ISSN 2072-8670 (Print) **НАУКА І ПРАВООХОРОНА**
NAUKA I PRAVOOKHORONA
DOI (Issue): https://doi.org/10.36486/np.2024.2(64) **Issue 2(64) 2024**
УДК 343.14:004.738.5

Гаврилюк Людмила Володимирівна,
кандидат юридичних наук, старший дослідник, начальник відділу
ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0002-9441-4073
Бурлака Владислав Васильович,
кандидат юридичних наук, начальник відділу Головного слідчого
управління Національної поліції України, м. Київ, Україна,
ORCID ID 0000-0003-1824-4380
Пелехатий Віталій Тадейович,
старший слідчий в особливо важливих справах 3-го відділу управління
організації роботи та методичного забезпечення Головного слідчого
управління Національної поліції України, м. Київ, Україна

ОСОБЛИВОСТІ ОГЛЯДУ ЦИФРОВИХ МАТЕРІАЛІВ З ВІДКРИТИХ ДЖЕРЕЛ МЕРЕЖІ «ІНТЕРНЕТ» ЗА ПРОТОКОЛОМ БЕРКЛІ

Статтю присвячено з'ясуванню сутності огляду цифрових матеріалів з відкритих джерел мережі «Інтернет» у кримінальному провадженні. Проаналізовано норми КПК України, Протокол Берклі та наукові джерела, за результатами чого визначено заходи, які слід вживати під час роботи з цифровими матеріалами з відкритих джерел. Акцентовано увагу на необхідності вжиття заходів безпеки під час роботи з цифровими матеріалами. Вироблено практичні рекомендації щодо дій слідчого під час огляду цифрових матеріалів із відкритих джерел.

Ключові слова: *кримінальне провадження, досудове розслідування, доказування, докази, слідчий, огляд, комп'ютерні дані, цифрова інформація, цифрові матеріали з відкритих джерел, електронні (цифрові) докази, цифрові дані, відкриті джерела цифрової інформації, Протокол Берклі.*

Сьогодні «великий масив інформації зберігається у відкритому доступі в мережі «Інтернет» і є доступним для необмеженого кола користувачів. Будь-хто за допомогою лише смартфону може створити повідомлення, фотозйомку, аудіо- чи відеозапис та поширити його в соціальних мережах, власних сайтах і таким чином поділитися своїми думками, подіями. Але ця ж інформація може мати значення для кримінального провадження» [1]. Для того, щоб така інформація набула доказового значення, її потрібно зібрати в передбаченому КПК України порядку.

Аналіз останніх досліджень і публікацій. Процесуальним та криміналістичним особливостям збирання та використання електронних (цифрових) доказів у кримінальному провадженні неодноразово присвячували свої роботи М.В. Гуцалюк, Ю.Ю. Орлов, Т.Г. Фоміна, Д.М. Цехан, С.С. Чернявський та ін.

Окремі аспекти використання цифрових даних із відкритих джерел під час розслі-

DOI (Article): https://doi.org/10.36486/np.2024.2(64).21

дування кримінальних правопорушень дослідили І.В. Басиста, Л.В. Гаврилюк, А.В. Гутник, А.Я. Хитра [1]. Процесуальний порядок, тактику проведення огляду комп'ютерних даних та особливості проведення огляду вебресурсів як різновиду огляду комп'ютерних даних ґрунтовно розкрив А.В. Коваленко [2; 3; 4]. Мінімальні стандарти для пошуку, збирання, зберігання, перевірки та аналізу таких матеріалів окреслено у Протоколі Берклі, який є лише практичним посібником з ведення розслідування з використанням відкритих цифрових даних [5]. За результатами аналізу судових рішень та матеріалів кримінальних проваджень можна констатувати, що сьогодні слідчі під час досудового розслідування різних категорій кримінальних правопорушень керуються наведеними в Протоколі Берклі рекомендаціями щодо збирання, збереження та використання в кримінальному провадженні цифрових даних із відкритих джерел. Дотримуватися визначеної в Протоколі Берклі послідовності дій щодо збору та збереження отриманих цифрових даних і недопущення видалення інформації з мережі «Інтернет» рекомендують і судді Касаційного кримінального суду у складі Верховного Суду [6]. Подальше дослідження цього питання зумовлено відсутністю належного правового регулювання порядку огляду цифрових матеріалів із відкритих джерел та уніфікованого порядку збирання і використання цифрових матеріалів із відкритих джерел як доказів у кримінальному провадженні.

Метою статті є дослідження кримінальних процесуальних та криміналістичних особливостей огляду цифрових матеріалів з відкритих джерел мережі «Інтернет» з урахуванням актуальної слідчої практики, положень Протоколу Берклі та вироблення практичних рекомендацій щодо порядку проведення та фіксування цієї слідчої (розшукової) дії слідчими під час досудового розслідування.

Виклад основного матеріалу. Передусім слід з'ясувати, що розуміється під відкритими джерелами цифрової інформації. У Протоколі Берклі виокремлено види цифрової інформації з відкритих джерел залежно від способу її отримання, а саме шляхом спостереження, купівлі та звернення із запитом. Такою інформацією може бути: 1) контент, який можна отримати перейшовши на відповідний сайт із використанням будь-якого безкоштовного веббраузера; 2) контент, який можна отримати шляхом входу або зареєструвавшись на онлайн-платформі з метою доступу до нього та його перегляду; 3) інформація, яка знаходиться на платних платформах, або на платформах, у яких додаткові функціональні можливості та доступ до даних є платними; 4) інформація, яка знаходиться в базах даних та на платформах, які можуть бути доступними для всіх представників громадськості лише на платній основі; 5) інформація, отримана за запитом, з яким може звернутися будь-яка особа до державних органів, які мають юридичні зобов'язання відповідати однаково всім особам, щодо публічної інформації відповідно до законодавства про інформацію [5]. Тобто «відкриті джерела цифрової інформації це – медіа, соціальні медіа, вебсайти, геопросторові платформи, бази даних, офіційні дані та інші платформи, на яких можна спостерігати, купувати або запитувати загальнодоступну інформацію» [1, с. 233].

Водночас потрібно чітко розуміти, що розвідка за відкритими джерелами не виконує функції збору інформації, пов'язаної із процесами розслідування, встановлення

елементів різних злочинів. «…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» [1, с. 233; 5, с. 26].

Окрім того, під час використання цифрової інформації з відкритих джерел мережі «Інтернет» слід керуватися ст. 84 КПК України, згідно з якою «доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню» [7].

У кримінальному процесі України одним із способів виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення є проведення передбаченої ст. 237 КПК України слідчої (розшукової) дії – огляду. На думку А.В. Коваленка, така слідча (розшукова) дія зазвичай спрямована на дослідження та фіксування матеріальної обстановки і є незамінним процесуальним засобом отримання доказової й орієнтуючої інформації від об'єктів матеріального світу. Проте, сьогодні надто часто в слідчих виникає необхідність у межах кримінального провадження дослідити зміст інформації з відкритих джерел мережі «Інтернет», що міститься в пам'яті комп'ютерної техніки таких пристроїв чи обробляється ними. З ухваленням Закону України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» від 15 березня 2022 р. № 2137-IX така інформація дістала назву «комп'ютерні дані», а процедура її вилучення, фіксування та оперативного дослідження стала новим легально визначеним видом огляду – «оглядом комп'ютерних даних» [3].

Термін *«комп'ютерні дані»* визначений у ст. 1 Конвенції про кіберзлочинність, як будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки в комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою [8]. Як убачається зі змісту Конвенції про кіберзлочинність, *комп'ютерна система* – це будь-який пристрій або група взаємопоєднаних або пов'язаних пристроїв, один чи більше з яких відповідно до певної програми виконує автоматичну обробку даних [8]. Розкриваючи сутність комп'ютерних даних, А.В. Коваленко зазначає, що за своїм визначенням це є інформацією, яка була зашифрована для обробки логічними процесорами комп'ютерної техніки і в оригінальному вигляді не може бути сприйнята органами чуття людини. Тому *безпосередньому дослідженню уповноваженими особами підлягає візуальне та аудіовізуальне вираження комп'ютерних даних після їх інтерпретації засобами комп'ютерної техніки* [3]. З огляду на зазначене можна констатувати, що *цифрові дані/інформація/матеріали з відкритих джерел є одним із видів комп'ютерних даних.*

Згідно зі ст. 237 КПК України огляд комп'ютерних даних проводиться з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення. Огляд цифрових матеріалів із відкритих джерел мережі «Інтернет» умовно можна поділити на такі етапи:

1) пошук необхідної інформації на вебсторінці, яка має значення для кримінального провадження;

2) безпосередній огляд, який включає:

- фіксацію інформації, яка розміщена на оглянутій вебсторінці, та ходу СРД в протоколі огляду з відображенням послідовності всіх дій під час проведення огляду;

- збереження цифрових матеріалів із відкритих джерел, які будуть використовуватися як доказ у кримінальному провадженні;

- формування додатків до протоколу огляду.

Кожний із цих етапів передбачає комплекс заходів, які необхідно вжити при підготовці для їх здійснення.

Так, у Протоколі Берклі йдеться, що слідчі, які проводять розслідування з використанням даних у відкритому доступі, повинні розпочинати розслідування в інтернеті лише після вжиття певних підготовчих заходів, які включають:

1) проведення цифрової оцінки загроз та ризиків:

- щоб визначити загальні та конкретні загрози, які можуть виникнути в результаті діяльності в інтернеті, зокрема відвідування цільових вебсайтів, постійного моніторингу конкретних джерел або вилучення даних із платформ соціальних медіа. Оцінку цифрових загроз і ризиків слід здійснювати консультуючись (або із залученням) спеціаліста із кібербезпеки;

2) проведення оцінки цифрового середовища:

- слідчі повинні розуміти цифрове середовище досліджуваної ситуації (тип доступної та використовуваної технології, у тому числі ким вона використовується), що матиме вплив на типи доступних цифрових даних;

3) розробку плану онлайн-розслідувань, який має охоплювати: 1) загальну стратегію розслідування; 2) конкретні операції з розслідування в інтернеті. Якщо онлайн-розслідування є частиною більш широкого розслідування з використанням традиційних методів, таких як взяття показань свідків або збір речових доказів, план онлайн-розслідування слід включити до основного плану розслідування;

4) встановлення політики щодо збереження даних, видалення даних, доступу до даних та обміну ними, перш ніж збирати та зберігати інформацію [5].

Відповідно до абзацу другого ч. 2 ст. 237 КПК України огляд комп'ютерних даних проводиться слідчим, прокурором, а також дізнавачем, який згідно з ч. 1 ст. 401 КПК України при здійсненні дізнання наділяється повноваженнями слідчого [7], 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).

Сутність огляду як одного зі способів виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення та зміст абзацу другого ч. 2 ст. 237 КПК України вказують на те, що «під час огляду комп'ютерних даних уповноважені особи мають особисто сприйняти зміст аудіовізуального виразу комп'ютерних даних і відобразити його у протоколі процесуальної дії та додатках до нього у формі, придатній для сприйняття такого змісту іншими людьми. Для безпосереднього сприйняття люди-

ною комп'ютерні дані, що містять текст, зображення, звуки й інші аудіовізуальні форми інформації, можуть бути відтворені через пристрої виведення даних (екран, аудіопристрої, принтери тощо), а код, що містить алгоритми дій, може бути виконано (запущено програму)» [3].

Згідно з ч. 3 ст. 237 КПК України для участі в огляді може бути запрошений потерпілий, підозрюваний, захисник, законний представник та інші учасники кримінального провадження. З метою одержання допомоги з питань, що потребують спеціальних знань, слідчий, прокурор для участі в огляді може запросити спеціалістів. Тобто КПК України не передбачає обов'язкової участі спеціаліста під час здійснення слідчим, прокурором огляду комп'ютерних даних. Але слід врахувати, що згідно з ч. 4 ст. 99 КПК України копії інформації, у тому числі комп'ютерних даних, які містяться в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, визнаються судом як оригінал документа за умови, якщо вони виготовлені слідчим, прокурором із залученням спеціаліста. Окрім того, ч. 2 ст. 71 КПК України передбачає, що під час досудового розслідування спеціаліст може бути залучений для надання безпосередньої технічної допомоги (фотографування, складення схем, планів, креслень тощо) сторонами кримінального провадження. Також згідно з ч. 1 ст. 41 КПК України слідчий може доручити проведення огляду сайтів, інтернет-ресурсів, відео та інших відомостей, розміщених у мережі «Інтернет», працівнику оперативного підрозділу, який володіє знаннями у сфері інформаційних технологій.

Резюмуємо, в нормах КПК України передбачено:

- огляд комп'ютерних даних як один із способів виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення;
- слідчий, дізнавач, прокурор, працівник оперативного підрозділу за дорученням слідчого, уповноважені суб'єкти з проведення огляду комп'ютерних даних;
- можливість залучення слідчим, прокурором спеціаліста з метою одержання допомоги з питань, що потребують спеціальних знань для проведення огляду комп'ютерних даних та надання технічної допомоги під час проведення СРД;
- виготовлення копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах слідчим, прокурором із обов'язковим залученням спеціаліста (що є умовою визнання їх судом як оригінал документа);
- форму відображення інформації, яку містять комп'ютерні дані, яка має бути придатною для сприйняття їх змісту;
- можливість використання електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або в паперовій формі як способи фіксації комп'ютерних даних.

Одним із основних етапів процесу розслідування з використання матеріалів з відкритих джерел є збір таких матеріалів, який відповідно до ст. 223 КПК України здійснюється шляхом проведення СРД, у цьому випадку під час огляду.

У Протоколі Берклі *збір* визначено як акт заволодіння інформацією в інтернеті за допомогою знімка екрана, конвертації в PDF, експертного завантаження чи іншої форми захоплення. Після того, як цифровий контент буде ідентифіковано та визнано відповідним для розслідування та prima facie відповідним і надійним для своєї мети, слідчий повинен визначити належний метод збору. Методи збору можуть змінюватися залежно від того, чи має онлайн-контент потенційну доказову силу, чи він буде використовуватися для прийняття рішень, чи він буде сприяти лише внутрішньому продукту роботи. У випадках, *коли йдеться просто про робочий продукт, може бути достатньо скріншоту або перетворення в PDF,* тоді як вміст, який має потенційну доказову силу, вимагає більш *ретельного та обґрунтованого методу збору* (наприклад, шляхом призначення значення хешу) [5, с. 86].

Збір онлайн-контенту може здійснюватися вручну за стандартною операційною процедурою або бути автоматизованим за допомогою різноманітних інструментів.

Вказівки щодо того, як і які цифрові матеріали збирати з відкритих джерел, наведено в п. 155 розділу VI Протоколу Берклі [5]. Наразі вони слугують мінімальними стандартами для надання доказів до суду. **Керуючись цими вказівками під час збору цифрових матеріалів із відкритих джерел слідчі повинні:**

1. Записати вебадресу зібраного контенту, також відому як єдиний локатор ресурсів (URL) або ідентифікатор (URI).

2. Захопити вихідний код HTML вебсторінки, якщо це можливо. Вихідний код HTML містить набагато більше інформації, ніж видима частина вебсайту. Вихідний код HTML сприятиме автентифікації зібраного матеріалу.

3. Захопити всю сторінку, яка оглядається. Зробити знімок екрана цільової вебсторінки із зазначенням дати та часу. Означений процес полягає в тому, щоб охопити все побачене під час збору.

4. Зібрати вбудовані мультимедійні файли. Наприклад, якщо завантажують вебсторінку з відео або зображеннями, ці конкретні елементи також слід витягти та зібрати з вебсторінки.

5. Зібрати вбудовані метадані, якщо вони є та застосовні. Метадані можуть змінюватися залежно від джерел, але загальні метадані включають ідентифікатор користувача завантажувача; ідентифікатор публікації, зображення чи відео; дату та час завантаження; геотег; хештег; коментарі; анотацію.

6. Зібрати контекстуальні дані. Контекстний контент також слід збирати, якщо він має значення для розуміння цифрового елемента. Вони можуть включати коментарі до відео, зображення чи публікації; передбачати завантаження інформації; та/або інформацію про завантажувача/користувача, таку як ім'я користувача, справжнє ім'я чи біографію. Необхідність збору навколишньої інформації слід визначити з огляду на специфіку випадку та цифрового матеріалу.

7. Записати всі відповідні дані (дані збору), які стосуються збору, такі як ім'я збирача, IP-адреса машини, яка використовується для збору інформації, віртуальна особистість, за наявності, та мітка часу. Слідчі мають переконатися, що системний годинник точний, бажано, шляхом його синхронізації з сервером мережевого протоколу

часу. Причиною цього кроку є забезпечення того, щоб метадані, пов'язані з часом, були точно представлені в зібраних файлах. Якщо для доступу до зібраної інформації використовується віртуальна особистість, це слід зазначити.

8. Додати хеш-значення. Хеш-значення – це унікальна форма цифрової ідентифікації, яка за допомогою криптографії підтверджує, що зібраний контент є унікальним і не змінювався з моменту збору. На момент збору слідчі, що проводять розслідування з використанням даних у відкритому доступі, повинні вручну додати – інструмент збирання – автоматично додати – значення хешу. Існує безліч різних типів хешів, і стандарти з часом змінилися. Слідчі мають оцінити, який хеш використовувати, зважаючи на прийнятий на цей момент стандарт [5].

Щоб визначитися чи варто збирати цифровий матеріал із відкритих джерел мережі «Інтернет», слідчі, які проводять розслідування з використанням таких матеріалів, *повинні врахувати такі фактори:*

1. Релевантність. Чи є цифровий елемент відповідним для конкретного розслідування?

2. Достовірність. Чи є інформація щодо цифрового контенту достовірною? Це може включати перевірку метаданих та спробу виявлення першоджерела матеріалу пов'язаної інформації та джерела [5, с. 85–87].

3. Видалення. Чи є ймовірність видалення цифрового елемента з інтернету чи загального доступу? Якщо так, потрібно зібрати найнадійнішу відому версію.

4. Безпека. Чи безпечно збирати цифровий елемент, чи можна і варто вживати додаткових заходів безпеки?

5. Подальші обов'язки. Слідчі, які проводять розслідування з використанням даних у відкритому доступі, мають визначити, які заходи необхідно буде вжити, наприклад, щодо збереження цифрових матеріалів [5].

У Протоколі Берклі «збереження цифрових матеріалів» передбачено як один із основних етапів процесу розслідування. Постійність і доступність інформації в інтернеті часто є нестабільними через те, що платформи соціальних медіа можуть видаляти контент зі своїх платформ відповідно до умов використання, або користувачі можуть вибирати видалення або редагування власного завантаженого контенту. Крім того, інформацію в інтернеті можна легко деконтекстуалізувати, втратити, стерти або пошкодити.

Тому, важливо, щоб слідчі під час роботи з цифровими матеріалами з відкритих джерел вжили всіх належних заходів для збереження їх властивостей упродовж необхідного часу для кримінального провадження.

На думку архівістів, властивості цифрового елементу, який потрібно охороняти та зберігати з плином часу, включають його автентичність, доступність, ідентичність, стійкість, можливість відображення та зрозумілість.

Іншими важливими питаннями, які можуть виникнути під час процесу збереження, є:

1. Ланцюг забезпечення збереження – хронологічна документація послідовності дій зберігачів інформації чи доказів, а також документація контролю, дати та часу, передачі, аналізу та розпорядження такими доказами.

2. Доказова копія – цифровий елемент, зібраний слідчим у його первинному ви-

гляді, який не варто змінювати. Цифрові елементи потрібно зберігати в оригінальному вигляді. Це означає збереження чистого оригіналу зібраного цифрового елемента в усіх форматах, у яких він був зібраний.

3. Робочі копії – копія або копії цифрового елементу, які потрібно створити для цілей аналізу та зберігати окремо, щоб слідчі могли працювати з копією, а не з оригіналом. Це дає змогу мінімально обробляти оригінал і зменшувати ризик його компрометації або зміни. Будь-які зміни до елементу, включаючи виготовлення копій, мають бути задокументовані. Якщо можливо, варто використовувати окремі системи зберігання для доказових копій та робочих копій.

4. Зберігання, що допомагає забезпечити довготривалість цифрових елементів та можливість їх пошуку та відновлення. Збереження цифрового матеріалу так, щоб зберегти його автентичність і документувати ланцюг забезпечення збереження, збільшить ймовірність того, що він може бути прийнятий як доказ у суді [5, с. 89–91].

Отже, зважаючи на положення Протоколу Берклі, норми КПК України, якими передбачено підстави, порядок проведення огляду комп'ютерних даних, визначено уповноважених суб'єктів на проведення цієї СРД, а також інших учасників кримінального провадження, які можуть бути присутніми під час проведення цієї СРД, тощо; особливості організації і тактики проведення огляду комп'ютерних даних, огляду вебресурсів тощо, які розкрито в працях А.В. Коваленка [2; 3; 9], порядок виявлення, вилучення та дослідження цифрових (електронних) слідів, визначений у навчальному посібнику «Криміналістика: криміналістична техніка» [10], під час огляду цифрових матеріалів з відкритих джерел *пропонуємо слідчим дотримуватися таких рекомендацій:*

1. Зазначений вид огляду може здійснюватися слідчим (при необхідності із залученням спеціаліста) у службовому кабінеті з використанням службового комп'ютера, на якому встановлено ліцензійне програмне забезпечення та організовано доступ до мережі «Інтернет», із застосуванням технічних засобів фіксації (якщо в цьому є потреба).

2. Перед початком огляду:

- при необхідності вжити заходів безпеки роботи з цифровими матеріалами;
- у браузері мають бути відключені всі додатки та надбудови, що можуть змінити вигляд вебсторінки, яка оглядається;
- слід підключити і налаштувати всі технічні засоби, які будуть використовуватися під час огляду.

3. Через пошуковий сервіс/додаток (наприклад, «Google», «Telegram Desktop» тощо) шляхом введення у пошукову стрічку запиту здійснити пошук необхідної інформації.

4. Перед початком огляду вебсторінка має бути масштабована у браузері на повний розмір (100%).

5. Огляду та опису підлягають лише ті цифрові матеріали, які мають значення для кримінального провадження.

6. Огляд знайденої вебсторінки здійснюється шляхом безпосереднього сприйняття слідчим розміщеної на ній інформації (візуального та аудіовізуального вираження комп'ютерних даних після їх інтерпретації засобами комп'ютерної техніки).

7. Має бути здійснене повне збереження оглянутої вебсторінки за допомогою будь-якого браузера (Google chrome, Firefox, Opera тощо).

8. У результаті збереження вебсторінки утворюється файл з назвою збереженої сторінки із розширенням «HTML» і папка, в якій містяться автоматично створені файли цієї сторінки.

9. За допомогою інтернет-ресурсів, призначених для архівації файлів (наприклад, «archive.today», «Wayback Machine» тощо), здійснюється архівація потрібної сторінки.

10. Потрібно зробити скрін кожної оглянутої сторінки, який розміщується в протоколі огляду після її опису.

11. Крім основних комп'ютерних даних, криміналістично значущу інформацію можуть містити й так звані метадані (від давньогрец. μετά – після, за межами й англ. data – дані) – додаткова інформація, що характеризує основні дані (файл «контейнер» даних, каталог індексації даних) та зберігається разом з основними даними чи окремо від них. Перелік і зміст метаданих залежать від формату основних даних, операційної системи, типу файлу та програмного забезпечення, з яким файл асоційовано тощо [9].

В операційних системах Microsoft Windows метадані файлу можна відобразити на екрані за кліком по ньому правою кнопкою миші та вибором опції «Властивості». Основними метаданими можна вважати розмір файлу (міра кількості даних, базовою одиницею є байт), назву, розширення назви (наприклад, *.doc, *.exe), назву асоційованого програмного забезпечення, каталог розташування, час створення, час останнього редагування, час останнього відкриття, кількість редакцій, найменування користувача, який створив чи останнім редагував файл тощо [10].

Наведені основні метадані підлягають обов'язковому дослідженню та фіксуванню під час проведення огляду комп'ютерних даних. В окремих випадках дослідженню та фіксуванню також підлягають більш специфічні метадані, притаманні деяким різновидам комп'ютерних файлів. Так, доказове значення можуть мати метадані, характерні для текстових файлів, зображень, аудіо- та відеофайлів, виконуваних файлів тощо [9; 10].

12. За допомогою програмних засобів, які використовуються для вивчення різних метаданих і є у відкритому доступі в мережі «Інтернет», провести аналіз необхідних файлів.

13. Зазначити в протоколі посилання, за яким розміщено «Звіт аналізу метаданих».

14. Перейти за цим посиланням та зробити знімок екрану, на якому відображено звіт аналізу, й розмістити його за змістом у описовій частині протоколу.

15. У разі потреби за допомогою програми «Rapid CRC Unicode 0.3.37.0» провести хешування отриманого файлу з метою отримання хеш-коду (алгоритм sha256).

16. Зробити знімок екрану й розмістити його за змістом у описовій частині протоколу/оформити додатком до протоколу.

17. Скопіювати цифрові матеріали на носій інформації, про що зазначити в протоколі огляду *(доцільно зробити кілька копій збереженої вебсторінки для того, щоб втрата чи пошкодження однієї з них не призвела до втрати матеріалу взагалі.*

18. Цифровий носій інформації, на який було скопійовано оглянуту інформацію, має бути належно упакований, засвідчений підписом слідчого та інших учасників слідчої (розшукової) дії, та використовуватися як додаток до відповідного протоколу.

19. При використанні технічного засобу фіксації СРД, після закінчення її прове-

дення слід відтворити запис за участю всіх учасників слідчої (розшукової) дії, про що зазначити в протоколі огляду.

20. Здійснити фіксування огляду цифрових матеріалів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Басиста І.В., Гаврилюк Л.В., Гутник А.В., Хитра А.Я.* Використання цифрових даних з відкритих джерел під час досудового розслідування кримінальних правопорушень: окремі аспекти. *Науковий вісник Університету Короля Данила.* 2024. Вип. 17 (29). С. 227–243.

2. *Коваленко А.В.* Огляд комп'ютерних даних: сутність і процесуальний порядок проведення. *Вісник Харківського національного університету внутрішніх справ.* 2023. № 3 (102), ч. 2. С. 187–197. DOI: https://doi.org/10.32631/v.2023.3.41.

3. *Коваленко А.В.* Організація і тактика проведення огляду комп'ютерних даних. *Науковий вісник Херсонського державного університету.* 2023. Вип. 4. С. 54. DOI: https://doi.org/10.32999/ksu2307-8049/2023-4-9.

4. *Коваленко А.В.* Особливості проведення огляду вебресурсів як різновиду огляду комп'ютерних даних. *Актуальні питання судової експертології, криміналістики та кримінального процесу:* матеріали V Міжнар. наук.-практ. конф. (м. Київ, 21 груд. 2023 р.) / КНДІСЕ. Київ, 2023. С. 199–202.

5. Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних: практ. посіб. щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О.В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення: 23.05.2024).

6. Слідчі (розшукові) дії та негласні слідчі (розшукові) дії: практика Верховного Суду. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2023_prezent/Prezent_Slidchi_dii.pdf (дата звернення: 23.05.2024).

7. Кримінальний процесуальний кодекс України: затв. Законом України від 13.04.2012 р. № 4651-VI. *Верховна Рада України.* URL: http://zakon3.rada.gov.ua/laws/show/4651-17 (дата звернення: 27.05.2024).

8. Конвенція про кіберзлочинність від 23.11.2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 27.05.2024).

9. *Коваленко А.В.* Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності.* 2023. Вип. 161. С. 202–214. DOI: https: //doi.org/10.21564/2414-990X.161.278117.

10. Криміналістика: криміналістична техніка: навч. посіб. / Р.Л. Степанюк та ін. Харків: ХНУВС, 2023. 388 с.

REFERENCES

1. *Basysta, I.V., Havryliuk, L.V., Hutnyk, A.V. and Khytra, A.Ya.* (2024). Vykorystannia tsyfrovykh danykh z vidkrytykh dzherel pid chas dosudovoho rozsliduvannia kryminalnykh pravoporushen: okremi aspekty. "The use of digital data from open sources during the pre-trial investigation of criminal offenses: some aspects". *Scientific Bulletin of King Danylo University.* Issue 17 (29). P. 227–243. [in Ukrainian].

2. *Kovalenko, A.V.* Ohliad kompiuternykh danykh: sutnist i protsesualnyi poriadok provedennia. "Review of computer data: substance and procedural procedure". *Bulletin of Kharkiv National University of Internal Affairs.* No. 3 (102), part 2. P. 187–197. DOI: https://doi.org/10.32631/v.2023.3.41 [in Ukrainian].

3. *Kovalenko, A.V.* (2023). Orhanizatsiia i taktyka provedennia ohliadu kompiuternykh danykh. "Organization and tactics of computer data review". *Scientific Bulletin of Kherson State University.* Issue 4. P. 54. DOI: https://doi.org/10.32631/v.2023.3.41 [in Ukrainian].

4. *Kovalenko, A.V.* (2023). Osoblyvosti provedennia ohliadu veb-resursiv yak riznovydu ohliadu kompiuternykh danykh. Aktualni pytannia sudovoi ekspertolohii, kryminalistyky ta kryminalnoho protsesu. *"Peculiarities of reviewing web resources as a type of computer data review. Actual issues of forensic expertise, criminology and criminal process"*: materials of the V International science and practice conf. (Kyiv, December 21, 2023) / KNDISE. Kyiv. P. 199–202 [in Ukrainian].

5. Protokol Berkli z vedennia rozsliduvannia z vykorystanniam vidkrytykh tsyfrovykh danykh. "The Berkeley protocol for conducting an investigation using open digital data: a practical guide to the effective use of digital information in the open access for the investigation of violations of international criminal law, human rights and humanitarian law" / non-official. trans. from English O.V. Ziuz, New York; Geneva: Center for Human Rights, University of California, Berkeley, School of Law, United Nations Office of the High Commissioner for Human Rights, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (Date of Application: 23.05.2024) [in Ukrainian].

6. Slidchi (rozshukovi) dii ta nehlasni slidchi (rozshukovi) dii: praktyka Verkhovnoho Sudu. "Investigative (search) actions and covert investigative (search) actions: the practice of the Supreme Court". URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2023_prezent/Prezent_Slidchi_dii.pdf URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2023_prezent/Prezent_Slidchi_dii.pdf (Date of Application: 23.05.2024) [in Ukrainian].

7. Kryminalnyi protsesualnyi kodeks Ukrainy. "Criminal Procedure Code of Ukraine": approved by the Law of Ukraine dated April 13, 2012 No. 4651-VI. *Verkhovna Rada of Ukraine.* URL: http://zakon3.rada.gov.ua/laws/show/4651-17 (Date of Application: 27.05.2024) [in Ukrainian].

8. Konventsia pro kiberzlochynnist. "Convention on cybercrime" dated November 23, 2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (Date of Application: 27.05.2024) [in Ukrainian].

9. Kovalenko, A.V. (2023). Klasyfikatsiia elektronnykh (tsyfrovykh) slidiv kryminalnoho pravoporushennia. Problemy zakonnosti. "Classification of electronic (digital) traces of a criminal offence". Problems of legality. Iss. 161. P. 202–214. DOI: https://doi.org/10.21564/2414-990X.161.278117 [in Ukrainian].

10. Kryminalistyka: kryminalistychna tekhnika. "Forensic science: forensic technique": ed. manual / R.L. Stepaniuk et al. Kharkiv: KhNUVS, 2023. 388 p. [in Ukrainian].

ISSN 2072-8670 (Print) **НАУКА І ПРАВООХОРОНА**
NAUKA I PRAVOOKHORONA

DOI (Issue): https://doi.org/10.36486/np.2024.2(64) **Issue 2(64) 2024**

UDC 343.14:004.738.5

Havryliuk Liudmyla,
Candidate of Juridical Sciences, Senior Researcher,
Head of the Department, State Research Institute MIA Ukraine,
Kyiv, Ukraine,
ORCID ID 0000-0002-9441-4073
Burlaka Vladyslav,
Candidate of Juridical Sciences,
Head of the Department, Main Investigative Department of the
National Police of Ukraine,
Kyiv, Ukraine,
ORCID ID 0000-0003-1824-4380
Pelekhatyi Vitalii,
Senior investigator in
the Office of the Main Investigative
Department of the National Police of Ukraine, Kyiv, Ukraine

SPECIAL FEATURES OF THE BERKELEY PROTOCOL FOR REVIEWING OPEN SOURCE DIGITAL MATERIALS ON THE "INTERNET"

The article is devoted to clarifying the essence of reviewing digital materials from open sources of the "Internet" in criminal proceedings. Based on the analysis of the provisions of the Criminal Procedure Code (CPC) of Ukraine regarding the review of computer data, the author states that the provisions of the CPC of Ukraine provide for: review of computer data as a means of identifying and recording information pertaining to the circumstances of a criminal offence; investigator, inquirer, prosecutor, employee of an operational unit acting on behalf of the investigator, and authorised subjects for the review of computer data; the option for investigators or prosecutors to engage a specialist to assist in matters requiring specialised knowledge, such as the review of computer data and the provision of technical assistance during the conduct of investigative actions; the copying of information, including computer data, contained in information systems, electronic communication systems, or information and communication systems, by an investigator or prosecutor with the obligatory involvement of a specialist (which is a condition for their recognition by the court as an original document); form of display of information contained in computer data, which must be suitable for perception of their content; the possibility of using electronic means, photography, video recording, screen recording and/or video recording, etc. or in paper form as a way of recording computer data. It is stated that the essence of investigative and search actions of inspection as one of the ways to identify and record information regarding the circumstances of a criminal offence and the content of the Second Paragraph of Part 2 of Article 237 of the CPC of Ukraine indicate that "during the inspection of computer data, authorized persons must personally perceive the content of the audiovisual expression of computer data and reflect it in the protocol of procedural action and its annexes in a form suitable for perception of such content by other

DOI (Article): https://doi.org/10.36486/np.2024.2(64).21

people. For direct human perception, computer data containing text, images, sounds and other audiovisual forms of information can be reproduced through data output devices (screen, audio devices, printers, etc.), and code containing action algorithms can be executed (run a program)". The article emphasises the importance of meticulous preparation for the review of digital materials sourced from open Internet resources. The authors puts forth a procedure for investigators to follow when reviewing digital materials from open sources.

Keywords: criminal proceedings, pre-trial investigation, proving, evidence, investigator, inspection, computer data, digital information, digital materials from open sources, (electronic) digital evidence, digital data, open sources of digital information, Burkley Protocol.

Отримано 04.06.2024