УДК 343.13
DOI https://doi.org/10.24144/2307-3322.2025.91.4.35

ОЦІНКА РЕЗУЛЬТАТІВ OSINT У СУДОВІЙ ПРАКТИЦІ: ОКРЕМІ ПИТАННЯ

Гловюк І.В.,
докторка юридичних наук, професорка,
професорка кафедри кримінального процесу та криміналістики
Одеського державного університету внутрішніх справ,
Заслужена юристка України

Гловюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання.

У статті розглянуто питання оцінки результатів OSINT у судовій практиці за критеріями належності, допустимості, достовірності. Звернено увагу на те, що є випадки оспорювання належності та допустимості таких доказів, а також їх достовірності. Наведено підходи практики Касаційного кримінального суду з цього питання. Детально проаналізовано ефективність такого оспорювання на прикладі постанови Касаційного кримінального суду у справі № 201/11849/23 у контексті аргументів захисту та контраргументів (щодо належності, допустимості та достовірності фактичних даних).

Зроблено висновок, що джерелом доказів при використанні результатів OSINT, зафіксованих у протоколі за ст. 237 КПК України з додатками, є саме протокол як різновид документу. Відповідно, питання допустимості можуть стосуватися виключно аспектів проведення та фіксування огляду, дотримання вимог КПК України щодо належного суб'єкта, строків досудового розслідування та інших питань порядку збирання та фіксування даних, які містяться у протоколі. Якщо ж є сумніви стосовно змісту первинних зафіксованих даних, їх походження у відкритих джерелах (автора контенту, особи, яка його розмістила і мету такого розміщення), створення їх штучним інтелектом, створення та поширення їх з метою дезінформації, правильності їх технічного збирання, незмінності онлайн-контенту будь-якого виду, метаданих, хеш-значеннях – мова може йти про недостовірність доказів. У цій ситуації ініціація визнання таких фактичних даних недопустимими доказами позбавлена сенсу. Результати OSINT можуть містити фактичні дані, що не мають властивість належності, але це ніяк не пов'язано з аналізом джерела походження – відкритих даних, адже встановлюється зв'язок (чи його відсутність) з усіма обставинами предмета доказування. Відповідно, ініціація визнання доказів неналежними через сумніви стосовно змісту первинних зафіксованих даних, їх походження у відкритих джерелах (автора контенту, особи, яка його розмістила і мету такого розміщення) також позбавлене сенсу.

У судових рішеннях результати OSINT мають бути відображені таким чином, щоб неупередженому спостерігачу було зрозуміло, чому суд вважає їх достовірними. Основою цього є правильне фіксування з дотриманням рекомендацій протоколу Берклі у досудовому розслідуванні.

Ключові слова: результати OSINT, перевірка доказів, оцінка доказів, належність доказів, допустимість доказів, достовірність доказів, протокол огляду

Hloviuk I.V. Assessment of OSINT results in judicial practice: selected issues.

The article examines the assessment of OSINT results in judicial practice through the criteria of relevance, admissibility, and reliability. Attention is drawn to instances where the relevance, admissibility, and reliability of such evidence have been challenged. The approaches of the Criminal Cassation Court to this issue are presented. The effectiveness of such challenges is analysed in detail on the example of the decision of the Criminal Cassation Court in case no. 201/11849/23, in the context of the defence's arguments and the counter-arguments (regarding the relevance, admissibility, and reliability of factual data).

It is concluded that, where OSINT results are recorded in a report under Article 237 of the Code of Criminal Procedure of Ukraine with annexes, the report itself constitutes the source of evidence, as a

type of document. Accordingly, issues of admissibility may concern exclusively the manner in which the inspection was conducted and recorded, compliance with the requirements of the Code of Criminal Procedure of Ukraine as to the competent authority, the time limits of the pre-trial investigation, and other procedural aspects of the collection and recording of the data contained in the report. By contrast, if doubts arise concerning the content of the originally recorded data, their origin in open sources (the author of the content, the person who published it, and the purpose of such publication), their possible creation by artificial intelligence, their creation and dissemination for the purpose of disinformation, the correctness of their technical collection, the immutability of online content of any kind, metadata, or hash values, the issue at stake is the reliability of the evidence. In this situation, initiating a claim for the recognition of such factual data as inadmissible evidence is meaningless.

OSINT results may contain factual data that lack the quality of relevance, but this is in no way connected with the analysis of their source – namely, open data – since relevance is determined by the existence (or absence) of a connection with the circumstances subject to proof. Accordingly, initiating a claim for the recognition of evidence as irrelevant on the basis of doubts concerning the content of the originally recorded data or their origin in open sources (the author of the content, the person who published it, and the purpose of such publication) is also meaningless.

In judicial decisions, OSINT results must be presented in such a way that an impartial observer can understand why the court considers them reliable. The foundation for this lies in proper recording during the pre-trial investigation, in compliance with the recommendations of the Berkeley Protocol.

Key words: OSINT results, examining of evidence, evaluation of evidence, relevance of evidence, admissibility of evidence, reliability of evidence, inspection report.

Постановка проблеми. Використання результатів OSINT є доволі поширеним у сучасному кримінальному процесуальному доказуванні, що зумовлено цифровізацією сучасного світу та суспільних відносин, а також технологіями комунікації та впливу на свідомість. Це надало поштовх для досліджень цих питань у контексті українських практик, і найбільше – в умовах збройного конфлікту. Хоча КПК України і не містить такої термінології, є лист-орієнтування Офісу Генерального прокурора від 28.08.2021 № 18/1-386 «Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел», де вказується на використання протоколу Берклі [1]. При цьому сам протокол не є нормативним актом, а є документом «soft law». Крім того, існують Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals [2] та Hala Protocol for the Collection, Processing, and Transfer of Audio Data [3], Рекомендації для громадських організацій. Документування міжнародних злочинів і порушень прав людини для притягнення до кримінальної відповідальності осіб, що їх вчинили [4], Оцінка цифрових знімків з відкритих джерел: Посібник для суддів і дослідників фактів [5]. В Україні діє ДСТУ EN ISO/IEC 27037:2022 (EN ISO/IEC 27037:2016, IDT; ISO/IEC 27037:2012, IDT Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Наразі вже є деяка судова практика щодо оцінки результатів OSINT як джерел доказів.

Стан опрацювання проблематики. Ці питання досліджуються в контексті електронних (цифрових) доказів, OSINT як діяльності, результатів OSINT та механізмів їх використання такими вченими, як Д. Афонін, Л. Гаврилюк, І. Басиста, І. Биков, В. Бурлака, Р. Бутко, Ю. Виходець, А. Гутник, Є. Демидова, В. Дрозд, К. Латиш, Д. Лісніченко, І. Каланча, М. Капустіна, С. Касапоглу, А. Коваленко, С. Корнійко, Б. Косохатько, О. Метелев, М. Пашковський, В. Пелехатий, М. Погорецький, А. Скрипник, І. Смаль, Г. Тетерятник, О. Торбас, А. Хитра, А. Шевчишен та ін. З зарубіжних вчених з цих питань доречно згадати Hanna Kuczyńska, Hannah van Beek, Sebastiaan Rietjens, Deniz Mykola Dirisu, Manon-Catherine Balbinot, Alexa Koenig, Emma Irving, Yvonne McDermott, Daragh Murray, Stephen Sharp Queener, Basile Simon, Stefano Trevisan, etc.

Метою цієї статті є виокремлення тенденцій судової практики щодо оцінки результатів OSINT з позицій належності, допустимості, достовірності на основі аналізу наявної судової практики, зокрема ККС ВС.

Виклад основного матеріалу. Слушно зазначає М.І. Пашковський, що: КПК України не містить будь-якої регламентації щодо проведення розслідування з використанням відкритих джерел, а отже застосовуються загальні правила доказування [6, с. 256]; наразі КПК України не містить будь-яких застережень щодо збирання та використання в кримінальному провадженні

цифрової інформації, що знаходиться у відкритому доступі [7, с. 85]. Отже, результати OSINT мають оцінюватися з позицій належності та допустимості як властивостей доказів, а також достовірності, що випливає зі ст. 94 КПК України.

У вироках використовуються результати OSINT, хоча суди, як правило, не зазначають чи вживалися учасником, який надав цифрові докази з відкритих джерел, якісь заходи з їх перевірки. Виклад доказів обмежується лише посиланням на протоколи огляду або довідки за результатами OSINT [6, с. 271], що детально проаналізовано у цитованому дослідженні. Разом з тим, є випадки оспорювання належності та допустимості таких доказів. Підходи до вирішення таких питань можна ідентифікувати в практиці ККС ВС.

Проаналізуємо ефективність такого оспорювання на прикладі провадження, у якому вирок нещодавно переглядався ККС ВС. З викладу у постанові ККС ВС можна виокремити такі аргументи сторони захисту для визнання протоколі огляду телеграм-каналів та інтернет-ресурсів є недопустимими й неналежними доказами: здобуті в порядку, не передбаченому КПК (не встановлено офіційного існування інтернет-ресурсів, їх власників та користувачів, а також відповідальних осіб за розміщення інформації на них і за її перевірку), та не підтверджують існування даних, за якими можливо ідентифікувати особу ОСОБА_7 [8].

ККС ВС, спростовуючи ці аргументи, навів такі контраргументи:

- фактичні дані, зафіксовані у протоколах оглядів інтернет-сайтів та телеграм-каналів, отримано в порядку, передбаченому КПК;
- сторона захисту не дала жодних відомостей щодо спростування цієї інформації і не аргументувала, що інформація, надана органом досудового розслідування, не відповідає дійсності, зокрема, містить ознаки фальсифікації та/або навмисного спотворення даних.
- сторона захисту хоча й ставила питання про **недостовірність** доказів, однак не заявляла будь-яких клопотань про залучення спеціалістів чи експертів, проведення експертизи; захисник не вказує на порушення, допущені судами попередніх інстанцій, які би полягали у нерозгляді його клопотання про призначення експертизи або незаконної відмови у задоволенні такого клопотання; сторона захисту не була позбавлена можливості заявити під час проведення як досудового розслідування, так і в суді клопотання про призначення судово-портретної експертизи, однак таким правом не скористалася» [8].

Аналіз аргументів та контраргументів свідчить про те, що розглядалося питання як належності та допустимості, так і достовірності доказів. Розглянемо детальніше аргументи та контраргументи стосовно: (а) допустимості; (б) належності; (в) достовірності.

Питання допустимості фактичних даних. Формулювання «здобуті в порядку, не передбаченому КПК (не встановлено офіційного існування інтернет-ресурсів, їх власників та користувачів, а також відповідальних осіб за розміщення інформації на них і за її перевірку), та не підтверджують існування даних, за якими можливо ідентифікувати особу ОСОБА_7» [8] містять в собі заперечення допустимості через аналіз зміст фактичних даних, а не порядку їх збирання. Отже, вони не стосуються допустимості доказів, бо допустимим у КПК України визнано доказ, отриманий у порядку, встановленому КПК України (ч. 1 ст. 86 КПК України). Належності фактичних даних може стосуватися лише аргумент «не підтверджують існування даних, за якими можливо ідентифікувати особу ОСОБА_7» [8].

Що стосується саме порядку фіксування результатів OSINT, то він полягає у проведенні огляду у порядку ст. 237 КПК України, вимоги до якого деталізовані у листі-орієнтування Офісу Генерального прокурора від 28.08.2021 № 18/1-386 «Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел», де вказується на використання протоколу Берклі. Зокрема, ч. 2 цієї статті передбачає, що огляд комп'ютерних даних проводиться слідчим, прокурором шляхом 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). Доволі великий перелік способів відображення у протоколі інформації без надмірної деталізації дозволяє виконати рекомендації та застосувати найкращі практики протоколу Берклі. Зокрема, у ньому є формулювання щодо особливостей збирання інформації (пар. 153-156).

У аналізованій постанові ККС ВС доволі детально розписав, що дотримано положення ст. 237 КПК України, а саме: «прокурор, а також, на виконання відповідних доручень, наданих у порядку ст. 40 КПК, оперуповноважений провели огляди інтернет-сторінок і телеграм-каналів, зробив-

ши скриншоти й завантаживши відеофайли, фотознімків, файлів з документами та «нормативно-правовими актами», які є додатками до протоколів огляду, оформлених відповідно до вимог КПК. Огляди зазначених інтернет-сайтів та телеграм-каналів проведено із дотриманням вимог ст. 237 КПК, зафіксовано (за допомогою функцій скриншоту, друку та запису на технічні носії інформації) зміст відображеної на інтернет-сайтах і в телеграм-каналах як електронних документах інформації, що підтверджує існування обставин, які підлягають доказуванню в цьому кримінальному провадженні» [8]. Слід визнати, що у постанові наведено належне обґрунтування саме допустимості фактичних даних з позицій порядку їх дотримання у кримінальному провадженні (безвідносно появи цих даних в мережі Інтернет).

Для порівняння, наведемо приклади проваджень, які розглядалися ККС ВС, де докази як результати OSINT визнано недопустимими саме через недотримання встановленого КПК України порядку їх збирання. Зокрема, прокурором військової прокуратури всупереч вимог ч. 5 ст. 280 КПК України у зупиненому кримінальному провадженні були проведені огляди інтернет сторінок та за їх результатами складені відповідні протоколи. У подальшому протокол огляду від 12.12.2016 інтернет-сторінки соціальної мережі «Вконтакте», протокол огляду від 12.12.2016 інтернет-сторінки соціальної мережі «Instagram» та від 16.12.2016 інтернет-сторінки соціальної мережі «Вконтакте» із додатками до них були предметом експертного дослідження і саме на інформацію, яка містилася у даних протоколах прокурор посилався як на підтвердження факту участі ОСОБА_1 у терористичній організації, а тому твердження прокурора про те, що огляд інтернет сторінок проводився виключно з метою встановлення місця знаходження розшукуваного підозрюваного, є необґрунтованими. Тому колегією суддів апеляційного суду правильно визнані твердження захисника про недопустимість як доказів протоколів огляду інтернет сторінок від 12.12.2016 («Вконтакте» та «Instagram»), 16.12.2016 («Вконтакте») через порушення встановленого кримінально-процесуальним законом порядку їх отримання [9].

У іншому провадженні ВС не погодився з висновками судів першої та апеляційної інстанцій з приводу допустимості протоколу огляду Telegram каналу «МВД ЛНР» від 26 лютого 2023 року, складеному прокурором після звернення з обвинувальним актом до суду, тобто поза межами строку досудового розслідування. Під час судового засідання 20 лютого 2023 року свідок ОСОБА_13 повідомив, що «бачив у мережі Інтернет, як ОСОБА_7 приймала присягу. На Telegram каналі опубліковано відео, як остання в червні приймає присягу для проходження служби в правоохоронних органах ЛНР та ДНР. Публікація даної присяги в телеграм каналі була на початку липня та стосувалася населеного пункту с. Мілове і ще декількох районів». Як повідомив прокурор під час наступного судового засідання, яке відбулося 28 березня 2023 року, з метою перевірки показань свідка ОСОБА_13 ним був проведений огляд Telegram каналу «МВД ЛНР». Заявлене клопотання прокурором про долучення протоколу цієї слідчої (розшукової) дії судом було задоволено, незважаючи на заперечення сторони захисту, а у подальшому результати огляду були покладені в основу обвинувального вироку. Натомість, матеріали провадження не містять клопотання (усного або письмового) прокурора про надання судом доручення на проведення цієї слідчої (розшукової) дії, як не містять матеріали провадження й ухвали суду про надання такого доручення. Колегія суддів вказала, що стороною обвинувачення під час судового розгляду слідчі (розшукові) дії з метою встановлення або перевірці обставин, які мають істотне значення для кримінального провадження можуть проводитися виключно за дорученням суду. З огляду на зазначене, колегія суддів дійшла висновку про недопустимість протоколу огляду від 26 лютого 2023 року та відеозапису, який міститься на диску, складеного прокурором за власної ініціативи під час судового розгляду без відповідного доручення на це суду [10].

Отже, у разі заявлення клопотання саме про недопустимість результатів OSINT, зокрема, протоколів оглядів, важливо аргументувати, що був недотриманий порядок або проведення та фіксування огляду, або інші правила збирання доказів (в межах строку досудового розслідування, збирання не у період зупинення досудового розслідування, належний суб'єкт тощо).

Питання належності фактичних даних. Обставини, які що стосуються ідентифікації особи, яка могла бути причетна до вчинення кримінального правопорушення, без сумніву, відносяться до предмету доказування, бо зазначені у п. 2 ч. 1 ст. 91 КПК України. Належними є докази, які прямо чи непрямо підтверджують існування чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження, а також достовірність чи недостовірність, можливість чи неможливість використання

інших доказів (ст. 85 КПК України). Більш спрощено під належністю слід розуміти здатність доказів своїм змістом бути засобом встановлення обставин, які мають значення для кримінального провадження [11, с. 363].

З вироку видно, що зазначено саме зміст тих даних, які були опубліковані на телеграм каналі, та стосуються «т. зв. «декан факультету філології та масових комунікацій» т.зв. «Маріупольського державного університету»» [12], «діяльності» на «посаді», «нагороди» за «роботу». Ці фактичні дані пов'язані з обставинами, які входять до предмету доказування при кваліфікації діяння за ч. 3 ст. 111-1 КК України.

При цьому складно погодитись, що дотримання вимог КПК України здатне підтвердити існування обставин, які підлягають доказуванню в кримінальному провадженні [8], адже дотримання вимог КПК України характеризує порядок збирання фактичних даних, але не його зміст (як зв'язок відомостей, які становлять його зміст доказу, із обставинами, що підлягають доказуванню [13]).

Питання достовірності фактичних даних. В силу специфіки джерел отримання інформації, форм її існування, можливості зміни / зникнення, механізмів фіксування задля використання у доказуванні у дослідженнях також наголошується на автентичності, достовірності та цілісності такої інформації [14, с. 125]; надійності конкретного джерела, інших характеристиках, що впливають на достовірність таких доказів, з урахуванням рекомендацій Протоколу Берклі [15, с. 994]; цілісності та автентичності електронних доказів [16, с. 224].

У пар. 149 Протоколу Берклі (у перекладі українською мовою) йдеться про «достовірність», утім, термін reliability точніше перекладається як «надійність». Отже, слідчі, які працюють з відкритими джерелами, повинні визначити, чи є інформація або твердження в цифровому контенті на перший погляд надійними, шляхом перегляду та оцінки контенту, а також контекстуальної інформації, що міститься у файлі. Це може включати перевірку вбудованих метаданих, пов'язаної інформації та джерела. Цей процес повинен включати спробу ідентифікувати оригінальне джерело матеріалу, що може вимагати відстеження походження даних в Інтернеті, особи, яка завантажила їх, або автора.

Зважаючи на те, що в українському законодавстві немає такої окремої властивості доказів, як надійність, що проявляється у правдоподібності, точності та аутентичності, то, виходячи з розуміння reliability у протоколі Берклі, у кримінальному провадженні України вона має досліджуватися у контексті достовірності. Достовірність не визначена у КПК України, утім, одне з доктринальних визначень пов'язує її з властивістю, яка відображає встановлену суб'єктом доказування за результатами їх перевірки та оцінки безсумнівність змісту доказів і засновану на цьому придатність використовуватися для встановлення обставин, що входять у предмет доказування [17, с. 175]. Як вважають А. Гутник та А. Хитра, оцінка електронного документа на достовірність здійснюється шляхом його зіставлення з іншими доказами, які в подальшому будуть зібрані у кримінальному провадженні, або уже наявні у ньому; перевірки технічного пристрою, за допомогою якого створювався електронний документ, на відсутність пошкоджень; перевірки програмного забезпечення та інших налаштувань; проведенням експертизи тощо [18, с. 100]. Якщо виходити з протоколу Берклі, використання якого у кримінальному провадженні прописано у листі-орієнтуванні Офісу Генерального прокурора від 28.08.2021 № 18/1-386 «Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел», то перевірка – це процес встановлення точності або правдивості інформації, яка була зібрана в Інтернеті (пар. 176).

З урахуванням цих позицій проаналізуємо доводи та контрдоводи, викладені у Постанові ККС ВС та вироку. Зокрема, довід про відсутність портретної експертизи, яка надала б можливість впевнитися у тому що особа, яка була зображена на фото і відео та обвинувачена ОСОБА_3 одна й та ж особа, було спростовано через:

- позицію, що проведення портретної експертизи є необхідним, коли орган досудового розслідування або суд не мають можливості іншим шляхом встановити особу, що зображена та фотознімках та/або відеозаписах;
- наявність протоколів пред'явлення для впізнання;
- наявність протоколів огляду, згідно з якими свідки впізнали на відеозаписі та фото з Telegram каналу особу ОСОБА_3;
- дослідженням публікацій з фото/відеоматеріалами, які досліджувалися в ході оглядів, у судовому засіданні, та встановленням їх відповідності змісту протоколів оглядів;

- сторона захисту не була позбавлена можливості заявити під час проведення як досудового розслідування, так і в суді клопотання про призначення судово-портретної експертизи, однак таким правом захисник не скористався [12].

З доводів та контрдоводів видно, що оспорювалася достовірність тих даних, за допомогою яких ідентифіковано особу обвинуваченого, а також їх достатність для безпомилкової ідентифікації.

Довід про визнання недопустимими і неналежними доказами результатів оглядів інтернет-сайтів та телеграм-каналів спростовано у тому числі контрдоводом, що сторона захисту не дала жодних відомостей щодо спростування цієї інформації і не аргументувала, що інформація, надана органом досудового розслідування, не відповідає дійсності, зокрема, містить ознаки фальсифікації та/або навмисного спотворення даних [8]. З формулювання «не відповідає дійсності» очевидно, що мова не йде ні про належність, ні про допустимість, а суто про достовірність. При цьому доволі сумнівним є формулювання щодо неспростування стороною захисту достовірності фактичних даних (що не є обов'язком сторони захисту) при тому, що сторона захисту вказувала на те, що «не встановлено офіційного існування інтернет-ресурсів, їх власників та користувачів, а також відповідальних осіб за розміщення інформації на них і за її перевірку» [8]. Отже, більшість доводів та контрдоводів стосувалася саме достовірності доказів, хоча ставилося питання про неналежність та недопустимість. Утім, ККС ВС вказував і на те, що «сторона захисту хоча й ставила питання про недостовірність таких доказів, однак не заявляла будь-яких клопотань про залучення спеціалістів чи експертів, проведення експертизи, а тому колегія суддів погоджується з висновками, зробленими місцевим судом» [8], що є більш доречним аргументом за цих обставин. О. Калінніков пише, що з огляду на тенденції у практиці ВС сторона захисту може ставити питання щодо недостовірності електронних (цифрових) доказів, що в деяких випадках може бути навіть більш ефективним, чим визнання доказів недопустимими. У випадку не вжиття стороною обвинувачення будь-яких дій щодо забезпечення підтвердження достовірності їх походження та цілісності неможливо підтвердити відсутність несанкціонованих дій щодо електронних (цифрових) доказі, в тому числі, неможливо підтвердити те, що не змінювався їх зміст. А тому такі докази є недостовірними, і на підставі таких доказів неможливо встановити дійсні обставини справи [19].

Для порівняння, у іншому кримінальному провадженні вже ставилося питання саме щодо недостовірності доказів: колегія суддів уважає непереконливими аргументи захисника про недостовірність даних, отриманих з відкритих джерел засобів масової інформації через перегляд сторінок мережі Інтернет, посилання на які детально наведені у відповідному протоколі огляду від 06 червня 2022 року, у зв`язку з таким. … З метою з`ясування обставин, які підлягають доказуванню, старший слідчий в особливо важливих справах слідчого відділу УСБУ в Херсонській області за участю спеціалістів відділу КІБ УСБУ в Херсонській області, провів огляд публікацій в засобах масової інформації через мережу Інтернет і задля збереження доступності інформації у відкритих джерелах, здійснив її цифрове зберігання – архівацію, яка надає змогу захистити та зберігати інформацію з плином часу, включаючи її справжність, доступність, ідентичність, постійність, рендеринг (візуалізацію) та зрозумілість, що корелюється зі стандартами, викладеними у Протоколах Берклі, визнаних Управлінням ООН. Крім цього, інформація зафіксована у згаданих протоколах огляду з відкритих джерел не суперечить іншим зібраним доказам, протоколи складені уповноваженою особою відповідно до вимог КПК України, а тому підстав для визнання зафіксованих у ньому даних недопустимими або неналежними Верховний Суд не вбачає. Крім цього, сторона захисту не дала жодних відомостей щодо спростування цієї інформації і не навела аргументів, які б вказували на те, що інформація, надана органом досудового розслідування, не відповідає дійсності, зокрема, що вона містить ознаки фальсифікації та/або навмисного спотворення даних» [20]. І у цьому випадку слід зазначити, що спростування достовірності доказів не є обов'язком сторони захисту.

У ще одній ситуації ККС ВС зазначив, що, перевіривши твердження захисту про неможливість використання даних із сайту «Миротворець» та соціальних мереж, суд зазначив наступне. Так, дані сайту «Миротворець», соціальних мереж «Вконтакте» та «Одноклассники», розміщені в публічному доступі мережі Інтернет та зафіксовані протоколом огляду від 18 серпня 2022 року щодо встановлення особи ОСОБА_8. Огляд зазначених інтернет-сайтів здійснено слідчим з дотриманням вимог ст. 237 КПК. Водночас, за наявною інформацією сайту «Миротворець», є «ОСОБА_8» ІНФОРМАЦІЯ_4, країна походження – РФ, адреса – АДРЕСА_5, тел. НОМЕР_7, НОМЕР_3. Вка-

зано, що ОСОБА_8, є співробітником головного розвідувального управління Генерального штабу РФ, проходив службу в т. зв. «Республіканській гвардії ДНР» [21]. Формулювання «неможливість використання даних» не дає можливості ідентифікувати, про які властивості доказів йде мова. Відмітимо, що у доктрині дається оцінка проблем використання інформації з сайту «Миротворець» [22].

При оцінці таких підходів практики слід врахувати ще один важливий аспект. Протокол Берклі вказує на потребу перевірки доказів, про що вже зазначалося вище. Адже існує багато причин, через які контент може бути ненадійним. Наприклад, контент може бути неправильно атрибутований або вирваний з контексту, як у випадку з відео, яке нібито зображувало турецькі атаки на півночі Сирії в 2019 році. Після поширення в основних новинах зрештою з'ясувалося, що це були кадри зі стрільбища в Кентуккі, США. Також можлива інсценізація контенту та його помилкова атрибуція реальним подіям. Відомим прикладом цього є справа «сирійського хлопчика-героя» у 2014 році. Пізніше було доведено, що відео, яке нібито зображувало хлопчика, який рятує дівчинку від обстрілу під час сирійського конфлікту, було інсценовано та знято на кіностудії на Мальті. Контент також може бути сфальсифікований або створений за допомогою штучного інтелекту (ШІ). Приклад цього з'явився у 2022 році в контексті війни в Україні. Метадані контенту, тобто «дані про дані», можуть вказувати на те, як, коли і ким був зібраний, створений, відкритий, змінений або відформатований цифровий файл. Метадані можуть допомогти виявити, чи є зображення фейком, або чи не збігаються час, дата чи місце зйомки з відповідною подією. Однак метадані також можуть бути підроблені або видалені, тому їх завжди слід розглядати як частину загального аналізу контенту [23]. Перевірка поділяється на три окремі елементи: джерело, цифровий об'єкт або файл та вміст, які слід розглядати сукупно та порівнювати на предмет узгодженості (пар. 176). Параграфи 176–194 протоколу Берклі містять доволі деталізовані підходи щодо такої перевірки, які доречно використовувати, щоб встановити надійність результатів OSINT, що безпосередньо стосується оцінки їх достовірності за ст. 194 КПК України. Для цих цілей лаконічність формулювання на кшталт «Огляди зазначених інтернет-сайтів та телеграм-каналів проведено із дотриманням вимог ст. 237 КПК, зафіксовано (за допомогою функцій скриншоту, друку та запису на технічні носії інформації) зміст відображеної на інтернет-сайтах і в телеграм-каналах як електронних документах інформації» [8] видається невиправданою.

У доктрині є пропозиція щодо нового джерела доказів – OSINT-звіт, під яким пропонується розуміти аналітичний документ, сформований фахівцями у сфері відкритих джерел інформації, що містить узагальнені фактичні дані, отримані у законний спосіб із загальнодоступних цифрових ресурсів, із обов'язковою фіксацією джерел, часу доступу, цифрових ідентифікаторів, технічних умов збору та ін. [24, с. 28] Зокрема, пропонується доповнити главу 4 КПК України параграфом 6 «OSINT-звіт», у якому має бути визначено поняття такого джерела доказів та процесуальні вимоги до нього. При цьому такий звіт може подаватися, як стороною обвинувачення, так і стороною захисту, що підвищує гарантії змагальності та рівності сторін у поданні суду доказів [24, с. 170-171]. Відмітимо, що посилання на схожий документ є в ухвалі:

«-довідкою за результатами OSINT-дослідження до № 4/1/1-15856 від 19.12.2024 …;

-довідкою за результатами OSINT-дослідження до № 4/1/1-15543 від 12.12.2024 …» [25].

Слушно пише О. Торбас, що очевидна проблема в даному випадку полягає в тому, що чинне кримінальне процесуальне законодавство не містить такого окремного процесуального документу як довідки, а тому не зовсім зрозуміло, чи було в даному випадку докази отримано в порядку, передбаченому КПК України, та, відповідно, чи можуть такі докази визнаватися допустимими. В межах даної доповіді дуже складно оцінити правову природу такої довідки, проте можна зробити припущення, що протокол огляду веб сайту та довідка за результатами OSINT дослідження вказують на різні ступені залучення інформації з відкритих джерел. Протокол огляду доцільно складати тоді, коли необхідно зафіксувати інформацію з одного конкретного джерела. Довідку ж доцільно складати тоді, коли доказове значення має не окреме джерело інформації, а ціла сукупність джерел. Крім того в такого роду довідках також можна пояснювати специфіку збору, оцінки, аналізу та фіксації такої інформації, що також може мати значення для кримінального провадження. Очевидною проблемою є те, що, як було зазначено вище, кримінальний процесуальний статус таких довідок не визначений чинним законодавством, що ускладнює їх застосування на практиці [26, с. 219].

Розглядаючи питання доречності та новизни запропонованого джерела доказів - OSINT-звіт, відмітимо, що пропоноване визначення свідчить про компіляцію фактичних даних. Утім, резуль-

тати OSINT мають бути зібрані та зафіксовані таким чином, щоб можна було перевірити джерело, цифровий об'єкт або файл та вміст, які слід розглядати сукупно та порівнювати на предмет узгодженості (пар. 176 протоколу Берклі). Тому якщо OSINT-звіт таких достатніх даних не міститиме, то він не може претендувати на те, щоб вважатися джерелом доказів. Якщо ж мова йде про аналітичну оцінку результатів OSINT, які містяться у інших джерелах, то доказами будуть ті фактичні дані, які містяться у джерелах, на основі яких сформовано цей звіт, що знову ж виключає можливість його тлумачення як джерела доказів. Чинне кримінальне процесуальне законодавство не забороняє робити будь-які аналітичні матеріали на основі OSINT, але доказове значення матимуть ті фактичні дані, які зафіксовані згідно з КПК України та з дотримання рекомендацій протоколу Берклі, викладені у протоколі огляду згідно ст. 237 КПК України.

Висновки. Отже, джерелом доказів при використанні результатів OSINT, зафіксованих у протоколі за ст. 237 КПК України з додатками, є саме протокол як різновид документу. Відповідно, питання допустимості можуть стосуватися виключно аспектів проведення та фіксування огляду, дотримання вимог КПК України щодо належного суб'єкта, строків досудового розслідування та інших питань порядку збирання та фіксування даних, які містяться у протоколі. Якщо ж є сумніви стосовно змісту первинних зафіксованих даних, їх походження у відкритих джерелах (автора контенту, особи, яка його розмістила і мету такого розміщення), створення їх ШІ, створення та поширення їх з метою дезінформації, правильності їх технічного збирання, незмінності онлайн-контенту будь-якого виду, метаданих, хеш-значеннях – мова може йти про недостовірність доказів. У цій ситуації ініціація визнання таких фактичних даних недопустимими доказами позбавлена сенсу. Результати OSINT можуть містити фактичні дані, що не мають властивість належності, але це ніяк не пов'язано з аналізом джерела походження – відкритих даних, адже встановлюється зв'язок (чи його відсутність) з усіма обставинами предмета доказування. Відповідно, ініціація визнання доказів неналежними через сумніви стосовно змісту первинних зафіксованих даних, їх походження у відкритих джерелах (автора контенту, особи, яка його розмістила і мету такого розміщення) також позбавлене сенсу.

У судових рішеннях результати OSINT мають бути відображені таким чином, щоб неупередженому спостерігачу було зрозуміло, чому суд вважає їх достовірними. Основою цього є правильне фіксування з дотриманням рекомендацій протоколу Берклі у досудовому розслідуванні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Berkeley Protocol on Digital Open Source Investigations A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf.
2. Leiden Guidelines on the Use of Digitally Derived Evidence. URL: https://leiden-guidelines.netlify.app/guidelines.
3. The Hala Protocol for the Collection, Processing, and Transfer of Audio Data. URL: https://protocol.halasystems.com.
4. Рекомендації для громадських організацій. Документування міжнародних злочинів і порушень прав людини для притягнення до кримінальної відповідальності осіб, що їх вчинили. URL: https://www.icc-cpi.int/sites/default/files/2023-06/2022.3769_UK_V1.pdf.
5. Оцінка цифрових знімків з відкритих джерел: Посібник для суддів і дослідників фактів. URL: https://www.trueproject.co.uk/_files/ugd/55728f_c247e350c0de42e6ad5c39fbf9d5104a.pdf.
6. Пашковський М.І. 3.1. Цифрова інформація з відкритих джерел. Відкриті цифрові дані у кримінальному провадженні. *Концептуальні основи цифровізації кримінального провадження України : монографія* / ред. Н.В. Глинська. Харків, 2024. 452 с. DOI: https://doi.org/10.31359/9786178612139. С. 233–274.
7. Пашковський М.І. Особливості використання OSINT при документуванні та розслідуванні колаборційної діяльності. *Актуальні питання кримінально-правової кваліфікації, документування та розслідування колабораціонізму: матеріали Всеукраїнської науково-практичної конференції, м. Одеса, 21 липня 2022 р*. Одеса: ОДУВС, 2022. С. 82–86.
8. Постанова ККС ВС від 21 липня 2025 року, справа № 201/11849/23. URL: https://reyestr.court.gov.ua/Review/129086893.

9. Постанова ККС ВС від 29 вересня 2022 року, справа № 552/3764/19. URL: https://reyestr.court.gov.ua/Review/106621769.
10. Постанова ККС ВС від 15 травня 2025 року, справа № 607/12421/22. URL: https://reyestr.court.gov.ua/Review/127537719.
11. Вапнярчук В.В. Загальна характеристика властивостей доказів та їх розмежування між собою. *Держава і право. Серія: Юридичні науки. 2015. Вип. 68*. С. 361–375. URL: https://dspace.nlu.edu.ua/bitstream/123456789/13433/1/Vapnyarchuk_361-375.pdf.
12. Вирок від 06 вересня 2024 року, Жовтневий районний суд м. Дніпропетровська, справа № 201/11849/23. URL: https://reyestr.court.gov.ua/Review/121525495.
13. Стоянов М. М. Властивості доказів у кримінальному процесі України: автореф. дис. ... канд. юрид. наук: 12.00.09. Одеса, 2010. 20 с. URL: https://dspace.nlu.edu.ua/bitstream/123456789/17810/1/Stoyanov_2010.pdf.
14. Смаль І.А. Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю (081 – Право). – Пенітенціарна академія України, 2025. 329 с.
15. Пашковський М.І. Обставини, що мають значення для кримінального провадження, та належність цифрових доказів з відкритих джерел. *Наукові перспективи*. 2024. № 10(52). С. 984–998. DOI: 10.52058/2708-7530-2024-10(52)-984-998.
16. Каланча І.Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy*. 2025. № 8(51) С. 206–230. DOI: 10.52058/2695-1592-2025-8(51)-206-230.
17. Тепак С.Я. Достовірність доказів у кримінальному провадженні. Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 Право. Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія». Київ, 2024. 238 с.
18. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: колективна монографія / А.В. Гутник, А.Я. Хитра. Львів: ЛьвДУВС, 2022. 204 с.
19. Калінніков О. Доведення недостовірності електронних доказів як ефективний засіб захисту в кримінальному провадження. URL: https://zib.com.ua/ua/162678.html.
20. Постанова ККС ВС від 30 січня 2025 року, справа № 490/6113/22. URL: https://reyestr.court.gov.ua/Review/125028785.
21. Постанова ККС ВС від 12 листопада 2024 року, справа № 199/6828/22. URL: https://reyestr.court.gov.ua/Review/123015852.
22. Басиста І.В. Гутник А.В. Використання інформації з бази даних Центру «Миротворець» у перебігу досудового розслідування: окремі аспекти. *Держава і суспільство: сучасні виклики та пошук рішень: Збірник матеріалів III Всеукраїнської науково-теоретичної конференції, 16 травня 2024 р., Київ*. К.: КТГГ, 2024. С. 395–398. URL: https://www.researchgate.net/publication/381153839.
23. Open-source imagery is transforming investigations of international crimes – but how do judges know if it's real? URL: https://theconversation.com/open-source-imagery-is-transforming-investigations-of-international-crimes-but-how-do-judges-know-if-its-real-236362.
24. Нікішев О.В. Особливості доказування у кримінальних провадженнях в умовах надзвичайних правових режимів. Дисертація на здобуття ступеня вищої освіти доктора філософії за спеціальністю 081 – Право. Одеський державний університет внутрішніх справ, Одеса, 2025. 268 с.
25. Ухвала Слідчого судді Шевченківського районного суду м. Києва від 21 березня 2025 року, справа № 761/10611/25. URL: https://reyestr.court.gov.ua/Review/126035663.
26. Торбас О. Особливості використання osint у кримінальному процесуальному доказуванні. *Роль OSINT-досліджень у підвищенні рівня національної безпеки України: матеріали круглого столу (м. Львів, 7 травня 2025 р.) / укладач І.О. Ревак. Львів: ЛьвДУВС*, 2025. 249 с. С. 217–220. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/ 8875/1/07_05_2025.pdf.