КРИМІНАЛЬНЕ ПРАВО, КРИМІНОЛОГІЯ, КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО. КРИМІНАЛЬНИЙ ПРОЦЕС, КРИМІНАЛІСТИКА ТА СУДОВА ЕКСПЕРТИЗА

УДК 343.13+378.147
DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243

ВИКОРИСТАННЯ ЦИФРОВИХ ДАНИХ З ВІДКРИТИХ ДЖЕРЕЛ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ: ОКРЕМІ АСПЕКТИ

Басиста Ірина Володимирівна,
докторка юридичних наук, професорка
професорка кафедри кримінального процесу та криміналістики Львівського державного університету внутрішніх справ,
вул. Городоцька, 26, м. Львів, Україна, 79007
e-mail: basysta-i@ukr.net,
ORCID: https://orcid.org/0000-0001-9707-7386

Гаврилюк Людмила Володимирівна,
кандидат юридичних наук, старший дослідник, начальник 3-го науково-дослідного відділу науково-дослідної лабораторії проблем правового та організаційного забезпечення діяльності Міністерства
Державного науково-дослідного інституту МВС України,
провулок Євгена Гуцала, 4а, м. Київ, Україна, 01011
e-mail: Lvg4323@ukr.net
ORCID: https://orcid.org/0000-0002-9441-4073

Гутник Аліна Володимирівна,
докторка філософії у галузі права
доцентка кафедри кримінального процесу та криміналістики Львівського державного університету внутрішніх справ,
вул. Городоцька, 26, м. Львів, Україна, 79007
e-mail: hutnyk_alina@ukr.net
ORCID: https://orcid.org/0000-0002-5447-7256

Хитра Андрій Ярославович,
кандидат юридичних наук, доцент,
завідуючий кафедрою кримінального процесу та криміналістики Львівського державного університету внутрішніх справ,
вул. Городоцька, 26, м. Львів, Україна, 79007
e-mail: andrkh78@gmail.com
ORCID: https://orcid.org/0000-0002-7125-1953

***Мета** статті полягає у є дослідженні можливостей використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень. **Методика.** Проведено аналіз національного*

законодавства, національної судової практики, протоколу Берклі з ведення розслідування з використанням відкритих цифрових даних (далі –Протокол Берклі), практики ЄСПЛ, МКС та наукових досліджень на основі яких, за допомогою синтезу, виокремлено основі проблеми. Використано індукцію та дедукцію при формуванні власних авторських висновків. ***Методи****. У процесі проведення наукового пошуку використано порівняльно-правовий, функціональний, системно-структурний, графічний методи.* ***Результати.*** *У роботі підтримано наукові погляди, суть яких зводиться до необхідність використання терміну «цифрові дані» для означення сприйнятої інформації у бінарному вигляді. Доведено, що слід відмежовувати «цифрову інформацію» від «цифрових доказів». Встановлено, що попри новизну розвідки за відкритими джерелами для національного законодавця, уже сформовані підходи щодо оцінки отриманої із відкритих джерел цифрової інформації, які знайшли своє відображення у Протоколі Берклі.* ***Наукова новизна.*** *Дослідження є одним із перших, де крізь призму аналізу положень Протоколу Берклі та вимог чинного КПК України до доказів та діяльності з їх збору, перевірки та оцінки, сформульовано авторський підхід щодо правил «роботи» з інформацією, яка наявна у відкритих джерелах та подальших можливостей її використання, у тому числі у доказуванні. Запропоновано авторське визначення «відкритих джерел» та аргументовано необхідності розробки концепції «цифрової інформації з відкритих джерел».* ***Практична значимість.*** *Результати дослідження можуть бути використані у перебігу досудового розслідування, коли виникає необхідність «роботи» з відкритими джерелами цифрової інформації.*

Ключові слова: *кримінальне провадження, досудове розслідування, доказування, докази, цифрові докази, електронні докази, відкриті джерела цифрової інформації, Протокол Берклі, OSINT, розвідка за відкритими джерелами, тяжкі міжнародні злочини.*

Iryna Basysta
Doctor of Legal Sciences, Professor, Professor at the Department of the Criminal Procedure and Criminology, Lviv State University of Internal Affairs
Member of the Academic Advisory Council under the Supreme Court,
26, Horodotska str, Lviv, Ukraine, 79007
e-mail: basysta-i@ukr.net

Liudmyla Havryliuk
Cand. Sci. (Law), Senior Researcher, Head of the 3rd Research Department of the Research Lab of the Problems of Legal and Organizational Support of Ministry's Activities,
State Research Institute MIA Ukraine
4a Ye. Gutsalo Lane, Kyiv, Ukraina, UA-01011
e-mail: Lvg4323@ukr.net

Alina Hutnyk
Ph. D. in Law, Associate Professor of Department of Criminal Procedure and Criminology
Lviv State University of Internal Affairs,
26, Horodotska str, Lviv7, Ukraine, 7900
e-mail: hutnyk_alina@ukr.net

Andrew Khytra
PhD in Law, Associate Professor, Head of the Department of Criminal Procedure and Criminology
Lviv State University of Internal Affairs,
26, Horodotska str, Lviv, Ukraine, 79007
e-mail: andrkh78@gmail.com

USE OF DIGITAL DATA FROM OPEN SOURCES DURING THE INVESTIGATION OF CRIMINAL OFFENSES: CERTAIN ASPECTS

The purpose *of the article is to study the possibilities of using digital data from open sources during the investigation of criminal offenses****. Methodology.*** *An analysis of national legislation, national judicial practice, the Berkeley protocol for conducting an investigation using open digital data (hereinafter referred to as the Berkeley Protocol), the practice of the European Court of Human Rights, the International Criminal Court and scientific research, based on which, by means of a synthesis, the basis of the problem was identified. Induction and deduction were used to form authors' conclusions.* ***Methods.*** *Comparative-legal, functional, system-structural, graphic*

methods were used in the process of scientific research. ***The results.*** *The work supports scientific views, the essence of which is in the need to use the term "digital data" to denote perceived information in binary form. It has been proven that "digital information" should be distinguished from "digital evidence". It has been established that despite the novelty of open source intelligence for the national legislator, approaches to the assessment of digital information obtained from open sources have already been formed, which were reflected in the Berkeley Protocol.* ***Scientific novelty.*** *The research is one of the first, where, through the prism of the analysis of the provisions of the Berkeley Protocol and the requirements of the current Code of Criminal Procedure of Ukraine for evidence and activities related to their collection, verification and evaluation, the author's approach to the rules of "working" with information available in open sources and its further possibilities is formulated use, including in proof. The author's definition of "open sources" is proposed and the need to develop the concept of "digital information from open sources" is argued.* ***Practical significance.*** *The results of the research can be used in the course of a pre-trial investigation when there is a need to "work" with open sources of digital information.*

Key words: *criminal proceedings, pretrial investigation, evidence, proof, digital evidence, electronic evidence, open sources of digital information, Berkeley Protocol, OSINT, open source intelligence, serious international crimes.*

Постановка проблеми. Великий масив інформації зберігається у відкритому доступі в мережі Інтернет та є доступним для необмеженого кола користувачів. Будь-хто за допомогою лише смартфону може створити повідомлення, фото, аудіо чи відеозапис та поширити його у соціальних мережах, власних сайтах і таким чином поділитися власними думками, подіями. Але ця ж інформація може мати значення для кримінального провадження. Особливо, під час розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку, коли доступ до певних місць є ускладнений, а то і неможливий, однак, вкрай необхідний для документування вчинених тяжких міжнародних злочинів.

Здавалось би, такий «дистанційний» процес збору інформації є простішим, адже його можна реалізовувати безпосередньо з робочого місця, проте нами встановлена ціла низка труднощів, як от: у національному кримінальному процесуальному законодавстві відсутнє поняття «електронного» чи «цифрового» джерела доказу; у судових рішеннях превалює вживання терміну «електронний доказ» у розумінні електронного документу; мають місце помилкові підходи до збору такої інформації та її збереження; відсутні критеріїв для її оцінки. З початку повномасштабного вторгнення багато уваги привертає розвідка з відкритих джерел (OSINT), інструменти якої використовують для встановлення та пошуку воєнних злочинців, збирання розвідувальної інформації. Проте, розвідка є діяльністю, яка належить до оперативно-розшукової роботи правоохоронних органів, військових підрозділів та не може використовуватися з метою доказування, що теж викликає нерозуміння на практиці. Разом із цим, є необхідність розпізнавати дезінформацію, маніпуляцію, яка навмисно створюється з політичною, військовою метою. Все це підтверджує, що використання інформації з відкритих джерел під час досудового розслідування є актуальним питанням, яке потребує детального дослідження.

Аналіз останніх досліджень та публікацій засвідчує, що такі науковці, як М. Гуцалюк, І. Каланча, Ю. Орлов, О. Сіренко, А. Скрипник, А. Столітній, Т. Фоміна, В. Хахановський, Д. Цехан, С. Чернявський та інші низку своїх наукових пошуків присвятили визначенню поняття, особливостей, місця цифрових доказів у кримінальному провадженні. Можливості збору та використання цифрової інформації з відкритих джерел досліджували такі вчені як Ю. Виходець, О. Манжай, Г. Тетерятник, О. Торбас, І.Федчак. Ґрунтовні рекомендації щодо обрання належного «процесуального інструментарію» пропонує нам А. Коваленко.

Незважаючи на суттєвий вклад цих науковців, без належних відповідей залишилися питання щодо співвіднесення положень Протоколу Берклі та вимог чинного КПК України до доказів та діяльності з їх збору, перевірки та оцінки. Слід узагальнити правила «роботи»

з інформацією, яка наявна у відкритих джерелах та подальші можливості її використання, у тому числі у доказуванні. Слід з'ясувати, що варто розуміти під «відкритими джерелами» тощо.

Постановка завдання. Ставиться завдання проведення аналізу та синтезу поглядів науковців і практиків, законодавчих положень, національної судової практики, а також рішень ЄСПЛ та МКС задля виокремлення наявних проблем у царині використання цифрових даних з відкритих джерел під час розслідування, у тому числі й злочинів проти миру, безпеки людства та міжнародного правопорядку. Також одним із завдань визначено формулювання пропозицій задля удосконалення такої діяльності.

Виклад основного матеріалу дослідження.

У чинному КПК України законодавець не виділяє такого різновиду доказів, як «електронні». При цьому, у ЦПК України йде мова про «електронні докази», «електронні документи та документообіг» [41] тощо, а його стаття 100 містить вказівку, що варто розуміти під таким різновидом доказів, порядок їх подання та засвідчення «електронних копій електронного доказу» [41]. Українські науковці також вживають термін «*електронні докази*» на позначення такого їх різновиду й за умов чинного КПК України [31; 32; 33; 25; 5]. Небезпідставно дотримуються й наукової позиції «щодо доцільності використання саме терміну «електронний (цифровий) доказ». Обґрунтовують це тим, що «електронний» вказує на вид пристрою, за допомогою якого був створений і збережений доказ, а «цифровий» – на тип запису інформації на відповідний пристрій. Але необхідно враховувати швидкоплинність технологічного прогресу, адже вже через певний проміжок часу можуть з'явитися як нові види пристроїв, так і нові типи запису інформації» [40, с. 209–210]. Судді Верховного Суду допускають вживання обох термінів [34], окремі представники Феміди оперують виключно поняттям «*цифрові докази*» [34], судові ж рішення різних інстанцій рясніють обома терміновживаннями, хоча, у переважній їх більшості, йдеться про *електронний доказ у розумінні електронного документу*. І хоча такий підхід не є вірним, все ж він логічне слідує із не досконалих положень чинного КПК України.

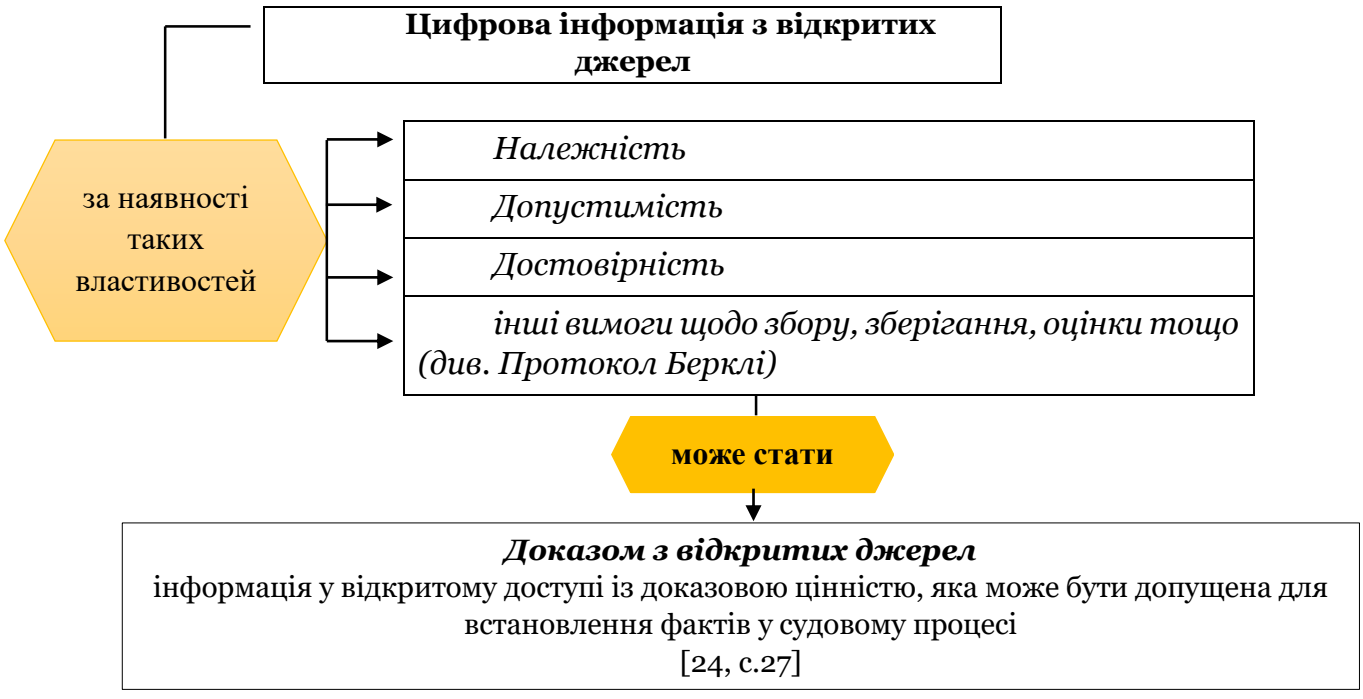
Радимо послуговуватися підходом виокремлення саме *цифрових доказів, цифрових відомостей, цифрової інформації, що отримані з відкритих джерел*. Такий терміновжиток є цілком прийнятним й за чинного КПК України та інших національних, діючих у цій сфері нормативно-правових актів, тощо (національного стандарту України «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження *цифрових доказів*» [6] (як бачимо йдеться про *цифрові докази)*; листа-орієнтування Офісу Генерального прокурора стосовно збереження *цифрової інформації* з відкритих джерел від 28 серпня 2021 року [23] тощо). Дороговказом також маємо український неофіційний переклад Протоколу Берклі з ведення розслідування з використанням відкритих *цифрових даних* [24].

Що варто вкладати у поняття «*електронні докази*» і чому радше слід оперувати такою категорією, як «*цифрова інформація*» та «*цифрові дані*»? Підкреслювалося, що через наявну семантичну наближеність термінів, для прикладу, у ДСТУ «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», який діє ще з 1.01.2019 «…*цифровий доказ* (digital evidence) визначається як *інформація* або *дані*, збережені або передані в бінарному вигляді, на які можна посилатися як на докази (п.3.5.)». «*Цифрова інформація*» існує у «*електронно-цифровому*» середовищі та не завжди набуде характеру, статусу і характеристик доказу у кримінальному провадженні. Вона характеризується *наявністю метаданих* (з англ. «дані

про дані») створюються разом із кожним файлом (1) автоматично програмою, або (2) автором цифрової інформації [25, с. 36; 30, с. 74–75, 94]. Не абсолютно-притаманною їй є ознака *позбавлення суб'єктивності* [30, с. 74–75, 94], адже авторство належить людині [1; 39]. Іншими ознаками виступають такі, як: *можливість існування у статичній та динамічній формах, закодованість* (через що є потреба у перетворенні в таку форму, яка може бути сприйнята людиною; *мобільність; тиражованість; «невловимий характер інформації» та легкість внесення змін або знищення*. Для відтворення *цифрової інформації* потрібні апаратні і програмні умови [30, с. 94–97].

На запитання про доцільність вживання терміну *електронний доказ,* то схильні дати ствердну нашу відповідь, але не у випадку із чинним національним правовим полем, у тому числі й за поширення дії положень КПК України. Отож, буде вірним вживати термін «*електронний доказ*», коли у чинному КПК України матиме закріплення уніфікований й адаптований до *електронної форми* порядок отримання, збереження або передання в бінарному вигляді відомостей про факти чи обставини (фактичні дані) [11, с. 417], на які можна посилатися як на докази, виходячи із притаманних їм властивостей належності, допустимості, достовірності.

Відмінності між цифровими доказами та цифровою інформацією, що отримана з відкритих джерел. На ці відмінності звернута увага у Протоколі Берклі. У його тексті підкреслено, що термін «докази» слід відрізняти від «інформації» [24, с. 27]. «Важливо не зловживати терміном «докази», посилаючись на інформацію взагалі, зокрема й з відкритих джерел. *Докази,* як правило визначаються як доказ факту (ів) який використовується під час розслідування і (або) подається на судовому слуханні» [24, с. 27]. «Цифрова інформація, що отримана з відкритих джерел (цифрова інформація у відкритому доступі) – інформація, що є у відкритому доступі в Інтернеті, до якої можна отримати доступ, наприклад, на загальнодоступних веб-сайтах, в Інтернет-базах даних або на платформах соціальних медіа» [24, с. 25, 27].



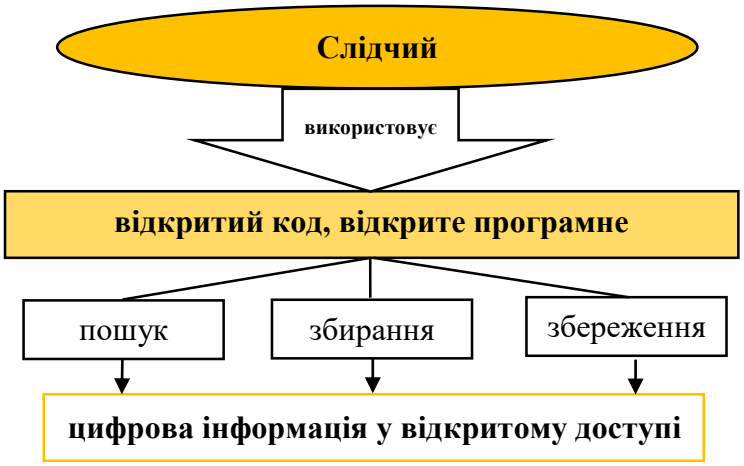
Якщо говоримо про *цифровий доказ* (digital evidence), то йдеться за *відомості про факти чи обставини (фактичні дані)* [11, с. 417], що отримані у передбаченому КПК України порядку, збережені або передані в бінарному вигляді, на які можна (бо вони відповідають таким властивостям, як належність, допустимість, достовірність) посилатися як на докази.

Ознаки цифрової інформації, які проявляються у доказуванні.

Наявні усталені обґрунтовані переконання, що *ознаками цифрової інформації, які проявляються у доказуванні є: комплексність доказу* (А.В. Скрипник резюмує, що окремі автори пропонують до структури цифрового доказу включати, як матеріальний носій, так і процесуальний документ (протокол огляду) із його описом та описом інформації (змісту, її реквізитів тощо) із нього, а також відповідну постанову про визнання означеної інформації доказом та долучення до справи [30, с. 99]. При цьому вже згаданий автор та інші знані українські дослідники цілком виправдано критикують такий підхід через неможливість віднесення процесуальних документів до елементів доказу, при цьому не заперечуючи існування вже згаданої ознаки [30, с. 99]); *специфічність порядку збирання* (є потреба використовувати програмні засоби, які унеможливлюють внесення змін до файлів на машинних носіях; необхідна компетентність слідчого, спеціаліста, понятих)*, перевірки та оцінки* (є спеціальні підстави такої оцінки (психологічні, гносеологічні та юридичні)). Його *джерелом є апаратні і програмні засоби.* З'ясування *належності* цифрових доказів є можливим лише під час відтворення інформації з використанням технічних засобів та комплексного аналізу її змісту і реквізитів; додатковими критеріями достовірності цифрових доказів є автентифікованість, ідентифікованість, верифікованість, незмінність і відтворюваність [30, с. 100–101].

Назріла розробка концепції цифрової інформації з відкритих джерел. Не можемо погодитися із тим, що у чинному КПК України є достатньо унормованим питання щодо отримання *цифрової інформації з відкритих джерел*, як і перевірки та оцінки таких вже *цифрових відомостей,* бо для цього замало наявних кримінальних процесуальних положень, на підставі яких ми лише можемо віднести такі джерела доказів до документів (зокрема електронного, бо саме такий шлях обрала слідча та наявна судова практика, про що розлогіше мова йтиме згодом) чи речових доказів (CD диск тощо). Це не вірно, і не достатньо, та й загалом ускладнює належний процесуальний збір *цифрової інформації.* Національному законодавцю радше варто слідувати досвіду Латвії, де виділено таке окреме джерело доказів.

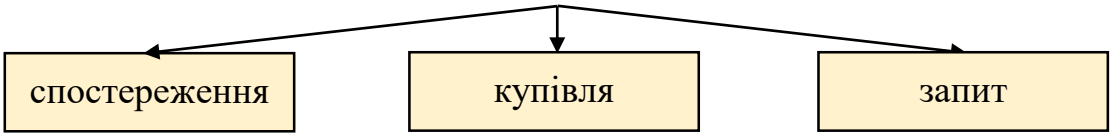
Також маємо проблему із різним розумінням «*відкритих джерел*» та їх переліком. Частково така прогалина усувається тим застосованим підходом, який має місце у Протоколі Берклі. Так, у ньому зазначено про *відкритий код, відкрите програмне забезпечення,* як дозволені «інструменти» для пошуку, збирання, збереження *цифрової інформації у відкритому доступі* [24, с. 25, 27].



Відкритий код, відкрите програмне забезпечення – побудоване з вихідного коду, який кожен, хто має доступ, може перевірити, змінити чи покращити. Код не бачать користувачі, але він підпадає під вказані маніпуляції програмістом. На відкрите програмне забезпечення не поширюються авторські права, патенти чи інші юридичні засоби контролю [24, с. 25, 27].

На підставі нашої науково-практичної розвідки, пропонуємо такий авторський підхід. *Відкриті джерела цифрової інформації це* – медіа, соціальні медіа, веб-сайти, геопросторові платформи, бази даних, офіційні дані та інші платформи, на яких можна спостерігати, купувати, або запитувати загальнодоступну інформацію.

Способи отримання інформації у відкритому доступі [24, с. 25–26]



Розвідка за відкритими джерелами **не виконує** функції збору інформації, пов'язаної із процесами розслідування, встановлення елементів різних злочинів (Протокол Берклі) [24, с. 26].

Звісно, що розвідка за відкритими джерелами може бути застосовною для вирішення питання про вжиття заходів забезпечення безпеки (захисту свідків) та як довідкова інформація для прийняття рішень тощо.

Хоча автори й розглядають «розвідку», дещо спрощено, зокрема, як «інформацію, яку можна зрозуміти та яка була оцінена у контексті її джерела та надійності» [38, с. 7], наділяючи OSINT, на відміну від інших розвідок (як от HUMINT, SIGINT, IMINT або PHOTINT чи GEOINT, MASINT [38, с. 8–9] тощо), *придатністю використання її інструментарію для розслідування злочинів*, у тому числі й воєнних [38, с. 164–173], все ж маємо певні власні аргументи з огляду саме такого спрощеного і буквального авторського підходу.

Так, сучасна практика розслідувань використовує методику OSINT для відшукання прихованих активів, таких, що мали б бути обкладені санкціями тощо. Поділяємо й підхід про придатність інструментарію OSINT для виявлення порушень у різних сферах, про що автори детально зазначають [37; 38]. Є й протилежна мета використання – «…кіберзлочинці з публічних даних складають портрет потенційної жертви» [37].

У рішеннях суддів також згадується OSINT і методи іменуються, як «аналітичне дослідження», чи «пошук» («…було проведено аналітичне дослідження відкритих джерел інформації методами OSINT» див. ухвала слідчого судді Комунарського районного суду міста Запоріжжя від 1.06.2022 у справі № 333/1938/22. *https://reyestr.court.gov.ua/Review/104556752*; «…у зв'язку з чим, було здійснено пошук на основі відкритих джерел (OSINT)» див. ухвала слідчого судді Святошинського районного суду м. Києва від 31.07.2019. у справі № 759/13808/19. https://reyestr.court.gov.ua/Review/83480188 тощо). Автори теж аналізуються ці та інші рішення, але під дещо іншим, не критичним, кутом зору [38].

При всьому викладеному, маємо власне бачення щодо «режиму» здобутої інформації та способів і шляхів її використання у національних розслідуваннях, з огляду дотримання вимог до доказів та доказування, як і запобігання порушенням конституційних, процесуальних та конвенційних прав учасників кримінального провадження тощо. Детальніші рекомендації наведемо у наступних наукових розвідках.

Також слід звернути увагу на те, що цитата у Протоколі Берклі у котрій йдеться «…що розвідка за відкритими джерелами, є підмножиною тієї інформації, яка «збирається, використовується та розповсюджується своєчасно серед відповідної аудиторії з метою задоволення конкретних вимог до розвідки» [24, с. 26], судячи із шпальт наявного неофіційного перекладу Протоколу Берклі та його оригіналу [42] взята авторами Протоколу зі стор. 8. Директиви про розвідувальну спільноту №301, 11 липня 2006 р. [43], (про це значиться у приторінковій виносці №15 Протоколу. Також див. ориг. Протоколу – «15. National Open Source Enterprise, Intelligence Community Directive No. 301, 11 July 2006, p. 8 (footnote omitted)» [42]). Очевидним є, що вже наявні глобальні сформовані підходи щодо отриманої із відкритих джерел цифрової інформації, яка збирається, використовується та розповсюджується, відповідно, й правил поводження з нею. Також маємо й не однаковий у різні часові періоди підхід МКС, про який йтиметься згодом.

Вірна оцінка джерела, як відкритого, передбачає й задіяння належних процесуальних механізмів. Є чимало питань щодо перебігу отримання, інформативності та збереження інформації, отриманої з відкритих джерел, як і долучення до матеріалів провадження і цьому свідченням є наявні судові рішення [3; 4], є й такі кінцеві процесуальні рішення судів, які успішно «встояли» у касації [22]. Суди також мають процесуальний клопіт й із правовою оцінкою скріншотів, співвідношенням оригіналу доказу та його копії тощо [34; 35]. Науковці радять з належною долею відповідальності підійти до оцінки джерела на предмет його відкритості, чи ні. Лише на її підставі слід обирати «процесуальні способи і засоби роботи». Обрання невірних підходів у застосування процесуальних механізмів є наслідком помилкового сприйняття джерела, як відкритого.

Також обрання не вірного підходу до роботи із відкритим джерелом, здатне унеможливити подальше *безпосереднє дослідження* судом цього *цифрового доказу з відкритого джерела*, як і перевірку його достовірності через стирання (зміну, корегування) тощо інформації [10]. Про цю практичну проблему із належною *архівацією даних, які містяться у відкритих джерелах* вже вели мову як судді Верховного Суду, вказуючи, що

іноді засади безпосередності «…взагалі неможливо дотриматися, оскільки перехід за відповідним посиланням в інтернеті не дає результату або ж за таким посиланням розміщена вже інша інформація»[34], так і науковці [10].

Важливо, щоб національна криміналізація тяжких міжнародних злочинів та «правила» національних розслідувань відповідали міжнародному праву прав людини, міжнародному гуманітарному праву та міжнародному кримінальному праву. Маємо у наших розслідуваннях бути дотичними із ситуаціями та тими провадженнями, які вже здійснює МКС, Міжнародний Суд ООН, ЄСПЛ та суди в інших країнах, зокрема й за принципом *універсальної юрисдикції.* Також прогнозованим та обговорюваним є створення трибуналів, зокрема й щодо вчиненої російської агресії. У Протоколі Берклі підкреслюється, «…коли слідчі, що ведуть розслідування з використанням даних у відкритому доступі, не знають (авт. – об'єктивно) конкретного механізму чи юрисдикції, вони повинні прагнути збирати та зберігати інформацію таким чином, щоб максимально використовувати її у найширшому діапазоні потенційно релевантних юрисдикцій. Якщо слідчі знають про відповідні вимоги до місця де врешті-решт буде розглядатися справа, вони повинні адаптувати свої процеси до тих конкретних вимог» [24, с. 44].

Для глибшого розуміння триваючих процесів наведемо приклад від початку 2024 року, як от щодо висунення в США обвинувачення російським військовим щодо подій, які трапилися на території України [7], що, як цілком аргументовано стверджує автор, дозволяє міжнародне право, якщо вчинено злочин щодо громадян цієї держави, адже її інтерес щодо захисту власних громадян від протиправних посягань за кордоном є абсолютно легітимним та іменується *юрисдикцією за принципом пасивної правосуб'єктності* [7].

Наявна й проблема у дещо іншій площині, зокрема з тим, як вірно зазначають правозахисники, що до початку повномасштабного вторгнення, більшість злочинів, пов'язаних з порушенням міжнародного гуманітарного права, кваліфікувалися як загальні кримінальні правопорушення [29]. Виникає питання щодо різниці у «режимах» кваліфікації та розслідування.

Чому інформація у відкритому доступі є корисною при міжнародних розслідуваннях, у тому числі й у перебігу розслідувань тяжких міжнародних злочинів за національними правилами кваліфікації та розслідування?

Із аналізу положень Протоколу Берклі з ведення розслідування з використанням відкритих цифрових даних слідує, що: так як розслідування тяжких міжнародних злочинів пов'язані із багатьма правовими та політичними процесами, які й дозволяють їх проводити чи блокують провадження у певний період часу, а лише згодом наступає така нагода реалізації, то й логічно, що вони віддалені від самих подій кримінальних правопорушень у просторі та часі [24, с. 22].

Застосування міжнародного гуманітарного права та/або міжнародного кримінального права не звільняє держави від виконання своїх зобов'язань за міжнародним правом у сфері прав людини (пп. 42-47 Бротоколу Берклі) [24]**.**

Цифрові відомості у доказуванні: рішення ЄСПЛ, МКС та національних судів. **Практика ЄСПЛ.** Ще у перших числах червня 2022 року доповідаючи на одному із науково-практичних заходів щодо допустимості електронних доказів з відкритих джерел, міжнародний консультант Ради Європи, баррістер Джеремі Макбрайд[1] констатував, що «…Європейському суду ще не довелося розглядати Берклійський протокол ….а конкретне

[1] Jeremy McBride. Судова палата Монктону у Великій Британії.

посилання на концепцію матеріалу з відкритих джерел, як форми доказу майже не фігурує в розгляді справ у Європейському суді. Зокрема, такі докази – на відміну від доказів з електронних джерел у цілому – ще не обговорювалися окремо з погляду їхньої прийнятності. Однак у Європейському суді, безсумнівно, є справи, у яких Держави покладаються на соціальні мережі та системи обміну повідомленнями –які можуть надавати докази, що підпадають під категорію доказів із відкритих джерел, – коли намагаються виправдати дії, які, на думку заявників, порушують їхні права людини. Подібні твердження поки що не увінчалися успіхом, *але це пов'язано не з формою, а з їхнім змістом»* [12]. «У справі «Грузія проти Росії (II)» (Georgia v. Russia (II)) [ВП], заява № 38263/08 від 21 січня 2021 року [26], Європейський суд посилався на звіт «Супутникові зображення високої роздільної здатності та конфлікт у Південній Осетії», опублікований Американською асоціацією сприяння розвитку науки (AAAS), встановивши, що аналіз супутникових знімків у звіті являє собою об'єктивний доказ, що стосується питань, які мають бути визначені у цій справі, і, зокрема, причини пошкодження будинків у Грузії» [12].

Наявні підходи у рішеннях міжнародних кримінальних трибуналів та Міжнародного кримінального суду (МКС). Що стосується тих справ, які розглядалися у міжнародних кримінальних трибуналах та МКС, то радимо вдатися до аналізу другого тому «Options for justice a handbook for designing accountability mechanisms for grave crimes»/ «Вибір заради справедливості: посібник зі створення механізмів притягнення до відповідальності за найтяжчі злочини» [2, с. 13]. Сконцентрований у цьому посібнику матеріал здатен пролити світло на концептуальні підходи Суду. Констатуємо, що МКС у своїй практиці оцінював матеріали, отримані з відкритих джерел на предмет їх доказової сили та віднесеності до доказів.

О.О. Торбас аргументовано резюмує, що «надмірне використання прокурором таких відомостей в якості прямих доказів призвело до того, що судді, починаючи з 2013» [38, с. 176–177] і фактично до 2016 року, «почали обмежувати відповідну практику, зазначаючи, що відомості з відкритих джерел насамперед мають використовуватися як орієнтуюча інформація або разом з іншими доказами» [38, с. 176–177]. МКСу довелося й констувати, що «…звіти громадських організацій та статті в пресі можуть бути корисним для розуміння історичного контексту конфлікту, але вони, як правило, не можуть замінити той тип доказів, який необхідний для забезпечення стандарту доказування щодо відповідних обвинувачень» (Gbagbo and Blé Goudé Case. International Criminal Court : website. URL: https://www.icc-cpi.int/cdi/gbagbo-goude) [38, с. 177].

Поряд із формулюванням вельми точних та вірних, вже цитованих нами умовиводів, О.О. Торбас зазначає й наступний висновок, а саме: «…проте в подальшому Суд стикнувся з новим викликом, адже на заміну звітам з відкритих джерел почали приходити електронні докази з відкритих джерел» [38, с. 178]. Не можемо погодитися із наведеним авторським підходом, так як з відкритих джерел ми все ж отримуємо інформацію, а не докази, про що вже йшлося на шпальтах цієї публікації та наголошувалося на відмінностях між цифровими доказами та цифровою інформацією, що отримана з відкритих джерел.

«На цей час робота МКС акумулює у своїй практиці сучасні підходи до оцінки матеріалів, отриманих з відкритих джерел. Наприклад, у справах Prosecutor v. Mahmoud al-Werfalli [28] та Prosecutor v. Ahmad Al Faqi Al Mahdi [27] щодо ситуації в Малі оцінювалися відео нападів на релігійні об'єкти під час процесу. Справа щодо збиття літака рейсу МН-17 на Донбасі також базувалася, як на фото та відео з відкритого доступу, так і перехопленнях телефонних розмов» [8]. На даному етапі МКС перейшов на «новий виток роботи». «Так,

в 2023 році прокурор МКС оголосив про запуск розширеної платформи для надання доказів OTPLink (https://otplink.icc-cpi.int)» [38, с.175].

Оцінка ж національними суддями цифрових даних здійснювалася у сукупності з іншими доказами (справа №677/2040/16-к (провадження № 51-5738км19) [18]; справа №161/5306/16-к (провадження № 51-3498км19) [17]; справа №404/700/17 (провадження № 51-4451км19) [20]; справа №236/4268/18 (провадження № 51-3124км20) [19]; справа №751/6069/19 (провадження № 51-1704км20) [16]) [36]. Висновок про допустимість електронного документа як доказу [34] зроблено у Постанові об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20) [21]. Національна судова практика фактично ототожнює електронний документ та електронний доказ, що не є вірним.

У національних розслідуваннях необхідно керуватися: загальними вимогами до доказів, їх джерел, визначених у КПК України, постановою Об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20). Більш розлоге про *стандарти цифрових доказів з відкритих джерел* наведено у Протоколі Берклі.

Оцінка цифрових даних, отриманих із відкритих джерел. За існуючими вимогами КПК України *цифрові дані з відкритих джерел* повинні оцінюватися з точки зору *належності, допустимості* та *достовірності* і *лише у сукупності та взаємозв'язку з іншими доказами* та використовуватися як *непрямі докази у сукупності та взаємозв'язку з іншими даними*, які *прямо викривають* обвинуваченого у вчиненні інкримінованого йому злочину [15, пп. 123–125].

У перебігу оцінки отриманих з *відкритих джерел цифрових даних важливо* задатися питанням, а *чи не є такі відомості дезінформацією*. Сучасні технології дозволяють створювати deepfake неймовірної якості та «глибини».

Така дезінформація продукується з різною метою, зокрема й задля психологічного впливу, загострення діалогу, шахрайства, фінансових афер тощо. Головно те, що через поширення фейків є ймовірність й порушення приватності, що у кінцевому результаті негативно впливатиме на особисте життя та професійну сферу тих, про кого поширили такі фейки [13].

У випадку поверхневої оцінки отриманих з *відкритих джерел цифрових даних* є висока ймовірність залучення у процес доказування таких *недостовірних даних*. Один із перших випадків *кіберзлочину* із *використанням діпфейків* трапився у 2021 році [14]. У національних судових розглядах вже теж маємо ситуації із таким станом справ, коли прокурору доводилося відмовлятися від підтримання обвинувачення, а відповідно суду – закривати кримінальне провадження [9; 13].

Висновки. Для позначення інформації у бінарному вигляді радимо послуговуватися таким слововжитком, як «цифрова», а не «електронна». Слід відмежовувати «цифрову інформацію» від «цифрових доказів», до яких ставляться вимоги належності, допустимості, достовірності. Щодо цифрових доказів, у тому числі й отриманих з відкритих джерел, ці вимоги «поглиблено» Протоколом Берклі. Для прикладу, важливо перевіряти цифрову інформацію чи не є вона діпфейком, адже такі відомості не відповідають критеріям достовірності, та не можуть бути використані як доказ у кримінальному провадженні.

У чинному КПК України законодавець не виділяє такого різновиду доказів, як «електронні» чи «цифрові». Це зумовлює (1) проблему із різним слововжитком серед науковців та практиків та (2) віднесення таких доказів до документів (як джерела доказів),

що хоч і узгоджується з нормами КПК України, проте не «пропонує» уповноваженому суб'єкту, як правильно збирати, оцінювати та перевіряти цифрові відомості, у тому числі й отримані з відкритих джерел. Очевидно на часі є розробка концепції цифрової інформації з відкритих джерел задля забезпечення належного процесу доказування.

Розвідка за відкритими джерелами (OSINT) може бути застосовною для вирішення питання про вжиття заходів забезпечення безпеки (захисту свідків), як довідкова інформація для прийняття рішень, відшукання прихованих активів, які мали б бути обкладені санкціями тощо. Мета доказування нею переслідуватися не може, про що також зазначено у Протоколі Берклі. У цьому ж Протоколі передбачено інші три способи отримання інформації з відкритих джерел.

ЄСПЛ поки не досліджував матеріали з відкритих джерел з погляду їхньої прийнятності та не розглядав Протокол Берклі. Проте, уже є рішення («Грузія проти Росії (II)» (Georgia v. Russia (II)) [ВП], заява № 38263/08 від 21 січня 2021 року [26]), у якому ЄСПЛ врахував звіт із супутниковим зображенням як об'єктивний доказ [12]. Натомість, МКС у своїй практиці оцінював матеріали, отримані з відкритих джерел на предмет їх доказової сили та віднесеності до доказів. Підкреслено, що цифрові докази з відкритих джерел повинні оцінюватися у сукупності із іншими доказами та не можуть замінити той вид доказів, який передбачений стандартом доказування (Gbagbo and Blé Goudé Case. International Criminal Court : website. URL: https://www.icc-cpi.int/cdi/gbagbo-goude) [38, с. 177]. Національна судова практика на даний час схиляється до оцінки цифрових доказів з відкритих джерел, як *непрямих доказів, які слід розглядати у сукупності та взаємозв'язку з іншими даними*, які *прямо викривають* обвинуваченого у вчиненні інкримінованого йому злочину [15, пп. 123–125].

Список використаних джерел

1. Басиста І.В., Удовенко Ж.В., Кулинич М.-М.А. Огляд тенденцій щодо штучного інтелекту та його перспективність для процесуальних рішень у перебігу кримінального провадження. *Науковий вісник Ужгородського Національного Університету, Серія ПРАВО*. 2024. Випуск 80: частина 3. С. 19–38. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/81_part-3.pdf
2. Вибір заради справедливості: посібник зі створення механізмів притягнення до відповідальності за найтяжчі злочини. Том 2. / за пер. О. Бондаренко; заг. ред. Р. Мартиновський, Л.Мороз. Переклад та видання здійснене за підтримки Програми «Права людини і правосуддя» Міжнародного фонду «Відродження». 2018. 544 с. URL: https://www.irf.ua/wp-content/uploads/2020/06/tom_ii_web.pdf
3. Вирок Київського районного суду м. Харкова від 14.08.2023 у справі № 953/2635/23 (провадження 1-кп/953/807/23). URL: https://reyestr.court.gov.ua/Review/112892204
4. Вирок Хмельницького міськрайонного суду Хмельницької області від 03.10.2023 у справі № 686/3769/23 (провадження № 1-кп/686/745/23). URL: https://reyestr.court.gov.ua/Review/113906215
5. Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: колективна монографія. Львів: ЛьвДУВС, 2022. 204 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/4725
6. ДСТУ ISO/IEC 27037:2017. «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів». Вид. офіц. Київ : УкрНДНЦ, 2018. VI. 31 с.
7. Задоя К. Перше кримінальне провадження в США щодо воєнних злочинів, вчинених в Україні. 1.02.2024. *Глобальна ініціатива T4P (Трибунал для Путіна):* веб-сайт. URL: https://t4pua.org/2281
8. Збір інформації з відкритих джерел як майбутній засіб доказів у найважчих міжнародних злочинах. 7.12.2023. *Antiraid:* веб-сайт. URL: https://antiraid.com.ua/news/zbir-informatsii-z-vidkrytykh-dzherel-iak-majbutnij-zasib-dokaziv-u-najvazhchykh-mizhnarodnykh-zlochynakh/
9. Кейс: Суд закрив кримінальне провадження у відношенні трансжінки, яка обвинувачилась у розповсюдженні порнографічних зображень. 17.05.2023. *Сайт ГО «ПРОЖЕКТОР» : веб-сайт*. https://www.projector.org.ua/projects_ua/public_hrc_ua/cases_hrc_ua/case_marii-vinichenko_sud/

10. Коваленко А.В. Огляд комп'ютерних даних під час розслідування колабораційної діяльності: типові об'єкти та приклади з практики. *Війна в Україні: зроблені висновки та незасвоєні уроки :* збірник тез Міжнародної науково-практичної конференції (22–23 лютого 2024 року) / упор. У. О. Цмоць. Львів : Львівський державний університет внутрішніх справ, 2024. С. 413–417. (1084 с.)

11. Кримінальний процес України: Академічний курс: у 3 т. Т.1: Загальна частина / В.Т. Нор, Н.Р. Бобечко, М.В. Багрій та ін. за ред. акад. НАПрН України, д-ра юрид. наук, проф. В.Т. Нора та д-ра юрид. наук, проф. Н.Р. Бобечка. Львів: ЛНУ ім. Івана Франка, 2021. 912 с.

12. Макбрайд Д. Застосовні міжнародно-правові рамки та стандарти щодо доказів із відкритих та електронних джерел: Європейська конвенція з прав людини. *Council of Europe :* веб-сайт. URL: https://rm.coe.int/coe-ukraine-open-uk/1680a6e571

13. Матвєєв В. Проблеми та виклики, пов'язані зі збором електронних доказів. 27.07.2023. *Justtalk:* веб-сайт. URL: https://justtalk.com.ua/post/problemi-ta-vikliki-povyazani-zi-zborom-elektronnih-dokaziv

14. Мороз М. Як розпізнати діпфейк: конспект вебінару Михайла Кольцова. 04.02.2022. *Journalism Teachers' Academy:* веб-сайт. URL: https://www.jta.com.ua/knowledge-base/instrumenty-dlia-perevirky-dipfeykiv-konspekt-vebinaru-mykhayla-koltsova

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

16. Постанова Верховного Суду від 10.09.2020 у справі № 751/6069/19 (провадження № 51-1704км20). URL: https://reyestr.court.gov.ua/Review/91722819

17. Постанова Верховного Суду від 15.01.2020 у справі № 161/5306/16-к (провадження № 51-3498км19). URL: https://reyestr.court.gov.ua/Review/87053591

18. Постанова Верховного Суду від 22.10.2020 у справі № 677/2040/16-к (провадження № 51-5738км19). URL: https://reyestr.court.gov.ua/Review/92458395

19. Постанова Верховного суду від 26.01.2021 у справі № 236/4268/18 (провадження №51-3124км20). URL: https://reyestr.court.gov.ua/Review/94905297

20. Постанова Верховного суду від 31.10.2019 у справі №404/700/17 (провадження № 51-4451км19). URL: https://reyestr.court.gov.ua/Review/85390646

21. Постанова Об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20). URL: https://reyestr.court.gov.ua/Review/96074938

22. Постанова Третьої судової палати Касаційного кримінального суду Верховного Суду від 28.02.2024 у справі №753/14148/21 (провадження № 51-6134 км 23). URL: https://reyestr.court.gov.ua/Review/117442733

23. Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел: лист-орієнтування Офісу Генерального прокурора від 28.08.2021 № 18/1-386 вих – 5150кв – 21.

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

25. Ратнова А.В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: дис…д-ра філ.: 081 – Право /Львівський державний університет внутрішніх справ. Львів, 2021. 248 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3747

26. Рішення ЄСПЛ у справі «Грузія проти Росії (II)» (Georgia v. Russia (II)) [ВП]. Заява № 38263/08 від 21.01.2021. URL: https://rm.coe.int/georgia-v-russia-ii-gc-ukr/1680a58450

27. Рішення МКС у справі «Прокурор проти Ахмада Аль-Факі Аль-Махді (Prosecutor v. Ahmad Al Faqi Al Mahdi). Заява ICC-01/12-01/15 від 27.09.2016. URL: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2016_07244.PDF

28. Рішення МКС у справі «Прокурор проти Махмуда Мустафи Бусайф аль-Верфаллі» (Prosecutor v. Mahmoud al-Werfalli). Заява ICC-01/11-01/17 від 04.07.2018. https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2018_03552.PDF

29. Розслідування воєнних злочинів в Україні: правозахисники анонімно опитали правоохоронців і зібрали дані. 21.09.2023. *Радіо Свобода :* веб-сайт. URL:

https://www.radiosvoboda.org/a/doslidzhennia-rozsliduvannia-voiennyh-zlochyniv-v-ukraini/32602285.html

30. Скрипник А.В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. 408 с.

31. Столітній А.В. Електронне кримінальне провадження на досудовому розслідуванні. дис. … д-ра юрид. наук : 12.00.09. МВС України. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018. 648 с.

32. Столітній А.В. Електронне кримінальне провадження на досудовому розслідуванні : автореф. дис. … докт. юрид. наук : 12.00.09. МВС України. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018. 42 с. URL: https://dduvs.in.ua/wp-content/uploads/files/Structure/science/rada/auto/20/3.pdf

33. Столітній А.В. Електронне кримінальне провадження: передумови виникнення, сучасний стан та перспективи розвитку: монографія. К.: Видавничий дім «АртЕк», 2016. 724 с.

34. Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел. 7.06.2022. *Верховний суд :* веб-сайт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/

35. Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. 28.10.2021. *Верховний суд :* веб-сайт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/

36. Судова практика ККС Верховного Суду щодо допустимості електронних доказів: презентація, підготовлена суддею Верховного Суду Надією Стефанів. Верховний суд : веб-сайт. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf

37. Топ-10 кращих інструментів OSINT для розвідки з відкритим вихідним кодом. 19.07.2022. *Софтліст:* веб-сайт. URL: https://ua.softlist.com.ua/articles/top-10-luchshykh-ynstrumentov-osint-dlia-razvedki-s-otkrytym-ishodnym-kodom/

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

39. Удовенко Ж.В., Басиста І.В. Використання штучного інтелекту у кримінальному провадженні: ілюзія чи реальність. *Штучний інтелект у правовій практиці: межі та можливості»* : збірник тез Всеукраїнського круглого столу (15 березня 2024 року) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2024. С. 188–197.

40. Фоміна Т.Г., Рачинський О.О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник ХНУВС.* 2023. № 3(102). С. 207–220. DOI: https://doi.org/10.32631/v.2023.3.43

41. Цивільний процесуальний кодекс України: Закон України від 18.03.2004 № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15?find=1&text=електронні+#w1_11

42. 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

43. Inteligence community directive № 301. National open source enterprise (effective : july 11, 2006). *Federation of American Scientists: website.* URL: https://irp.fas.org/dni/icd/icd-301.pdf

References

1. Basysta, I., Udovenko, Zh., & Kulynych, M.-M. (2024). Ohliad tendentsii shchodo shtuchnoho intelektu ta yoho perspektyvnist dlia protsesualnykh rishen u perebihu kryminalnoho provadzhennia. [Review of trends regarding artificial intelligence and its prospects for procedural decisions during criminal proceeding] *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu, Seriia PRAVO,* 80: 3, 19–38. https://doi.org/10.24144/2307-3322.2024.81.3.3 (in Ukrainian)

2. Martynovskyi, R., & Moroz, L. (Ed.). (2018). *Vybir zarady spravedlyvosti: posibnyk zi stvorennia mekhanizmiv prytiahnennia do vidpovidalnosti za naitiazhchi zlochyny*. [Options for justice: a handbook for designing accountability mechanisms for grave crimes]. (O. Bondarenko transl.) Vol. 2. (in Ukrainian)

3. The verdict of the Kyiv District Court of Kharkiv of August 14, 2023 in case No. 953/2635/23. Available at: https://reyestr.court.gov.ua/Review/112892204 (accessed 16 may 2024) (in Ukrainian)

4. The verdict of the Khmelnytskyi City District Court of Khmelnytskyi region of 03.10.2023 in case No. 686/3769/23 (proceedings No. 1-kp/686/745/23). Available at: https://reyestr.court.gov.ua/Review/113906215 (accessed 16 may 2024) (in Ukrainian)

5. Hutnyk, A. V., & Khytra, A. Ya. (2022). *Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni*. [Criminal procedural and criminalistics fundamentals of the use of electronic documents exchange in proof of evidence]. Lviv: LvDUVS. (in Ukrainian)

6. Informatsiini tekhnolohii. Metody zakhystu. Nastanovy dlia identyfikatsii, zbyrannia, zdobuttia ta zberezhennia tsyfrovykh dokaziv. (2018). DSTU ISO/IEC 27037:2017. Kyiv : UkrNDNTs. (in Ukrainian).

7. Zadoia, K. (2024, February 1). Pershe kryminalne provadzhennia v SShA shchodo voiennykh zlochyniv, vchynenykh v Ukraini. [The first criminal proceedings in the USA regarding war crimes committed in Ukraine]. *T4P*. Retrieved from: https://t4pua.org/2281 (accessed 16 may 2024) (in Ukrainian).

8. Gathering information from open sources as a future means of evidence in the most serious international crimes. *ANTIRAID*. (2023, December 7). Retrieved from: https://antiraid.com.ua/news/zbir-informatsii-z-vidkrytykh-dzherel-iak-majbutnij-zasib-dokaziv-u-najvazhchykh-mizhnarodnykh-zlochynakh/ (accessed 16 may 2024) (in Ukrainian).

9. Case: The court closed the criminal proceedings against a transwoman who was accused of distributing pornographic images (2023, May 17). PROZhEKTOR. Retrieved from: https://www.projector.org.ua/projects_ua/public_hrc_ua/cases_hrc_ua/case_marii-vinichenko_sud/ (accessed 16 may 2024) (in Ukrainian)

10. Kovalenko, A. (2024). Ohliad kompiuternykh danykh pid chas rozsliduvannia kolaboratsiinoi diialnosti: typovi obiekty ta pryklady z praktyky [Review of computer data in collaborative investigation: typical objects and examples from practice]. *Viina v Ukraini: zrobleni vysnovky ta nezasvoieni uroky: zbirnyk tez Mizhnarodnoi naukovo-praktychnoi konferentsii* (pp. 413–417). Lviv: Lvivskyi derzhavnyi universytet vnutrishnikh sprav. (in Ukrainian)

11. Nor, V., Bobechko, N., Bahrii, M., & Bobechko, N. (2021). Kryminalnyi protses Ukrainy: Akademichnyi kurs: u 3 t. [Criminal process of Ukraine: Academic course: in 3 volumes] (Vol. 1. Zahalna chastyna [Common part]). Lviv: LNU im. Ivana Franka. (in Ukrainian)

12. Makbraid, D. (n.d.). Zastosovni mizhnarodno-pravovi ramky ta standarty shchodo dokaziv iz vidkrytykh ta elektronnykh dzherel: Yevropeiska konventsiia z prav liudyny. [Applicable international legal framework and standards for evidence from open and electronic sources: European Convention on Human Rights]. *Council of Europe*. Retrieved from: https://rm.coe.int/coe-ukraine-open-uk/1680a6e571 (accessed 16 may 2024) (in Ukrainian).

13. Matvieiev, V. (2023, July 27). Problemy ta vyklyky, poviazani zi zborom elektronnykh dokaziv. [Problems and challenges associated with the collection of electronic evidence]. *JustTalk*. Retrieved from: https://justtalk.com.ua/post/problemi-ta-vikliki-povyazani-zi-zborom-elektronnih-dokaziv (accessed 16 may 2024) (in Ukrainian)

14. Moroz, M. (2022, February 4). Yak rozpiznaty dipfeik: konspekt vebinaru Mykhaila Koltsova. [How to recognize a deepfake: synopsis of Mykhailo Koltsov's webinar]. *Akademiia vykladachiv zhurnalistyky*. Retrieved from: https://www.jta.com.ua/knowledge-base/instrumenty-dlia-perevirky-dipfeykiv-konspekt-vebinaru-mykhayla-koltsova (accessed 16 may 2024) (in Ukrainian)

15. Resolution of the Grand Chamber of the Supreme Court, dated 28/02/2024, case no. 415/2182/20. Available at: https://reyestr.court.gov.ua/Review/117555176 (accessed 16 may 2024) (in Ukrainian)

16. Resolution of the Supreme Court, dated 10/09/2020, case no. 751/6069/19. Available at: https://reyestr.court.gov.ua/Review/91722819 (accessed 16 may 2024) (in Ukrainian)

17. Resolution of the Supreme Court, dated 15/01/2020, case no. 161/5306/16-к. Available at: https://reyestr.court.gov.ua/Review/87053591 (accessed 16 may 2024) (in Ukrainian)

18. Resolution of the Supreme Court, dated 22/10/2020, case no. 677/2040/16-к. Available at: https://reyestr.court.gov.ua/Review/92458395 (accessed 16 may 2024) (in Ukrainian)

19. Resolution of the Supreme Court, dated 26/01/2021, case no. 236/4268/18. Available at: https://reyestr.court.gov.ua/Review/94905297 (accessed 16 may 2024) (in Ukrainian)

20. Resolution of the Supreme Court, dated 31/10/2019, case no. 404/700/17. Available at: https://reyestr.court.gov.ua/Review/85390646 (accessed 16 may 2024) (in Ukrainian)

21. Resolution of the joint chamber of the Criminal Court of Cassation of the Supreme Court, dated 29/03/2021, case no. 554/5090/16-к. Available at: https://reyestr.court.gov.ua/Review/96074938 (accessed 16 may 2024) (in Ukrainian)

22. Resolution of the Third Judicial Chamber of the Criminal Court of Cassation of the Supreme Court, dated 28/02/2024, case no. №753/14148/21. Available at: https://reyestr.court.gov.ua/Review/117442733 (accessed 16 may 2024) (in Ukrainian)

23. On the organization of investigative actions on the collection and preservation of digital information from open sources: orientation letter № 18/1-386vykh – 5150kv– 21 (2021, August 28). Ofis Heneralnoho prokurora. (in Ukrainian)

24. *Berkeley Protocol on Digital Open Source Investigations*. (O. Ziuz, unofficial translation) (2020). United Nations, on behalf of the Office of the United Nations High Commissioner for Human Rights (OHCHR), and the Human Rights Center at the University of California, Berkeley, School of Law.. Tsentr z prav liudyny Kaliforn. un-tu, Berkli, Yuryd. shk., OON Upr. Verkhov. komisara z prav liudyny. Available at: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (accessed 16 may 2024) (in Ukrainian)

25. Ratnova, A. (2021). *Criminal procedural and criminalistics fundamentals of the use of electronic documents exchange in proof of evidence:* PhD diss. Lviv: LvDUVS. Available at: https://dspace.lvduvs.edu.ua/handle/1234567890/3747 (accessed 16 may 2024) (in Ukrainian)

26. The ECHR judgement "Georgia v Russia (II)" (2021, January 21), case no. 38263/08. Available at: https://rm.coe.int/georgia-v-russia-ii-gc-ukr/1680a58450 (accessed 16 may 2024) (in Ukrainian)

27. Public Judgment and Sentence ICC in the case of the Prosecutor v. Ahmad Al Faqi Al Mahdi dated 27/09/2016, ICC-01/15. Available at: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2016_07244.PDF (accessed 16 may 2024)

28. Public Second Warrant of Arrest ICC in the case of the Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli, dated 04/07/2018, ICC-01/17. Available at: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2018_03552.PDF (accessed 16 may 2024)

29. Investigating war crimes in Ukraine: human rights defenders anonymously interviewed law enforcement officers and collected data (2023, September 21). *Radio Svoboda*. Available at: https://www.radiosvoboda.org/a/doslidzhennia-rozsliduvannia-voiennyh-zlochyniv-v-ukraini/32602285.html (accessed 16 may 2024) (in Ukrainian)

30. Skrypnyk, A. (2022). *Vykorystannia tsyfrovoi informatsii v kryminalnomu protsesualnomu dokazuvanni* [Use of digital information in criminal procedure evidence]. Nats. yuryd. un-t im. Yaroslava Mudroho. Kharkiv: Pravo. (in Ukrainian)

31. Stolitnii, A. (2018). *Elektronne kryminalne provadzhennia na dosudovomu rozsliduvanni*. [Electronic criminal proceedings at pre-trial investigation]: Doctor's degree in Law diss. Dnipro: Dnipropetrovskyi derzhavnyi universytet vnutrishnikh sprav. (in Ukrainian).

32. Stolitnii, A. (2018). *Elektronne kryminalne provadzhennia na dosudovomu rozsliduvanni.* [Electronic criminal proceedings at pre-trial investigation]*:* Doctor's degree in Law thesis abstract. Dnipro. Dnipropetrovskyi derzhavnyi universytet vnutrishnikh sprav. (in Ukrainian)

33. Stolitnii, A. (2016). *Elektronne kryminalne provadzhennia na dosudovomu rozsliduvanni.* [Electronic criminal proceedings at pre-trial investigation]. K.: Vydavnychyi dim «ArtEk». (in Ukrainian)

34. Supreme Court judges discussed the admissibility of electronic evidence obtained from open sources with experts (2022, June 7). Verkhovnyi Sud. Available at: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/ (accessed 16 may 2024) (in Ukrainian)

35. The judges of the CCS of the Supreme Court discussed the problematic issues of the admissibility of electronic evidence during the trial (2021, October 28). Verkhovnyi Sud. Available at: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/ (accessed 16 may 2024) (in Ukrainian)

36. Stefaniv, N. (n. d.). *Sudova praktyka KKS Verkhovnoho Sudu shchodo dopustymosti elektronnykh dokaziv*. [Judicial practice of the Supreme Court of the Supreme Court on the admissibility of electronic evidence]. Verkhovnyi Sud. Available at: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf (accessed 16 may 2024) (in Ukrainian)

37. Top 10 Best Open Source OSINT Intelligence Tools (2021, July 19). Softlist. Available at: https://ua.softlist.com.ua/articles/top-10-luchshykh-ynstrumentov-osint-dlia-razvedki-s-otkrytym-ishodnym-kodom/ (accessed 16 may 2024) (in Ukrainian)

38. Torbas, O. (2024). *OSINT pry rozsliduvanni kryminalnykh pravoporushen*. [OSINT in the investigation of criminal offenses]. O.: «Yurydyka». (in Ukrainian)

39. Udovenko, Zh., & Basysta, I. (2024). Vykorystannia shtuchnoho intelektu u kryminalnomu provadzhenni: iliuziia chy realnist. [The use of artificial intelligence in criminal proceedings: illusion or reality]. *Shtuchnyi intelekt u pravovii praktytsi: mezhi ta mozhlyvosti»: zbirnyk tez Vseukrainskoho kruhloho stolu* (pp. 188–197). Lviv: Lvivskyi derzhavnyi universytet vnutrishnikh sprav. (in Ukrainian)

40. Fomina, T. H., & Rachynskyi, O. O. (2023). Electronic evidence in criminal proceedings: problematic issues of theory and practice. *Bulletin of Kharkiv National University of Internal Affairs*, 102

(3 (Part 2)), 207–220. https://doi.org/10.32631/v.2023.3.43 (in Ukrainian)

41. Civil Procedure Code of Ukraine (2004, March 18) № 1618-IV (Ukraina). Available at: https://zakon.rada.gov.ua/laws/show/1618-15#Text (accessed 16 may 2024) (in Ukrainian)

42. *Berkeley Protocol on Digital Open Source Investigations*. (2022). United Nations, on behalf of the Office of the United Nations High Commissioner for Human Rights (OHCHR), and the Human Rights Center at the University of California, Berkeley, School of Law. Available at: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (accessed 16 may 2024). (in English)

43. Inteligence community directive, № 301 (2006). Federation of American Scientists. Available at: https://irp.fas.org/dni/icd/icd-301.pdf (accessed 16 may 2024). (in English)

Стаття: надійшла до редакції 08.03.2024
прийнята до друку 28.03.2024
The article: is received 08.03.2024
is accepted 28.03.2024

Бібліографія: 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: Журнал. Серія Право*. Івано-Франківськ: Редакційно-видавничий відділ Університету Короля Данила, 2024. Вип. 17 (29). С. 227-243. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243