УДК 004.08:343.98
DOI https://doi.org/10.32999/ksu2307-8049/2023-4-9

ОРГАНІЗАЦІЯ І ТАКТИКА ПРОВЕДЕННЯ ОГЛЯДУ КОМП'ЮТЕРНИХ ДАНИХ

Коваленко Артем Володимирович,
кандидат юридичних наук, доцент,
професор кафедри правосуддя
Луганського навчально-наукового інституту імені Е.О. Дідоренка
Донецький державний університет внутрішніх справ
new4or@gmail.com
orcid.org/0000-0003-3665-0147

Мета. *Стаття присвячена формулюванню практично орієнтованих рекомендацій щодо організації та тактики проведення огляду комп'ютерних даних у кримінальному провадженні. Під час здійснення дослідження використано* **методи** *аналізу, синтезу, моделювання, прогнозування, формально-логічний, формально-юридичний.*

Результати. *Зазначено, що огляд комп'ютерних даних через специфіку об'єкта й особливості процесуального порядку потребує окремого комплексу тактичних рекомендацій щодо організації і тактики його проведення. Ці тактичні рекомендації мають бути спрямовані на підвищення ефективності діяльності уповноважених осіб під час здійснення такої процесуальної дії. Автор наголошує, що в межах підготовки до проведення огляду комп'ютерних даних доцільно попередньо з'ясувати, з якими пристроями та типами даних доведеться працювати, забезпечити участь спеціалістів і наявність необхідних технічних засобів. Установлено, що сутність огляду комп'ютерних даних полягає в безпосередньому сприйнятті та фіксуванні уповноваженими особами аудіовізуального виразу змісту комп'ютерних даних після їх інтерпретації засобами комп'ютерної техніки та відтворення через пристрої виведення даних. Визначено, що основною й обов'язковою формою фіксування перебігу та результатів огляду комп'ютерних даних є протокол, до описової частини якого доцільно заносити детальний опис дій уповноважених осіб і зміст досліджених комп'ютерних даних. Автор рекомендує додавати до протоколу носії з повними копіями досліджених даних, відеозаписами екрана пристрою, за допомогою якого проводився огляд, роздруківки досліджених даних, друковані фототаблиці тощо як невід'ємні додатки.*

Висновки. *Огляд комп'ютерних даних є одним з основних передбачених чинним Кримінальним процесуальним кодексом України засобів збирання та дослідження електронних (цифрових) доказів (електронних документів) під час досудового розслідування кримінальних правопорушень, ефективність його проведення залежить, зокрема, від наявності відповідних практично орієнтованих тактико-криміналістичних рекомендацій.*

Ключові слова: *кримінальне провадження, огляд, комп'ютерні дані, тактика, збирання доказів, дослідження доказів.*

ORGANIZATION AND TACTICS OF COMPUTER DATA INSPECTION

Kovalenko Artem Volodymyrovych,
Candidate of Juridical Sciences, Associate Professor,
Professor at the Department of Justice
Luhansk Educational and Scientific Institute named after E.O. Didorenko
Donetsk State University of Internal Affairs
new4or@gmail.com
orcid.org/0000-0003-3665-0147

Purpose. *The article is devoted to the formulation of practically oriented recommendations regarding the organization and tactics of computer data inspection in criminal proceedings. During the research,* **methods** *of analysis, synthesis, modeling, forecasting, formal-logical, formal-legal were used.*

Results. *It is noted that the inspection of computer data requires a separate set of tactical recommendations regarding the organization and tactics of its implementation due to the specificity of the object and the peculiarities of the procedural order. Such tactical recommendations should be aimed at improving the efficiency of the activities of authorized persons during the conduction of such a procedural action. The author emphasizes that as part of the preparation for conducting an inspection of computer data, it is advisable to first find out what devices and types of data will be inspected, to ensure the participation of specialists and check the availability of the necessary technical means. It was established that the essence of computer data inspection consists in the direct perception and recording by authorized persons of the audiovisual expression of the content of computer data after their interpretation by means of computer equipment*

and reproduction through data output devices. It was determined that the main and mandatory form of recording the progress and results of the inspection of computer data is a protocol, in the descriptive part of which it is advisable to enter a detailed description of the actions of authorized persons and the content of the examined computer data. The author recommends adding media with full copies of the researched data, video recordings of the screen of the device used for the inspection, printouts of the examined data, printed photo tables, etc. as integral appendices to the protocol.

Conclusions. *Inspection of computer data is one of the main means of collecting and examining electronic (digital) evidence (electronic documents) during pre-trial investigation of criminal offenses provided for by the current Code of Criminal Procedure of Ukraine, and the effectiveness of its conduct depends, in particular, on the availability of relevant practically-oriented tactical forensic recommendations.*

Key words: *criminal proceedings, inspection, computer data, tactics, collection of evidence, examination of evidence.*

Вступ. У кримінальному провадженні огляд є одним з основних процесуальних засобів збирання доказів. Дана 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 з поступальним рухом науково-технічного прогресу та розповсюдженням комп'ютерної техніки все частіше постає потреба в межах кримінального провадження дослідити зміст інформації, що міститься в пам'яті таких пристроїв чи обробляється ними. З ухваленням Закону України № 2137–IX від 15 березня 2022 р. «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» (Про внесення змін) така інформація дістала назву «комп'ютерні дані», а процедура її вилучення, фіксування й оперативного дослідження стала новим легально визначеним різновидом огляду – оглядом комп'ютерних даних.

Криміналістичні рекомендації щодо тактики огляду комп'ютерної техніки й інформації, що міститься в її пам'яті, у своїх працях розробляли П. Є. Антонюк, А. В. Гутник, М. В. Гуцалюк, О. В. Захарова, А. В. Коваленко, В. В. Коваленко, С. О. Корона, О. В. Манжай, В. В. Носов, О. В. Одерій, О. А. Самойленко, С. В. Самойлов, В. Г. Хахановський, А. Я. Хитра, М. Г. Щербаковський та інші вчені-криміналісти. Але огляд комп'ютерних даних як слідча (розшукова) дія є новелою вітчизняного кримінального процесуального законодавства і ще не набув належного теоретичного опрацювання та сталої практики застосування. Через це правоохоронці потребують тактико-криміналістичних рекомендацій щодо організації та проведення згаданої слідчої (розшукової) дії.

Тому **метою** статті є формулювання практично орієнтованих рекомендацій щодо організації та тактики проведення огляду комп'ютерних даних у кримінальному провадженні.

1. Сутність і зміст тактичних рекомендацій щодо огляду комп'ютерних даних

Під тактикою огляду К. О. Чаплинський розуміє комплекс найбільш раціональних і ефективних дій або найдоцільнішу лінію поведінки уповноважених осіб, що забезпечує виявлення максимальної кількості слідів кримінального правопорушення та речових доказів, інформації про досліджувану подію (Чаплинський, 2011: 25). Погоджуємося із цитованим науковцем, що рекомендації тактико-криміналістичного характеру мають бути спрямовані саме на забезпечення максимально ефективної поведінки уповноважених осіб під час проведення слідчих (розшукових) та інших процесуальних дій.

Зазвичай тактичні рекомендації щодо проведення слідчих (розшукових) дій, зокрема й огляду, фокусуються на алгоритмах дій уповноважених осіб у найбільш типових ситуаціях під час підготовки, проведення та фіксування результатів відповідної процесуальної дії. Видається, що частина «традиційних» тактичних рекомендацій щодо проведення огляду матеріальних об'єктів може бути безпосередньо адаптована до огляду комп'ютерних даних (зокрема, аспекти підготовки до проведення, загальні алгоритми підбору та залучення спеціалістів тощо). Водночас специфіка об'єкта огляду (нематеріальні комп'ютерні дані), визначені Кримінальним процесуальним кодексом (далі – КПК) України вимоги до процесуального порядку його проведення дають підстави до формулювання окремого комплексу тактичних рекомендацій щодо проведення даної процесуальної дії.

Огляд комп'ютерних даних можна визначити як гласну слідчу (розшукову) дію, що проводиться стороною обвинувачення з використанням електронно-обчислювальної техніки шляхом безпосереднього сприйняття аудіовізуального виразу комп'ютерних даних із метою отримання відомостей про факти, що мають значення для кримінального провадження. Згадана слідча (розшукова) дія є одним з основних засобів збирання та дослідження електронних (цифрових) доказів (електронних документів) під час досудового розслідування, а рекомендації щодо організації і тактики її проведення – важливою складовою частиною криміналістичного вчення про збирання, дослідження та використання доказів у кримінальному провадженні.

Варто зазначити, що з метою формулювання тактичних рекомендацій ми розмежовуємо огляди комп'ютерних даних і комп'ютерної техніки, які можуть проводитися як водночас, так і окремо. У разі їх одночасного проведення огляд комп'ютерних даних варто вважати самостійною складовою частиною огляду комп'ютерної техніки, яка має власний об'єкт, завдання та закономірності. У разі одночасного проведення названих

процесуальних дій практикам доцільно орієнтуватися, зокрема, і на особливості тактики огляду самої техніки, які були неодноразово докладно викладені у працях вітчизняних науковців. Тому в межах даного дослідження ми сконцентруємося на загальних засадах дослідження комп'ютерних даних, що містяться на вилученому носії, були скопійовані на спеціально підготований носій чи є публічно доступними в інтернеті.

2. Підготовка до проведення огляду комп'ютерних даних

Підготовчі дії до проведення огляду комп'ютерних даних мають починатися з попередньої розвідки. Уповноваженій особі доцільно ознайомитися з раніше сформованими матеріалами кримінального провадження, з'ясувати, які пристрої чи носії даних будуть оглядатись, які типи файлів можуть бути виявлені під час огляду, які відомості можуть нести оглядувані дані.

Незамінною складовою частиною підготовки до проведення будь-якої слідчої (розшукової) дії є визначення складу її учасників. Зокрема, до огляду комп'ютерних даних як спеціалістів доцільно залучати судових експертів, уповноважених на проведення комп'ютерно-технічних експертиз. За їх відсутності надавати технічну допомогу під час проведення такої процесуальної дії можуть особи, які мають комп'ютерно-технічну, комп'ютерно-інженерну освіту та досвід роботи з комп'ютерно-технічними засобами та програмними продуктами. За наявності необхідних знань і технічних навичок огляд комп'ютерних даних може проводитися слідчим (дізнавачем, детективом), прокурором, оперативним співробітником самостійно, без залучення спеціалістів. Коли огляд комп'ютерних даних поєднаний з оглядом комп'ютерної техніки, до його проведення доцільно також залучити спеціаліста-криміналіста з метою виявлення та фіксування матеріально-фіксованих слідів кримінального правопорушення на таких пристроях і в місцях їх розташування.

До технічних засобів, необхідних для проведення огляду комп'ютерної техніки й огляду комп'ютерних даних, дослідники відносять портативний комп'ютер з автономним джерелом живлення; комплекти запасних батарей; привод CD-ROM (DVD-ROM); диски з операційними системами й іншими програмними засобами, накопичувачі інформації, зокрема носій ємністю, більшою від ємності накопичувача, який підлягає огляду; блокувач жорсткого диска та/або набір дублікаторів; викрутки й інші інструменти; польовий комплект спеціаліста-криміналіста тощо (Вінаков та ін., 2017: 103–104). Підготовка відповідних технічних засобів покладається на залученого спеціаліста або уповноважену особу, яка проводить огляд комп'ютерних даних самостійно.

3. Робоча стадія огляду комп'ютерних даних

У межах робочої стадії згаданої слідчої (розшукової) дії уповноважені особи мають ознайомитись зі змістом комп'ютерних даних і вжити заходів до їх фіксування (збереження) у формі, доступній для сприйняття людиною.

Огляд комп'ютерних даних, що були скопійовані правоохоронцями на окремі носії або вилучені разом з оригінальними носіями, здійснюється шляхом підключення такого носія до службового комп'ютера, відкриття (виконання) файлів засобами асоційованого програмного забезпечення та безпосереднього сприйняття уповноваженою особою інформації, яку несуть такі дані. Варто пам'ятати, що вилучені носії комп'ютерних даних можуть містити шкідливий код (так звані «віруси»). Для убезпечення робочого комп'ютера та збереження досліджуваних даних від видалення антивірусними програмами огляд даних доцільно здійснювати з використанням так званих «віртуальних машин» (Степанюк та ін., 2023: 124). Окрім того, особа, яка проводить огляд (або залучений спеціаліст), має вжити заходів для недопущення внесення змін до оглядуваних даних під час їх дослідження.

Дані, що містяться в інтернеті у відкритому доступі (на вебсайтах), оглядаються з використанням службового комп'ютера з доступом до інтернету та програмного забезпечення веббраузера. Комп'ютерні дані, що містяться на публічних ресурсах у межах сторінок, груп, пабліків у месенджерах (Telegram, Viber, WhatsApp, Signal, WeChat тощо) можуть бути оглянуті з використанням вебверсії відповідного месенджера засобами програми веббраузера, а за відсутності вебверсії – з використанням програми-клієнта такого месенджера.

Укотре наголосимо, що будь-які дії з комп'ютерними даними мають здійснюватися уповноваженими особами суто за допомогою сертифікованого та справного службового обладнання, з використанням ліцензійного програмного забезпечення. Використання несертифікованого, несправного обладнання або неліцензійного програмного забезпечення може призвести до викривлення інформації, отриманої з комп'ютерних даних, через апаратні та/або програмні збої та помилки (Коваленко, 2017: 184). Коли досліджуваний носій комп'ютерних даних захищений чи зашифрований і в разі, якщо в залученого спеціаліста відсутні технічні можливості дослідити його вміст (наприклад, відсутній необхідний інтерфейс підключення або програмне забезпечення), носій може бути направлений для дослідження в межах судової експертизи комп'ютерної техніки та програмних продуктів.

Дані, що не можуть бути скопійовані (наприклад, переписки в месенджерах), оглядаються з використанням пристрою, у пам'яті якого вони містяться. Для фіксування таких даних доцільно здійснювати безперервну відеофіксацію екрана пристрою. Водночас прилади, що можуть під'єднуватися до телекомунікаційних та інтернет-мереж (мобільні телефони, смартфони, ноутбуки, «розумна» побутова техніка, мережеве обладнання тощо), мають оглядатися в умовах, що унеможливлюють підключення та віддалений доступ до них (наприклад, після переведення пристрою в режим «польоту» чи з використанням клітки Фарадея).

О. В. Манжай слушно наводить загальний порядок виявлення та дослідження комп'ютерних даних, що зберігаються на носіях: 1) аналіз доступних (відкритих) файлів шляхом контекстуального пошуку за ключовими фразами; 2) пошук прихованих і зашифрованих, тимчасових, специфічних даних; 3) спроба відновлення видалених файлів (Манжай, 2016: 118).

Виявлення електронних (цифрових) слідів кримінального правопорушення під час огляду комп'ютерних даних, що містяться на носієві, може здійснюватися шляхом пошуку необхідних даних за реквізитами (контекстом) засобами операційної системи чи сторонніх програм, а також шляхом суцільного дослідження файлів. Деякі файли можуть бути прихованими, для їх виявлення потрібно увімкнути відображення прихованих файлів у налаштуваннях програми-файлового менеджера (Степанюк та ін., 2023: 124). Щодо спроб виявлення та відновлення видалених файлів, то традиційно такі операції відносять до завдань експертизи комп'ютерної техніки та програмних продуктів (Теплицький, 2019: 27), отже, є складовою частиною експертного дослідження комп'ютерних даних. Водночас виконання таких дій можливе й у межах оперативного дослідження комп'ютерних даних під час їх огляду із залученням спеціаліста.

Комп'ютерні дані за своїм визначенням є інформацією, що була зашифрована для обробки логічними процесорами комп'ютерної техніки і, відповідно, в оригінальному вигляді не може бути сприйнята органами відчуття людини. Тому безпосередньому дослідженню уповноваженими особами підлягає візуальний і аудіовізуальний вираз комп'ютерних даних після їх інтерпретації засобами комп'ютерної техніки. Сутність огляду як засобу збирання та дослідження доказів та вимоги абз. 2 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 людиною 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). Кожний досліджений файл (якщо він містить інформацію, яка має значення для кримінального провадження) рекомендується зберігати та фіксувати у протоколі одразу після його дослідження, що дещо розмиває межі робочої та заключної стадій такого огляду.

Окрім основних комп'ютерних даних, криміналістично значущу інформацію можуть нести 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 (Коваленко, 2023: 207). 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 (Степанюк та ін., 2023: 115). Перелічені 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, що притаманні деяким різновидам комп'ютерних файлів. Так, доказове значення можуть мати метадані, характерні для текстових файлів, зображень, аудіо- та відеофайлів, виконуваних файлів тощо.

4. Фіксування огляду комп'ютерних даних

Ключовою складовою частиною огляду комп'ютерних даних є належне фіксування перебігу та результатів його проведення. Виходячи зі змісту ст. 104, абз. 2 ч. 2 ст. 237 КПК України, основною й обов'язковою формою фіксування такої слідчої (розшукової) дії (далі – С(Р)Д) є протоколювання.

У вступній частині відповідного протоколу з урахуванням вимог ч. 3 ст. 104 КПК України доцільно зазначати відомості про місце, час проведення огляду, уповноважену особу, яка його проводить, усіх присутніх осіб, зокрема й залучених спеціалістів, застосовані технічні засоби фіксації, їхні технічні характеристики та використані носії інформації, відомості щодо повідомлення учасників С(Р)Д про застосування технічних засобів. Наприклад, коли здійснюється безперервне відеофіксування екрана електронно-обчислювального пристрою, за допомогою якого оглядаються комп'ютерні дані, у вступній частині протоколу має бути вказано модель і серійний номер використаної камери або назву та версію програмного забезпечення для захоплення зображення з екрана. Окрім того, у даній частині протоколу рекомендується указувати відомості про технічні характеристики та серійні номери обладнання, назви та версії програмного забезпечення, що використовувались уповноваженими особами під час огляду.

До описової частини протоколу огляду комп'ютерних даних доцільно занести детальний опис дій/операцій уповноважених осіб і спеціалістів із комп'ютерною технікою та результати таких дій. Окрім того, відповідно до вимог абз. 2 ч. 2 ст. 237 КПК України, до названої частини протоколу має бути занесена інформація, яку містять оглянуті електроні дані, у формі, придатній для сприйняття їхнього змісту людиною (тобто у візуальній формі, тоді як аудіовізуаль-

ний вираз цієї інформації може міститися на комп'ютерних носіях серед додатків до протоколу). Законодавець пропонує фіксувати таку інформацію за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо, або в паперовій формі. Уважаємо, що в даній частині протоколу доцільно відображати не абсолютно всю досліджену інформацію, а тільки ті дані, які, на думку уповноваженої особи, мають значення для кримінального провадження та можуть використовуватись у доказуванні. Водночас повні копії досліджених даних (зокрема, для їх повторного чи судового дослідження) мають міститися на носії комп'ютерних даних серед додатків до протоколу.

До текстової складової частини описової частини протоколу можна заносити витримки, розшифровки, текстові описи ключових моментів аудіо- та відеофайлів; для відеофайлів також скріншоти[1] стопкадрів ключових моментів, на яких відображено події, місця, речі чи осіб, відомості про які мають значення для кримінального провадження. Витримки та стопкадри мають подаватися з указівкою на таймкод (часову відмітку, той момент відео- чи аудіозапису, коли відбулась подія), назву файлу та каталог його розміщення на носії. Таймкоди дозволять уповноваженим особам надалі, під час повторного огляду чи дослідження в судовому провадженні, швидко перейти до ключових моментів аудіо-, відеозапису та не витрачати час на їх повне відтворення. У межах дослідження текстових електронних документів, комп'ютерного коду до описової частини протоколу можуть заноситися виписки (цитати) ключових моментів або весь текстовий зміст даних. За результатами дослідження зображень, вебсторінок до протоколу рекомендується заносити скріншоти відповідних даних і їх текстові описи. Під час дослідження комп'ютерних програм (виконуваних файлів) фіксуванню підлягають основні елементи інтерфейсу програми, виконані користувачем (уповноваженою особою) дії та отримані від програми результати таких дій.

У заключній частині протоколу огляду комп'ютерних даних доцільно з урахуванням вимог п. 3 ч. 3 ст. 104 КПК України вказувати на виготовлені копії комп'ютерних даних, спосіб їх виготовлення, використані технічні засоби, носії даних і способи їх упакування й ідентифікації, залученого до цієї процедури фахівця, а також спосіб ознайомлення учасників протоколу з його змістом та, за наявності, зауваження й доповнення до нього.

Основною формою додатка до протоколу огляду комп'ютерних даних є носії комп'ютерних даних (CD-, DVD-диски, флеш-диски, HDD-накопичувачі тощо), на які уповноваженими особами за участі спеціаліста було поміщено копії (дублікати) досліджених даних. Таким способом можуть бути збережені фото-, відео- й аудіофайли, вебсторінки й інші типи оглянутих комп'ютерних даних. За результатами огляду даних, що містяться на оригінальному носієві, доцільно створювати як мінімум два носії з копіями даних: на першому має міститися повна незмінна копія всіх даних (наприклад, побітна копія чи образ носія, на якому вони містилися). Цілком слушною є пропозиція І. Г. Каланчі й А. М. Гаркуші щодо обов'язкового застосування вимог ДСТУ ISO/IEC 27037:2017 та підтвердження цілісності та справжності скопійованих даних шляхом гешування первинної інформації та її копій із подальшим порівнянням геш-значень (Каланча, Гаркуша, 2021: 338). На другому носії доцільно розмістити копії лише тих даних, що мають безпосереднє значення для кримінального провадження, скріншоти та записи екрана, виготовлені під час огляду тощо.

Текстові документи, а також зображення, що оглядались, можуть бути роздрукувані за допомогою службового принтера та додані до протоколу огляду як невід'ємні додатки. Окрім того, доцільним може бути створення друкованих фототаблиць, що містять скріншоти ключових елементів досліджених комп'ютерних даних. Виготовлення такого додатка допоможе додатково проілюструвати основну частину протоколу та дозволить ознайомитись зі змістом оглянутих даних без використання комп'ютерної техніки.

Висновки. Отже, огляд комп'ютерних даних є одним з основних передбачених чинним КПК України засобів збирання та дослідження електронних (цифрових) доказів (електронних документів) під час досудового розслідування кримінальних правопорушень. Ефективність проведення такої слідчої (розшукової) дії залежить, серед іншого, і від наявності відповідних практично орієнтованих тактико-криміналістичних рекомендацій.

У межах підготовки до проведення названої слідчої (розшукової) дії уповноваженим особам доцільно здійснити попередню розвідку та з'ясувати, з якими комп'ютерно-технічними засобами та типами даних доведеться працювати; забезпечити участь у процесуальній дії як спеціаліста судового експерта, уповноваженого на проведення комп'ютерно-технічних експертиз, або іншого носія спеціальних комп'ютерно-технічних знань; переконатись у наявності у фахівця або самостійно забезпечити наявність необхідних технічних засобів. У межах робочої стадії огляду комп'ютерних даних уповноважені особи мають ознайомитись зі змістом комп'ютерних даних і вжити заходів до їх збереження у формі, доступній до сприйняття людиною. Так, огляд комп'ютерних даних, що були скопійовані на окремі носії, вилучені разом з оригінальними носіями, чи ті, що містяться в інтернеті, здійснюється з використанням службового комп'ютера; огляд даних, що не можуть бути скопійовані – з використанням пристрою, у пам'яті якого вони містяться. Безпосередньому дослідженню уповноваженими особами підлягає візуальний і аудіовізуальний вираз комп'ютерних даних після їх інтерпретації засобами комп'ютерної техніки та відтворення через пристрої виведення даних. Основною формою фіксування перебігу та результатів огляду комп'ютерних даних є протокол, до описової частини якого заноситься детальний опис дій уповноважених

[1] Від англ. *screenshot* – знімок екрана, український неологічний відповідник – *зняток*.

осіб і зміст досліджених комп'ютерних даних. Додатками до протоколу такої процесуальної дії можуть бути носії комп'ютерних даних із повними копіями досліджених даних, відеозаписами екрана пристрою, за допомогою якого проводився огляд, роздруківки досліджених даних, друковані фототаблиці тощо.

Перспективним видається здійснення класифікації огляду комп'ютерних даних на підвиди за тактико-значущими критеріями та розроблення рекомендацій щодо організації та проведення різновидів такої процесуальної дії.

ЛІТЕРАТУРА

1. 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 : Закон України від 15.03.2022 р. № 2137–IX / Верховна Рада України. *База «Законодавство України»*. URL: https://zakon.rada.gov.ua/laws/show/2137-20 (дата звернення: 23.08.2023).

2. Чаплинський К.О. Організаційно-тактичні основи проведення слідчого огляду. *Криміналістичний вісник*. 2011. № 1 (15). С. 22–29.

3. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій : навчальний курс / А.В. Вінаков та ін. Київ, 2017. 148 с.

4. Криміналістика: криміналістична техніка : навчальний посібник / Р.Л. Степанюк та ін. Харків : ХНУВС, 2023. 388 с.

5. Коваленко А.В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналістів. *Вісник Національної академії правових наук України :* збірник наукових праць. 2017. № 1 (88). С. 182–191.

6. Манжай О.В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. № 3 (74). С. 111–120.

7. Теплицький Б.Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 2 (18). С. 24–32.

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

9. Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*. 2021. № 8. С. 336–339. DOI: 10.32782/2524-0374/2021-8/77.

REFERENCES

1. Pro vnesennia zmin do Kryminalnoho protsesualnoho kodeksu Ukrainy ta Zakonu Ukrainy "Pro elektronni komunikatsii" shchodo pidvyshchennia efektyvnosti dosudovoho ... [On making changes to the Criminal Procedure Code of Ukraine and the Law of Ukraine "On Electronic Communications" to increase the effectiveness of pre-trial …]: Zakon Ukrainy vid 15.03.2022 № 2137–IX / Verkhovna Rada Ukrainy. *Baza "Zakonodavstvo Ukrainy"*. URL: https://zakon.rada.gov.ua/laws/show/2137-20 [in Ukrainian].

2. Chaplynskyi, K.O. (2011). Orhanizatsiino-taktychni osnovy provedennia slidchoho ohliadu [Organizational and tactical foundations of investigative review]. *Kryminalistychnyi visnyk – Forensic Herald*, № 1(15), pp. 22–29 [in Ukrainian].

3. Vinakov, A.V. et al. (2017). Vyiavlennia, poperedzhennia ta rozsliduvannia zlochyniv torhivli liudmy, vchynenykh iz zastosuvanniam informatsiinykh tekhnolohii: navchalnyi kurs [Detection, prevention and investigation of human trafficking crimes committed with the use of information technologies: training course]. Kyiv, 148 p. [in Ukrainian].

4. Stepaniuk, R.L. et al. (2023). Kryminalistyka: kryminalistychna tekhnika : navch. posib. [Forensic science: forensic technique: teaching manual]. Kharkiv: KhNUVS, 388 p. [in Ukrainian].

5. Kovalenko, A.V. (2017). Osoblyvosti taktyky ohliadu elektronnykh dokumentiv pid chas dosudovoho rozsliduvannia posiahan na zhyttia ta zdorovia zhurnalistiv [Peculiarities of the tactics of inspection of electronic documents during the pre-trial investigation of attacks on the life and health of journalists]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy – Bulletin of the National Academy of Legal Sciences of Ukraine*, № 1 (88), pp. 182–191 [in Ukrainian].

6. Manzhai, O.V. (2016). Osoblyvosti ohliadu zasobiv komp'iuternoi tekhniky [Peculiarities of inspection of computer equipment]. *Visnyk KhNUVS – Herald of KhNUVS,* № 3(74), pp. 111–120 [in Ukrainian].

7. Teplytskyi, B.B. (2019). Zavdannia, obiekty ta pytannia komp'iuterno-tekhnichnoi sudovoi ekspertyzy [Tasks, objects and issues of computer-technical forensic examination]. *Yurydychnyi chasopys Natsionalnoi akademii vnutrishnikh sprav – Legal journal of the National Academy of Internal Affairs*, № 2 (18), pp. 24–32.

8. Kovalenko, A.V. (2023). Klasyfikatsiia elektronnykh (tsyfrovykh) slidiv kryminalnoho pravoporushennia [Classification of electronic (digital) traces of a criminal offense]. *Problemy zakonnosti – Problems of legality*, iss. 161, pp. 202–214. DOI: 10.21564/2414-990X.161.278117.

9. Kalancha, I.H. & Harkusha, A.M. (2021). Kopiia elektronnoi informatsii yak dokaz u kryminalnomu provadzhenni: protsesualnyi ta tekhnichnyi aspekty [Copy of electronic information as evidence in criminal proceedings: procedural and technical aspects]. *Yurydychnyi naukovyi elektronnyi zhurnal – Legal scientific electronic journal*, № 8, pp. 336–339. DOI: 10.32782/2524-0374/2021-8/77.

Стаття надійшла до редакції 04.09.2023.
The article was received 4 September 2023.