) and digital intelligence tools: AI-based vehicle recognition systems, Google and Bing Maps geospatial data, as well as the analysis of digital footprints from the accused's anonymous email. The experience of various US states in combating poaching is investigated, where investigators establish facts of illegal hunting, the use of prohibited feed, and farm trespassing through social media profiling, geotag monitoring, and the analysis of publications by tagged friends of the perpetrators. Of utmost importance is the described experience of countering organized crime in the field of human trafficking using the Memex program developed by DARPA. Furthermore, the authors of the article highlight the powerful preventive potential of OSINT in predicting social unrest, using the example of the events at the US Capitol in 2021, where automated hashtag searches helped identify coordinating influencers and extremist plans, after which the FBI successfully engaged the public in gathering digital media files. The importance of OSINT for customs administrations is separately emphasized for the purpose of identifying smuggling patterns, creating high-risk profiles, and comparing the declared value of goods. A landmark achievement of independent open-source intelligence recognized by the authors is the Bellingcat case regarding the investigation of the downing of flight MH17: a thorough analysis of photos and videos from social networks allowed tracing the route of the "Buk" surface-to-air missile system, which was later verified by the official international investigation. The legal boundaries of applying these methodologies are examined: information gathering is considered legal only if public data is used without violating constitutional rights and with mandatory compliance with the Berkeley Protocol recommendations to ensure the reliability of digital evidence in court. In the conclusion, the authors state that while OSINT is a standardized tool in international practice, its potential is insufficiently unlocked in Ukraine. The critical need to implement advanced OSINT experience and machine learning technologies into domestic practice to combat crime and properly document war crimes in the current conditions is substantiated.

Key words: OSINT, criminal proceedings, criminal procedural evidence, digital (electronic) evidence, criminal proceedings of foreign states, war crimes investigation, due process of law.

Постановка проблеми. Входження людства в епоху цифровізації та домінування інформаційних потоків неминуче вплинуло і на злочинну діяльність. Представники кримінальної сфери не лише використовують переваги кіберпростору, узгоджуючи свої злочинні плани за допомогою соціальних мереж чи здобуваючи необхідну інформацію з публічних джерел, а і неминуче залишають будь-якими своїми діями в мережі «цифровий слід», що зумовлює необхідність адекватної і технологічної відповіді на дані виклики сьогодення з боку правоохоронних інституцій.

Одним з ефективних інструментів у межах реагування та протидії вищезгаданим викликам сьогодення може бути використання методик розвідки на основі відкритих джерел даних, які нині демонструє виняткову ефективність у межах збору доказової чи іншої супутньої інформації, зробивши OSINT невід'ємною частиною роботи сучасних правоохоронних органів та незалежних громадських інституцій, що фіксують чи надають розголосу фактам протиправної чи злочинної поведінки.

Мета дослідження. Стаття спрямована на підвищення обізнаності та стимулювання наукової дискусії щодо проблематики використання OSINT-методів у збиранні та використання доказової інформації при розкритті кримінальних правопорушень. Досягненню вказаної мети сприятиме розв'язання таких завдань: визначення окремих успішних практичних кейсів використання OSINT у практиці зарубіжних органів досудового розслідування, завдяки яким було здобуто важливі для кримінальних проваджень дані; аналіз ефективності та результатів використання зазначеного досвіду, зокрема – з точки зору можливості його застосування в українських реаліях слідчої та судової практики.

Стан опрацювання проблематики. Проблематика застосування методик розвідки на основі відкритих джерел та подальшого використання OSINT-даних в межах кримінального провадження, зокрема – у формі електронних (цифрових) доказів, наразі є перспективним науковим напрямом у

доктрині кримінального процесу України, який вже представлений окремими науковими працями за авторством, зокрема: І. Басистої, Л. Гаврилюк, А. Гутник, А. Хитри [1], І. Гловюк [2], І. Калančі [3], М. Погорецького [4], А. Скрипника [5], І. Смаль [6], О. Торбаса [7], М. Пашковського [8], В. Шевчука [9], В. Шепітька, М. Шепітька, К. Латиш, М. Капустіної, Є. Демидової [10] та інших дослідників.

Виклад основного матеріалу. Розвідка з відкритих джерел мережі Інтернет загальновідомо вважається потужним інструментом здобуття тих чи інших відомостей, які зберігаються у «всесвітній павутині» чи становлять цифровий слід певної особи, а тому – за своєю сутністю може бути надзвичайно ефективним інструментом доказування в руках відповідних фахівців правоохоронних органів.

Наукові розробки з питань використання OSINT наразі є порівняно новим явищем у глобальній науці та галузі інформаційної безпеки безпосередньо, хоча різноманітні методики збору інформації з відкритих джерел були досить усталеною практикою на різних етапах розвитку людства. Натомість у сучасному розумінні термін «розвідки» зазвичай пов'язується з процесом збору, аналізу та інтерпретації певної цінної для ухвалення рішень інформації і традиційно асоціюється з військовою чи безпековою справою.

Сутність OSINT полягає в отриманні інформації (зокрема й розвідувальної) з легальних, відкритих джерел. На відміну від таємної чи технічної розвідки, OSINT не потребує подолання заборон або здобуття доступу до секретної інформації. Англійський термін «Open Source Intelligence» (OSINT) буквально перекладається як «розвідка з відкритих джерел». Ключове слово «open» у цьому контексті означає публічну доступність джерела інформації та відсутність необхідності в таємних методах його отримання [11]. Доречно згадати, що локальними актами НАТО визначено, що розвідка з відкритих джерел має результатом певну розвідувальну продукцію, засновану на публічно доступній інформації, яка була зібрана, оброблена та розповсюджена вчасно, щоб задовольнити потреби конкретного користувача – міжнародною організацією акцентується увага на тому, що в межах OSINT здобувається не лише набір відкритої інформації, а оброблений фахівцями кінцевий системний продукт інтелектуальної діяльності [12]. Дослідники також дотримуються схожого підходу до визначення дефініції OSINT через призму кінцевої мети застосування цього виду розвідки, характеризуючи дане поняття як процес збору, обробки та аналізу публічно доступної інформації з метою отримання корисної розвідувальної інформації для прийняття рішень [13].

У наукових джерелах наголошується на тому, що важливо відрізняти OSINT від інших видів розвідки, таких як HUMINT (розвідка з використанням людських джерел), SIGINT (радіоелектронна розвідка), IMINT (візуальна розвідка) та CYBINT (кіберрозвідка). Основна відмінність полягає саме в природі джерел інформації. У той час як інші види розвідки часто використовують таємні або непублічні джерела, OSINT цілком покладається на публічно доступну інформацію і може застосовуватись багатогранністю в широкому спектрі галузей, включаючи національну безпеку, правоохоронну діяльність, бізнес-аналітику, журналістику розслідувань, кібербезпеку та академічні дослідження, не лише збираючи необхідну галузеву інформацію, але й проводячи її ретельний аналіз, контекстуалізацію та інтерпретацію для отримання цінних висновків [14].

Важливо наголосити, що сучасна історія застосування розвідки з відкритих джерел даних містить успішні практики застосування методів та інструментів OSINT не лише іноземними правоохоронними органами, а й інститутами громадянського суспільства. Зокрема, не можна обійти увагою успішні кейси, реалізовані представниками незалежної міжнародної журналістської спільноти «Bellingcat», Центром інформаційної стійкості (Centre for Information Resilience), приватною розвідувальною та аналітичною агенцією Molfar Intelligence Firm у ході запобігання та протидії злочинності та формуванні доказової бази при розслідуванні кримінальних правопорушень, окремі з яких проаналізовані в цій роботі.

Так, одним з вдалих кейсів застосування OSINT при розслідуванні особливо тяжких злочинів на території Лонг-Айленду, США є випадок виявлення серійного вбивці, відомого як «Gilgo Beach Murders» [15]. Ним виявився місцевий 59-річний архітектор з округу неподалік, який був успішно виявлений та ідентифікований завдяки аналізу баз відкритих даних в мережі Інтернет. Ключовим елементом доказової бази, сформованої за результатами використання OSINT методик стали дані про один з автомобілів, зареєстрованих за обвинуваченим – Chevrolet Avalanche першого покоління, марка та модель якого стала предметом спостереження випадкового свідка на місці одного з епізодів серійних вбивств. При встановленні зловмисника ключову роль відіграли наступні напрямки залучення OSINT:

– інструменти роботи з базами даних номерних знаків, VIN номерів та місцевих систем розпізнавання авто на базі штучного інтелекту «CarNet» – підтвердили зв'язок потенційного підозрюваного з автомобілем, що бачили на місці зникнення однієї з жертв;

– геопросторові дані та панорамні знімки вулиць сервісів Google та Bing Maps засвідчили, що вищезазначена модель автомобіля перебувала на подвір'ї підозрюваного у межах потенційного періоду вчинення епізодів серійних вбивств;

– аналіз цифрового сліду показав, що обвинуваченим була допущена необережність у вигляді використання особистого номеру телефону задля доступу до анонімної електронної пошти з метою спілкування з однією з жертв [16].

На додачу до вищезгаданої сукупності даних слідчими у ході спостереження за обвинуваченим було вилучено коробку з піцою, на одному з залишків якої було виявлено ДНК-зразки, які збіглися з ДНК чоловічої волосини, знайденої біля однієї з жертв. Ця справа продемонструвала, що збір і аналіз, на перший погляд, непов'язаних та розпорошених відкритих цифрових даних і застосування традиційних доказових методик щодо даних по автомобілю, геолокації, електронних аккаунтах та ДНК підозрюваного дозволили швидко прослідкувати логічні зв'язки та розкрити злочин [17].

Методики вивчення фотоматеріалів та метаданих зображень, що публікуються у соціальних мережах, суттєво полегшують ідентифікацію та притягнення до відповідальності осіб, які підозрюються у браконьєрстві. В останні роки слідчими органами різних штатів США успішно використовується аналіз соціальних мереж потенційних зловмисників та їх постів-вихвалянь, що обов'язково супроводжуються фотографіями чи відео на підтвердження своїх дій. Ресурс Bowhunting, зокрема, у одній зі статей вказує про щонайменше вісім успішних кейсів встановлення фактів браконьєрства на підставі звернення громадськості уваги на публікації мисливцями фотографій з дичиною, з яких слідчими органами було ідентифіковано, зокрема: випадки використання забороненого корму; полювання на тварин, щодо яких у конкретний період була заборона на відстріл; проникнення та полювання на територіях приватних угідь тощо, що стало достатніми початковими підставами для ініціювання розслідування та подальшого покарання винних у браконьєрстві [18].

У подібних випадках органами досудового розслідування використовувались наступні OSINT методики:

– аналіз геотегів з огляду на можливість безперешкодного доступу до них, яка надається соціальними мережами, у т.ч. Instagram, для визначення конкретної локації;

– аналіз спільноти потенційного браконьєра (яка теж може бути причетною до аналогічної протиправної діяльності) шляхом перегляду позначених друзів чи інших супутніх облікових записів, які часто взаємодіяли з профілем зловмисника;

– профілювання соціальних мереж підозрюваного шляхом відстеження його активності протягом певного часу, що дає змогу побудувати логічні зв'язки його активності в певних місцях [19].

У контексті викриття та розслідування мереж організованої злочинності з торгівлі людьми варто розглянути результати дослідження Л. Мейєр та Л. Шеллі, які звертають увагу на те, що сучасні злочинні організації цієї сфери використовують мережу Інтернет задля розширення своєї діяльності та охоплення дедалі більшої кількості клієнтів, одночасно забезпечуючи високий рівень власної анонімності [20]. Авторки вказують, що одним з рішень цієї проблеми стала розробка програми Memex Агентством передових оборонних дослідницьких проєктів США (DARPA) з метою індексації та аналізу даних з поверхневої частини мережі Інтернет та «даркнету», зосереджуючи свою увагу на даних з сайтів експорт-оголошень та форумів покупців сексуальних послуг. Memex надав правоохоронцям можливість візуалізувати зв'язки між, на перший погляд, непов'язаними оголошеннями, використовуючи такі ідентифікатори, як номери телефонів, електронні адреси, вебсайти, а також аналізуючи контекст оголошень та зображення, що дозволило перейти до проактивних, мережевих розслідувань, спрямованих на виявлення та знешкодження цілих злочинних організацій. У якості яскравої ілюстрації ефективності цього підходу авторки наводять вдалий кейс викриття китайської злочинної мережі, відомої як «Supermatchescort» [20].

Розслідування, що почалося з одного оголошення на сайті Backpage, завдяки аналізу даних у системі Memex переросло у викриття глобальної мережі операцій злочинної організації. Аналітики змогли відстежити та зв'язати понад 350 000 ескорт-оголошень, що розміщувалися протягом майже десятиліття. Мережа діяла на трьох континентах, у понад 50 містах, і мала клієнтську базу з 30 000 осіб. Слідчі відстежували номери телефонів, більшість з яких були мережевими VoIP-номерами (Voice over Internet Protocol), що вказувало на прагнення до анонімності і дистанційного керування, а також аналізували електронні адреси та, зрештою, виявили два ключові ідентифікатори мережі WeChat, які слугували центральними комунікаційними вузлами для всієї мережі [20].

У подальшому слідчі ідентифікували спільні мовні патерни, унікальні фрази та навіть послідовні орфографічні помилки в тисячах оголошень. Аналіз зображень виявив використання професійно знятих (але вкрадених) фотографій та послідовні методи приховування обличь (розмиття, емодзі), що слугувало візуальним почерком злочинної мережі. Аналіз, проведений із залученням розвідки з відкритих джерел, дозволив ідентифікувати ключових організаторів, розкрити їхню ієрархічну

структуру, логістичні ланцюги постачання жертв із Китаю та фінансові потоки і мав результатом пред'явлення обвинувачень семи громадянам Китаю та конфіскацію понад 500 веб-доменів, пов'язаних із діяльністю мережі [20].

Практика доводить, що OSINT може бути потужним інструментом правоохоронних органів для моніторингу, превенції та розслідування фактів соціальних заворушень. З аналізу звіту, підготовленого компанією Cobwebs Technologies на прикладі заворушень, що відбулися 6 січня 2021 року біля Капітолія США, вбачається, що події, які відбулися того дня, могли бути спрогнозовані з використанням засобів OSINT ще у ході автоматизованого аналізу соціальних мереж та форумів відповідними програмними засобами, що дозволило б не лише ідентифікувати потенційно небезпечних осіб, але й отримати інформацію про їхні плани, а також визначити точні місця збору злочинних груп у режимі реального часу, що є ключовим заходом для запобігання ескалації [20].

У випадку зі штурмом Капітолія, автоматизований пошук за ключовими словами та хештегами, такими як #dcprotest, #Stopthesteal, «Election fraud», «Proud boys», дав змогу отримати 247 результатів, що вказували на потенційні профілі та групи інтересу, аналіз яких показав, що агітатори використовували соцмережі для поширення ідеології та координації протесту, де були виявлені обговорення планів демонстрації, організації транспортування учасників, зокрема, за ключовими словами «rally», «caravan» [20].

Правоохоронцями були ідентифіковані «топ-інфлюенсери», чиї дописи отримували найбільше поширень та лайків, що вказувало на їхню лідерську роль – дані особи висловлювали прямі заклики до насильства, підпалів, вбивства поліцейських та скоординованих нападів, а інструменти візуалізації даних показали, як інфлюенсери та їхні послідовники поширювали повідомлення, залучаючи групи білих супремасистів, конспірологів та екстремістів. Зрештою, у наступні дні після штурму було заарештовано кількох підозрюваних, а Федеральне бюро розслідувань США вперше в історії звернулося до громадськості через свій веб-сайт із проханням надати будь-яку інформацію та цифрові медіафайли, що могли б допомогти ідентифікувати осіб, які підбурювали до насильства [21].

У контексті використання OSINT у запобіганні митних правопорушень заслуговує на увагу звіт Всесвітньої митної організації (ВМО) 2024 року, у якому підкреслюється, що роль митних адміністрацій значно розширилася - окрім традиційного збору доходів, митні органи відіграють ключову роль у забезпеченні національної та міжнародної безпеки, боротьбі з незаконною торгівлею та захисті суспільства [22]. Інтеграція OSINT у практику митних адміністрацій є не просто бажаною, а необхідною еволюцією у сучасному світі з огляду на численне зростання обсягу цифрових даних. Відтак, у звіті пропонується потенційне використання у майбутньому розвідки з відкритих джерел у наступних напрямках:

– автоматичний моніторинг глобальних новин, соціальних мереж та спеціалізованих форумів для раннього виявлення нових методів контрабанди, змін у маршрутах незаконного обігу та нових тенденцій у торгівлі;

– створення детальних профілів осіб, компаній та вантажів з високим ризиком, аналіз їх діяльності, ділових зв'язків та історії діяльності, подальша візуалізація зв'язків між учасниками незаконної діяльності, що допомагає виявляти та знешкоджувати цілі контрабандні мережі на основі виявлення закономірностей у базах та джерелах відкритих даних;

– ретроспективна аналітика даних з відкритих джерел, яка дозволяє прогнозувати майбутні ризики у діяльності митних органів, наприклад, сплески контрабанди під час свят або економічних спадів;

– перевірка автентичності торговельних документів шляхом порівняння даних з рахунків-фактур з інформацією з комерційних баз даних, корпоративних реєстрів та інших відкритих джерел;

– порівняння задекларованої вартості товарів з ринковими цінами та виявлення значних розбіжностей, що можуть свідчити про ухилення від сплати мит [22].

В контексті огляду OSINT-розслідувань не можна лишити поза увагою проведення громадського розслідування збиття рейсу MH17 у 2014 році, яке стало одним із найвизначніших прикладів успішного застосування OSINT, де ключову роль відіграло незалежне об'єднання розслідувачів Bellingcat [23]. Використовуючи виключно відкриті джерела, команда Bellingcat змогла відтворити події, що передували трагедії. Основним методом був ретельний аналіз значної кількості фотографій та відео, опублікованих у соціальних мережах свідками та учасниками подій. Центральним об'єктом розслідування став зенітно-ракетний комплекс «Бук». Bellingcat вдалося відстежити точний маршрут переміщення цієї установки до місця, звідки, ймовірно, було здійснено запуск ракети, а потім її повернення до попереднього місця розміщення. Аналітики порівнювали деталі на фотографіях, визначили місцевість та вибудовували хронологію руху колони, що дозволило з високою точністю ідентифікувати конкретну одиницю озброєння та її приналежність. Висновки, зроблені Bellingcat,

були опубліковані у детальному звіті, який отримав широкий розголос, а згодом – був верифікований офіційним міжнародним розслідуванням, яке очолювали Нідерланди. Цей кейс вкотре продемонстрував світові, що ретельний аналіз відкритих даних може бути таким же потужним інструментом у встановленні істини, як і традиційні методи розвідки [23].

Наостанок зазначимо, що слідчою практикою різних країн, які мали досвід використання OSINT-методик у сфері розслідування кримінальних правопорушень, застосовуються різні підходи до розуміння правових і етичних рамок застосування розвідки з відкритих джерел у сфері протидії злочинності. Загальною тенденцією, напевно, можна назвати визнання OSINT законним інструментом, якщо збір інформації відбувається виключно з публічних джерел відкритих даних, і при цьому не порушуються нормативні акти у сфері захисту персональних даних чи інших конституційних прав людини і громадянина та нівелюється можливість порушень відповідних процесуальних правил проведення досудового розслідування. Відмітимо, що на важливості дотримання процедурних вимог, які покликані забезпечити не лише допустимість, а й достовірність отриманої доказової інформації, наголошують й вітчизняні дослідники. До прикладу, І. Гловюк, з посиланням на відповідні кейси з судової практики, акцентує увагу на тому, що при формуванні судового рішення результати OSINT мають бути відображені таким чином, щоб неупередженому спостерігачу було зрозуміло, чому суд вважає їх достовірними, основою чого є правильне фіксування правоохоронними органами здобутих в результаті OSINT доказів з дотриманням рекомендацій протоколу Берклі у досудовому розслідуванні [2].

Висновки. Проаналізовані зразки окремих успішних практик застосування розвідки з відкритих джерел даних в мережі Інтернет дають можливість констатувати, що OSINT набуває статусу невід'ємної та ефективної складової сучасних кримінальних розслідувань у досвіді зарубіжних країн на рівні стандартизованої практики, яка у тому чи іншому вигляді вже інтегрована у повсякденну роботу правоохоронних органів від місцевого до міжнародного рівня.

Постійна еволюція OSINT-методик та інструментів значно підвищує ефективність виявлення, запобігання та розкриття злочинів, сліди яких можливо простежити, аналізуючи цифрові дані у відкритих джерелах у кожному конкретному злочинному діянні.

Водночас, попри доведену практичну результативність використання OSINT іноземними правоохоронцями, у національній слідчій практиці розкриття потенціалу використання OSINT скоріше виняток, ніж правило (не в останню чергу через наявну неузгодженість між наявними технологічними можливостями та правилами їх належної процесуальної, методологічної і тактичної інкорпорації в слідчу практику).

Для України, яка прагне інтегруватися у світову правову систему (у тому числі у сфері розбудови ефективної системи протидії злочинності) вивчення та впровадження передового іноземного досвіду використання OSINT, штучного інтелекту та машинного навчання є життєво необхідним кроком. Вказаний напрям є надважливим як у контексті забезпечення загальної атмосфери дотримання прав людини та законності у цифрову епоху, так і з огляду на потребу належної фіксації воєнних злочинів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Басиста І.В., Гаврилюк Л.В., Гутник А.В., Хитра А.Я. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право*. 2024. Вип. 17. С. 227–243. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243.
2. Гловюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 91, ч. 4. С. 251–259. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.35.
3. Каланча І.Г. Докази електронної форми у кримінальному процесі України: теорія та практика: дис. … д-ра юрид. наук: 12.00.09. Київ, 2025. 617 с. URL: https://elar.navs.edu.ua/items/359020b0-8ac4-40b5-adbe-3ba8085b450e.
4. Погорецький М.А. Цифрові (електронні) докази та цифрова (електронна) форма доказів: розмежування понять і його значення для кримінального процесу. *Аналітично-порівняльне правознавство*. 2026. № 1, ч. 3. С. 115–125. DOI: https://doi.org/10.24144/2788-6018.2026.01.3.18.
5. Скрипник А.В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Харків: Право, 2022. 408 с. DOI: https://doi.org/10.31359/9789669982940.
6. Смаль І.А. Теоретичні та практичні аспекти використання електронних доказів у кримінальному процесі України: монографія. Київ: Юрінком Прес, 2025. 282 с.

7. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень: підручник. Одеса : Юридика, 2024. 180 с. DOI: https://doi.org/10.32837/11300.27740.
8. Пашковський М.І. Цифрова інформація з відкритих джерел. Відкриті цифрові дані у кримінальному провадженні. *Концептуальні основи цифровізації кримінального провадження України: монографія* / ред. Н.В. Глинська. Харків: Право, 2024. С. 233–274. DOI: https://doi.org/10.31359/9786178612139.
9. Шевчук В.М. Використання технологій штучного інтелекту в OSINT як напрям підвищення ефективності розслідування воєнних злочинів. *Роль OSINT-досліджень у підвищенні рівня національної безпеки України: матеріали круглого столу (м. Львів, 7 трав. 2025 р.)*. Львів, 2025. С. 239–243. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/8875.
10. Цифрова криміналістика та її роль у формуванні доказової інформації в умовах воєнних дій: монографія / за ред. В.Ю. Шепітька. Харків: Право, 2025. 200 с.
11. Lowenthal M.M. Intelligence: From Secrets to Policy. 8th ed. Washington, DC: CQ Press, 2017. 616 p.
12. NATO Open Source Intelligence Handbook. Norfolk, VA : NATO Intelligence Branch, 2001. 49 p. URL: https://archive.org/details/NATOOSINTHandbookV1.2/page/n5/mode/2up.
13. Blanco V.M. An Introduction to Open Source Intelligence (OSINT). Praha : Center for Security Analyses and Prevention (CBAP), 2022. 8 p. URL: https://cbap.cz/wp-content/uploads/Introduction-to-OSINT-CBAP.pdf.
14. Omand D., Bartlett J., Miller C. Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*. 2012. Vol. 27, No. 6. P. 801–823. DOI: http://dx.doi.org/10.1080/02684527.2012.716965.
15. Catching the Long Island Serial Killer: The Crucial Role of Digital Data. Pt. 1. *Evidence Solutions.* 2023. URL: https://evidencesolutions.com/digital-evidence-articles/catching-the-long-island-serial-killer-the-crucial-role-of-digital-data-part-1.
16. Catching the Long Island Serial Killer: The Crucial Role of Digital Data. Pt. 2. *Evidence Solutions.* 2023. URL: https://evidencesolutions.com/digital-evidence-articles/catching-the-long-island-serial-killer-the-crucial-role-of-digital-data-part-2.
17. Sgueglia K., Gingras B., Miller J., Beech S. Burner phones. Pizza crust. DNA on burlap. A New York architect was charged with killing 3 women in Gilgo Beach serial killings cold case. *CNN US*. 2023, 17 July. URL: https://edition.cnn.com/2023/07/14/us/gilgo-beach-murders-suspect-arrest/index.html.
18. Scherder R. 8 Poachers Busted by Social Media Posts. *Bowhunting*. 2022, 16 March. URL: https://www.bowhunting.com/article/7-poachers-busted-by-social-media-posts/.
19. Gupta V. K. Case Studies of Successful OSINT Investigations. *LinkedIn*. 2024, 10 October. URL: https://www.linkedin.com/pulse/case-studies-successful-osint-investigations-vijay-gupta--0b7cc/.
20. Meyer L. F., Shelley L. I. Human Trafcking Network Investigations: Te Role of Open Source Intelligence and Large-Scale Data Analytics in Investigating Organized Crime. *International Journal on Criminology*. 2020. Vol. 7, No. 2. P. 87–100. URL: https://par.nsf.gov/servlets/purl/10183848.
21. Using OSINT in Times of Social Unrest: Capitol Hill Riots Intelligence Report. *Cobwebs Technologies*. 2021. URL: https://static.carahsoft.com/concrete/files/9617/3384/0566/Cobwebs_-_Using_OSINT_in_Times_of_Social_Unrest.pdf.
22. World Customs Organization. Unlocking the Value of Open-Source Intelligence (OSINT) for Customs Enforcement: Study Report. Brussels, Belgium : WCO, 2024. 42 p. URL: https://www.wcoomd.org/en/media/newsroom/2024/august/unlocking-the-value-of-osint-in-customs-enforcement.aspx.
23. Higgins E. MH17 - The Open Source Evidence: A bell¿ngcat Investigation. *Bellingcat*. 2015, 8 October. URL: https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-the-open-source-evidence/.

Дата першого надходження рукопису до видання: 27.02.2026
Дата прийняття до друку рукопису після рецензування: 20.03.2026
Дата публікації: 3.04.2026