УДК 343.1
DOI https://doi.org/10.32782/2524-0374/2024-11/106

ОСОБЛИВОСТІ ВИКОРИСТАННЯ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ (OSINT) У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

PECULIARITIES OF USING OPEN SOURCE INTELLIGENCE (OSINT) IN CRIMINAL PROCEEDINGS

Коновалова Д.О., студентка IV курсу
Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка

У статті досліджуються особливості та проблемні аспекти використання розвідки на основі відкритих джерел (OSINT) у кримінальному провадженні. Розглядаються правові засади збору та процесуального оформлення даних, отриманих за допомогою OSINT-технологій. Проаналізовано міжнародні нормативно-правові акти, що регулюють діяльність розвідки на основі відкритих джерел, зокрема Протокол Берклі. Висвітлено основні етапи OSINT-розслідування, включаючи формування завдання, збір інформації, оцінку, узагальнення та аналіз даних. Особлива увага приділяється проблемам захисту персональних даних при зборі інформації та ризику деанонімізації слідчого. Автор детально зупиняється на методах і інструментах OSINT, таких як пошукові системи (Google, DuckDuckGo), штучний інтелект (наприклад, Clearview AI), а також веб-скрейпінг. Опис інструментів охоплює як базові, так і інноваційні засоби. Таким чином, у статті обґрунтовано важливість комплексного підходу до захисту слідчих і обробки даних під час OSINT-розслідувань. Серед практичних рекомендацій зазначено необхідність документування зібраної інформації, використання сучасних OSINT-інструментів та дотримання міжнародних стандартів. У статті також зазначено, що ризики деанонімізації посилюються через цифрові загрози, такі як фішингові атаки, атаки типу «відмова в обслуговуванні» (DoS), шкідливе програмне забезпечення та маніпуляції соціальної інженерії. Для мінімізації цих загроз необхідно розробляти чіткі стратегії кіберзахисту та використовувати лише перевірені OSINT-інструменти. Окремо висвітлено роль спеціалістів у сфері OSINT для підвищення ефективності розслідувань. На основі аналізу судової практики визначено особливості допустимості електронних доказів, отриманих з відкритих джерел, у кримінальному провадженні. Наголошується, що результати OSINT-розслідувань мають значення лише за умови їх правильної правової фіксації, що забезпечує допустимість електронних доказів у суді. Пропонується вдосконалення законодавства України шляхом закріплення термінів «електронні докази» та «розвідка на основі відкритих джерел» у КПК України.

Ключові слова: розвідка на основі відкритих джерел, OSINT, кіберрозвідка, досудове розслідування, електронні докази.

The article examines the peculiarities and problematic aspects of using open source intelligence (OSINT) in criminal proceedings. The legal basis for the collection and procedural processing of data obtained through OSINT technologies is considered. The author analyses international legal acts regulating the activities of open source intelligence, in particular, the Berkeley Protocol. The main stages of an OSINT investigation are highlighted, including the formation of a task, collection of information, evaluation, synthesis and analysis of data. Particular attention is paid to the problems of personal data protection during information collection and the risk of de-anonymisation of the investigator. The author elaborates on OSINT methods and tools, such as search engines (Google, DuckDuckGo), artificial intelligence (e.g., Clearview AI), and web scraping. The description of the tools covers both basic and innovative tools. Thus, the article substantiates the importance of an integrated approach to the protection of investigators and data processing during OSINT investigations. The practical recommendations include the need to document the information collected, use modern OSINT tools and comply with international standards. The article also notes that the risks of de-anonymisation are increasing due to digital threats, such as phishing attacks, denial-of-service (DoS) attacks, malware and social engineering manipulations. To minimise these threats, it is necessary to develop clear cyber defence strategies and use only proven OSINT tools. The article also highlights the role of OSINT specialists in improving the effectiveness of investigations. Based on the analysis of case law, the author identifies the peculiarities of admissibility of electronic evidence obtained from open sources in criminal proceedings. It is emphasised that the results of OSINT investigations are relevant only if they are properly recorded in law, which ensures the admissibility of electronic evidence in court. The author suggests improving the legislation of Ukraine by introducing the terms ‘electronic evidence’ and ‘open source intelligence’ into the Code of Criminal Procedure of Ukraine.

Key words: open source intelligence, OSINT, cyber intelligence, pre-trial investigation, electronic evidence.

Постановка проблеми. Російська збройна агресія значно поширила використання OSINT-технологій у світі та Україні, зокрема, сприяла заснуванню InformNapalm, «Миротворець», «Molfar», які проводять збір інформації з відкритих джерел. Наприклад, компанія «Molfar» безкоштовно надає військовий аналіз українським медіа-організаціям та поширює інформацію про ключові військові події в Україні серед представників міжнародних коаліцій, послів країн ЄС в Україні та міжнародних організацій, які розслідують військові злочини. Проте, існує ряд проблемних питань пов’язаних з процесуальним оформленням даних, отриманих за допомогою інструментів OSINT-досліджень, захисту персональних даних при зборі інформації, ризик деанонімізації слідчого, дізнавача, прокурора (суб’єктів розслідування) під час проведення розслідувань кримінальних правопорушень.

Аналіз досліджень та публікацій. Серед міжнародних нормативно-правових актів, що регулюють діяльність розвідки на основі відкритих джерел є Конвенція Ради Європи про кіберзлочинність від 23.11.2001 та Другий додатковий протокол до Конвенції Ради Європи про кіберзлочинність, Директива Європейського Союзу 2019/1024 Про відкриті дані та повторне використання інформації державного сектору, Директива Європейського Союзу 2019/790 Про авторське право та суміжні права, Загальний регламент про захист даних (GDPR) та Протокол Берклі.

Теоретичні та практичні аспекти застосування OSINT у кримінальному провадженні досліджуються вітчизняними науковцями, зокрема Торбасом О.О., Кожевніковим О.А., Паламарчуком О.А., Демедюком С.В. та іншими.

Мета роботи. Мета роботи полягає у комплексному дослідженні особливостей та проблемних аспектів використання розвідки на основі відкритих джерел (OSINT) у кримінальному провадженні, зокрема аналізі правових засад збору та процесуального оформлення даних, отриманих у ході розвідки на основі відкритих джерел як доказів, вивченні методів та засобів проведення OSINT-розслідувань, а також формулюванні практичних рекомендацій щодо ефективного застосування OSINT-технологій під час розслідування кримінальних правопорушень.

Виклад основного матеріалу. В умовах сьогодення, одним з перспективних джерел отримання вагомої інформації для досудового розслідування є технологія OSINT. Наприклад, ордер на арешт Махмуда Мустафи Бусайфа Аль-Верфаллі – командира бригади «Аль-Сайка» Лівійської національної армії, був виданий Міжнародним кри-

мінальним судом на основі інформації з відкритих джерел. Сім відеозаписів опублікованих у соцмережах стали ключовими доказами для суду у винесенні вироку Аль-Верфаллі у вчиненні умисного вбивства як воєнного злочину згідно ст. 8(2)(c)(i) Римського статуту [1].

Тому використання методів OSINT-розслідувань є надзвичайно ефективним під час проведення розслідувань кримінальних правопорушень, у тому числі воєнних злочинів, оскільки дозволяє отримати інформацію, яка є у відкритому доступі. Надалі, щоб дана інформація у відкритому доступі могла бути використана як доказ у суді, суб'єкти розслідування, як правило, повинні мати змогу встановити її достовірність, етапи збору та забезпечення збереження.

З огляду на це, варто керуватися Протоколом Берклі [2], який є першим у світі міжнародним порадником для отримання загальнодоступної інформації, яка у подальшому може мати вагоме значення для досудового розслідування та судового розгляду кримінальних проваджень.

До того ж, слідчий, дізнавач, прокурор, які проводять розслідування з використанням OSINT-інструментів мають керуватись такими принципами, як підзвітність, компетентність, об'єктивність, законність, проінформованість про безпеку, тощо. Так, суб'єкт розслідування повинен фіксувати у протоколі інструменти або програмне забезпечення, що використовуються під час роботи, мати належний рівень підготовки та вдосконалювати технічні навички для проведення OSINT-розслідування, а також мати базову обізнаність щодо оперативної безпеки для мінімізації свого цифрового сліду [2]. Слідчі, дізнавачі та прокурори мають бути усвідомлені про три основні рівні інформаційної безпеки – конфіденційність, цілісність, доступність. Дотримання вимоги конфіденційності означає надання лише повноважним користувачам отримувати доступ до даних, із забезпеченням того аби інформація не змінювалась неавторизованими користувачами (цілісність). Суб'єктам розслідування має бути забезпечено доступ до систем та даних, коли вони цього потребують.

Перед початком проведення OSINT-розслідування, варто враховувати цифрові загрози та ризики, а також скласти план онлайн-розслідування, який охоплює загальну стратегію розслідування та конкретні операції з його здійснення в інтернеті. Даний план пошуку можна поділити на етапи: формування завдання, збір інформації, її оцінка, узагальнення, аналіз та подальше розповсюдження. Формування завдання передбачає постановку мети та обсягу необхідного завдання. Саме після чіткого визначення основних завдань суб'єкт розслідування починає планування подальших дій [3].

Збір інформації полягає у здатності знаходити та використовувати дані за допомогою OSINT-інструментів, які постійно змінюються та вдосконалюються. Ще до початку проведення OSINT-розслідування, слідчий, дізнавач, прокурор має самостійно здійснити пошук необхідних інструментів, враховуючи власні технічні можливості, якими він володіє та пам'ятаючи про важливість не конкретного інструменту, а цінності інформації, що може бути отримана завдяки інструменту.

Проводячи OSINT-розслідування суб'єкт розслідування може скористатись пошуком, або ж виявленням інформації та джерел інформації за допомогою загальних або розширених методологій пошуку та моніторингу, що полягає у відстеженні встановленого джерела інформації з плином часу. На даному етапі слідчому важливо проводити попередню оцінку отриманого матеріалу, який він ідентифікує та забезпечити дотримання захисту права на приватне життя. Збір інформації, що була виявлена у ході OSINT-дослідження може здійснюватись будь-якими методами залежно від її доказової сили (скріншот, визначення хеш-суми тощо).

Найпоширенішими OSINT-інструментами у роботі є пошукові сервіси – Google або DuckDuckGo. Робота пошукового сервісу складається зі сканування інформації, її аналізу, зберігання в індексі та обслуговування результатів пошуку. Наприклад, Google для сканування та вибірки сторінок використовує програму Googlebot, яка застосовує алгоритмічний процес. Надалі, у ході індексації пошуковий сервіс групує разом сторінки, що мають подібний вміст і обирає ту, що є найбільш репрезентативною та якісною, розміщуючи її на запит користувача [3]. Інноваційним є застосування SearchGPT – пошукової системи на основі штучного інтелекту, що не лише генерує відповіді та посилання, а й надає оригінальні матеріали та першоджерела. Таким чином, суб'єкт розслідування, керуючись пошуковими сервісами, може зібрати ключову інформацію для досудового розслідування, отримавши її документальне підтвердження.

Штучний інтелект, як інструмент OSINT-розслідування, допомагає швидко отримувати інформацію, аналізувати великі обсяги даних з різних джерел, визначати закономірності та виявляти потенційні загрози, а також розпізнавати обличчя. Наприклад, в Україні з 2022 року, суб'єктами розслідування використовується програмне забезпечення Clearview AI, що допомагає ідентифікувати російських солдатів та диверсантів на контрольно-пропускних пунктах, а також встановлювати підозрюваних осіб у вчиненні військових злочинів. База даних містить навіть ті зображення, які були видалені з інтернету.

Натомість, відповідно до ч. 1 ст. 9 Загального регламенту захисту даних ЄС та ч. 1 ст. 7 Закону України «Про захист персональних даних», забороняється обробка біометричних або генетичних даних [4; 5]. Так, компанії Privacy International, Digital Human Rights та Homo Digitalis подали кілька юридичних позовів проти компанії Clearview AI, стверджуючи про наявність порушення положень Загального регламенту захисту даних ЄС щодо обробки чутливих даних, відсутності прозорості та законних підстав для обробки даних [6]. Таким чином, варто пам'ятати, що певне програмне забезпечення може не відповідати вимогам міжнародного та українського законодавства у сфері захисту даних.

На етапі узагальнення зібраної інформації у ході проведення OSINT-розслідування відбувається копіювання та збереження інформації. Отримані дані, що містять важливу інформацію для досудового розслідування, варто зберігати як в оригінальному вигляді, так і забезпечити додаткове збереження шляхом створення копій на окремому носії інформації. До того ж, для підвищення ефективності OSINT- розслідування, може здійснюватись переклад, об'єднання різних наборів даних та їхнє переформатування. Вказані дії мають виконуватись на робочих копіях цифрового елемента та бути обов'язково задокументовані та внесені у протокол відповідної процесуальної дії. Єдиним можливим інструментом документування зібраних даних на етапі досудового розслідування є протокол огляду. Протокол дозволяє зафіксувати зміст досліджуваної сторінки та зберегти сам матеріал, зазначивши про це в додатку.

Важливим етапом розслідування є перевірка виявлених даних, яка полягає у технічному аналізі, перевірці надійності джерела та аналізу контенту. Збираючи дані в мережі Інтернет варто брати до уваги походження джерела, його надійність, належність та допустимість. Суб'єкт розслідування має дослідити зв'язки між об'єктом, стосовно якого здійснюється збір даних, та відповідним джерелом.

Аналіз окремих сторінок переважно відбувається шляхом дослідження зображення, відео, самого вебсайту, його коду тощо. Суб'єкт розслідування при здійсненні аналізу коду вебсайту першочергово має звертати увагу на шапку документа, яка містить метадані, та так зване «тіло документа» [3]. Процес збору інформації сайту який включає

в себе надсилання запиту до сервера, отримання HTML вмісту сторінки та копіювання цього змісту має назву вебскрейпінг (Web Scraping), що може надавати додаткові відомості про веб-сайт.

Поверхневе дослідження цифрових даних не є абсолютним підтвердженням їх достовірності, тож у певних випадках варто здійснювати глибший аналіз, що може включати підтвердження контенту метаданими. Для перевірки цілісності файлу, піддаються аналізу метадані – дані, які описують та надають інформацію про формат файлу зображень та вихідний код, який легко переглядається за допомогою програмного забезпечення. Вихідний код може містити інформацію про дані, прихований або змінений контент, а також відображатиме структуру посилань та непрацюючі посилання. Це надасть суб'єкту розслідування розуміння про цілісність файлу, його ймовірні зміни та модифікації.

Без фіксації метаданих ефективність OSINT-досліджень на основі зображень і відео може знижуватись. Це пов'язано з тим, що метадані містяться у фото, відео, веб-сайтах, pdf файлах тощо, оскільки надають відомості про саме джерело інформації незалежно від її типу. Також варто пам'ятати, що певні соціальні мережі автоматично видаляють дані про координати місця, де було зроблено фото, одразу після завантаження такого фото у мережу. Однак, відомості, отримані з метаданих, не можуть використовуватися як докази в кримінальному провадженні, а тільки можуть вказувати на інші відомості, які потребують подальшої перевірки.

Аналізуючи зібрану інформацію, суб'єкту розслідування варто спиратись на візуальні підказки, що містяться у відео, зображенні або документі. Наприклад, напередодні обстрілу торгово-розважального центру «Retroville» 20.03.2022 у м. Київ, невідомим автором було викладено відеоматеріал у соціальну мережу «TikTok» з розміщенням української бойової техніки поблизу центру [7]. Можна стверджувати, що ворог отримав вказану інформацію з використанням відкритих джерел, проте наявність відкритого профілю автора в соціальній мережі може надати також вагому інформацію для притягнення його до кримінальної відповідальності.

Таким чином, згідно Протоколу Берклі, на етапі аналізу та фіксації інформації суб'єкту розслідування пропонується звертати увагу на такі елементи цифрового контенту, як цільова веб-адреса (єдиний локатор ресурсів), вихідний код, вбудовані метадані та мультимедійні файли, контекстуальні дані, дані збору та хеш-значення, оскільки вказана інформація може бути використана в подальшому у ході досудового розслідування [2].

Аналізуючи мережу інтернет, варто пам'ятати про існування трьох його рівнів – поверхневий інтернет (сайти новин, соціальні мережі), глибокий інтернет (бази даних установ, вхід в які здійснюється за допомогою подолання систем логічного захисту) та тіньовий інтернет (Dark Web) або ж сукупність усіх мереж Dark Net. Слідчий, дізнавач, прокурор, який буде проводити розслідування в тіньовому інтернеті, як правило, буде робити це саме у зв'язку із вчиненням злочинів конкретно в Dark Web, а не через те, що йому необхідно отримати додаткову інформацію про об'єкт розслідування, відомості про який містяться в поверхневому інтернеті[3].

Окремою проблемою під час здійснення OSINT розслідування може стати деанонімізація слідчого, дізнавача чи прокурора. Щоб цього уникнути слід обирати надійні та перевірені інструменти для проведення розслідування, що не привертають увагу. Наприклад, програмне забезпечення Maltego надає можливості для безпечного обміну отриманими у ході дослідження результатами, ознайомлює з оглядом загроз і звітом про розслідування всередині компанії, яка веде дослідження. Суб'єктами розслідування використовуються спеціальні інструменти запобігання отримання несанкціонованого доступу до камер та мікрофонів на пристрої проведення розслідування та встановлення трекерів, маячків, маскування IP-адреси та блокування файлів cookie. Загрозами, згідно гл. 4 Протоколу Берклі є також атаки: «відмова в обслуговуванні» (DoS – атака), фішингові атаки, атаки через посередника та шкідливе програмне забезпечення [2]. Так звана DoS – атака є одним з найпоширеніших методів нападу, що полягає у насиченні атакованого комп'ютера великою кількістю зовнішніх запитів. Найбільш небезпечними є атаки соціальної інженерії (фішинг), оскільки зловмисники проводять дослідження особи, щоб знайти слабкі місця в системі безпеки. Серед прикладів відомих соціальних інженерних атак є фішинг, коли зловмисник виманює особу надати свої конфіденційні дані, шляхом підміни сайту або електронної пошти.

Найбільш вагомою є об'єктивна потреба в кваліфікованому експертному вивчені зовнішності осіб на етапі аналізу зібраних даних в OSINT- розслідуванні. Уповноваженими на проведення даного виду дослідження є спеціалісти та експерти, що мають кваліфікацію за експертною спеціальністю 6.2 «Ідентифікація особи за ознаками зовнішності за матеріальними зображеннями» [8]. Крім того, залучення спеціаліста дозволить суб'єкту розслідування звернути увагу на важливі компоненти зібраних даних у ході розвідувальної діяльності. Відповідно до п. 9 ч. 4 ст. 71 Кримінального процесуального кодексу України (далі – КПК України), спеціаліст, на основі зібраних суб'єктом розслідування даних має право надавати довідки, висновки з питань, що належать до сфери його знань, зокрема щодо ідентифікації особи. Відповідно до ч. 2 ст. 84 КПК України, процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів. Згідно положень ст. 99 КПК України, до документів, за умови наявності в них відомостей, ч. 1 цієї статті, можуть належати довідки, висновки та інші документи спеціалістів. [9]. Отже, висновок спеціаліста на основі зібраних суб'єктом розслідування даних має доказове значення відповідно до положень ст. 99 КПК України

Оскільки під час OSINT-розслідувань дані збираються з відкритих джерел, постає питання про подальше використання їх як доказів (електронних доказів) у кримінальному провадженні. Відповідно до п. 21 Протоколу Берклі, термін «докази» слід відрізняти від «інформації». Докази з відкритих джерел – це інформація у відкритому доступі із доказовою цінністю, яка може бути допущена для встановлення фактів у судовому процесі [2].

Для того щоб фактичні дані у подальшому могли використовуватися у кримінальному провадженні як докази (електронні докази), вони мають отримуватися в передбаченому процесуальним законом порядку, у протилежному випадку вони будуть визнаватися недопустимими доказами.

Відповідно до ч. 2 ст. 84 КПК України, процесуальними джерелами доказів є показання, речові докази, документи та висновки експертів. Згідно з ч. 1 ст. 99 КПК України, документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. Оригіналом електронного документа є його відображення, якому надається таке ж значення, як документу (ч. 3 ст. 99 КПК України). При цьому дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста,

визнаються судом як оригінал документа (ч. 4 ст. 99 КПК України) [9].

Як зазначено в постанові Об'єднаної Палати Касаційного кримінального суду у складі Верховного Суду від 29 березня 2021 року у справі № 554/5090/16-к, для виконання завдань кримінального провадження, з огляду на положення Закону України «Про електронні документи та електронний документообіг» (далі – Закон), допустимість електронного документа як доказу не можна заперечувати винятково на підставі того, що він має електронну форму (ч. 2 ст. 8). Відповідно до ст. 7 цього Закону у випадку його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа [10]. Один і той самий електронний документ може існувати на різних носіях. Усі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом і датою створення. Питання щодо ідентифікації електронного документа як оригіналу можуть бути вирішені уповноваженою особою, яка його створила (за допомогою спеціальних програм порахувати контрольну суму файлу або каталогу з файлами CRC-сума, hash-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень.

Відповідно до постанови суддів Другої судової палати Касаційного кримінального суду у складі Верховного Суду від 06 лютого 2024 року у справі № 645/6247/16-к, технічний носій інформації, на якому зафіксовано проведення слідчої дії, за обставин кримінального провадження, є електронним доказом, на якому міститься інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи. Технічний носій інформації на якому зафіксовано проведення слідчого експерименту, а саме його відеозапис містить достатні відомості, що відображають хід його проведення, що за своєю природою є самостійним джерелом доказів, визначеним ст. 84 КПК України [11].

Висновки та пропозиції. Процес OSINT-розслідування складається з наступних етапів: формування завдання, збір інформації, оцінка, узагальнення та аналіз даних, що вимагає від суб'єкта розслідування відповідних технічних навичок та знань. З розвитком OSINT технології та впровадження їх задля спротиву російській агресії важливо підвищити рівень їх регулювання на законодавчому рівні.

Зокрема, пропонується внести зміни до ст. 15 Закону України «Про захист персональних даних», доповнюючи її додатковими гарантіями проти незаконної обробки особливих категорій даних, наприклад правом на забуття. Право на забуття міститься в ст. 17 Загального регламенту про захист даних і означає, що особа має право «на стирання своїх персональних даних» яке повинен здійснити контролер без будь-якої безпідставної затримки. Доцільним є введення на законодавчому рівні діяльності контролера, що уповноважений на «видалення» персональних даних.

До того ж, пропонуємо закріплення поняття розвідки на основі відкритих джерел та електронних доказів, шляхом внесення наступних змін в КПК України. Так, частину 2 статті 84 КПК України пропонуємо викласти в наступній редакції: «процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів та електронні докази». Доповнити статтю 84 КПК України частиною 3, виклавши її наступним чином: «електронні докази – це будь-яка інформація, що генерується, зберігається або передається в цифровій формі, яка згодом може знадобитися для підтвердження або спростування факту, оскаржуваного в межах провадження(в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних й інші дані в електронній формі» [12]. Пункт 1 частини 2 статті 237 КПК України пропонується викласти в такій редакції задля законодавчого закріплення поняття розвідки на основі відкритих джерел: «огляд комп'ютерних даних проводиться слідчим, прокурором шляхом розвідки на основі відкритих джерел (OSINT) та відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі).

Вказані зміни, на нашу думку, повинні забезпечити ефективне проведення OSINT-розслідувань слідчим, дізнавачем, прокурором та сприятимуть повному й швидкому розслідуванню і судовому розгляду кримінальних правопорушень.

ЛІТЕРАТУРА

1. Розслідування воєнних злочинів: Пошук у відкритих джерелах. Global Investigative Journalism Network. URL: https://gijn.org/ua/resurs-ua/rozsliduvanna-voennih-zlociniv-posuk-u-vidkritih-dzerelah/ (дата звернення: 03.11.2024).

2. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних: Пошук у відкритих джерелах. (б. д.). Організація Об'єднаних Націй. https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

3. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Юридика, 2024. URL: https://doi.org/10.32837/11300.27740 (дата звернення: 03.11.2024).Про захист персональних даних. (б. д.). Офіційний вебпортал парламенту України. https://zakon.rada.gov.ua/laws/show/2297-17#Text

4. Загальний регламент про захист даних (GDPR) – GDPR-Text.com. GDPR-Text.com – GDPR Text, Translation and Commentary. URL: https://gdpr-text.com/uk/ (дата звернення: 03.11.2024).

5. Закон України «Про захист персональних даних». *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 03.11.2024).

6. Наскільки «прозора» законність діяльності Clearview AI в Україні? – Лабораторія цифрової безпеки. Лабораторія цифрової безпеки – Захищаємо громадянське суспільство. URL: https://dslua.org/publications/clearview-ai-v-ukraini/ (дата звернення: 03.11.2024).

7. Учасники проектів Вікімедіа. Ракетний удар по торговому центрі «Retroville» у Києві – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Ракетний_удар_по_торговому_центрі_«Retroville»_у_Києві (дата звернення: 03.11.2024).

8. Кожевніков О. Залучення спеціаліста у галузі портретної експертизи на окремих етапах OSINT розслідувань. Теоретичні та прикладні проблеми судової експертизи і криміналістики. Харків. 2022. С. 85.

9. Кримінальний процесуальний кодекс України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 03.11.2024).

10. Постанова Об'єднаної Палати ККС ВС у справі №554/5090/16-к. URL: https://verdictum.ligazakon.net/document/96074938 (дата звернення: 03.11.2024).

11. Огляд судової практики Касаційного кримінального суду у складі Верховного Суду за І півріччя 2024 року. Верховний Суд. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/ogliady/Oglyad_KKS_I_pivr_2024.pdf (дата звернення: 08.11.2024).

12. Akhtyrska N. Legal regulation of electronic evidence and the practice of their use in the judiciary of Ukraine. Uzhhorod National University Herald. Series: Law. 2023. Vol. 2, no. 75. P. 141–150. URL: https://doi.org/10.24144/2307-3322.2022.75.2.23 (date of access: 07.11.2024).