УДК 343.98
DOI https://doi.org/10.32844/2618-1258.2025.4.32

ДРОЗД В.Ю.

ОГЛЯД КОМП'ЮТЕРНИХ ДАНИХ ПІД ЧАС РОЗСЛІДУВАННЯ КОРУПЦІЙНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ ПРАЦІВНИКАМИ ПРАВООХОРОННИХ ОРГАНІВ

REVIEW OF COMPUTER DATA DURING THE INVESTIGATION OF CORRUPTION CRIMINAL OFFENSES COMMITTED BY LAW ENFORCEMENT OFFICIALS

У статті комплексно досліджено процесуальні й криміналістичні особливості огляду комп'ютерних даних під час розслідування корупційних кримінальних правопорушень, учинених працівниками правоохоронних органів. З огляду на складність досліджуваних кримінальних правопорушень, саме електронні джерела інформації дозволяють реконструювати алгоритм незаконних дій, визначити спосіб маскування неправомірної діяльності, встановити роль кожного учасника та підтвердити його причетність до протиправної поведінки. У цьому контексті огляд комп'ютерних даних є вкрай важливою слідчою (розшуковою) дією, яка потребує чіткої організації, спеціальних технічних знань і відповідного криміналістичного забезпечення.

Підкреслено, що сучасні носії електронної інформації характеризуються різноманіттям форматів, великою швидкістю оновлення даних, нестабільністю частини цифрової інформації, а також високою вразливістю до модифікації. Саме тому своєчасність і правильність дій слідчого, а також здатність компетентних осіб забезпечити цілісність даних, є ключовою умовою збереження доказового значення інформації.

У статті проаналізовано нормативне підґрунтя проведення огляду комп'ютерних даних, визначене ст. 99 та ст. 237 КПК України. Наголошено, що закон розглядає комп'ютерні дані як різновид документів, що надає слідчому право оглядати їх у загальному порядку, а результати огляду – фіксувати у протоколі з використанням додаткових засобів фіксації.

Значну увагу приділено питанню залучення спеціаліста під час огляду комп'ютерної техніки і комп'ютерних даних. У статті звертається увага на різні рівні доступу до даних: локальний (безпосереднє підключення до пристрою) і віддалений (доступ через мережу, хмарні сервіси, вебінтерфейси).

Автором підкреслено, що значна частина цифрової інформації, яка має криміналістичне значення, залишається невидимою для користувача і потребує спеціальних методів виявлення. Стаття приділяє увагу також важливості фіксації аудіовізуального виразу комп'ютерних даних – тобто інформації, яку пристрій відображає на моніторі чи відтворює у вигляді звуку або зображення.

Ключові слова: *цифрові докази, комп'ютерні дані, огляд комп'ютерних даних, корупційні правопорушення, працівники правоохоронних органів, криміналістичні сліди, цифрова криміналістика.*

The article comprehensively investigates the forensic, tactical and procedural features of the review of computer data during the investigation of corruption criminal offenses committed by law enforcement officers. Given the complexity of corruption-

© ДРОЗД В.Ю. – кандидат юридичних наук, науковий співробітник науково-дослідної лабораторії з проблем запобігання кримінальним правопорушенням факультету № 3 (Донецький державний університет внутрішніх справ) https://orcid.org/0000-0002-3872-8879

related criminal offenses committed by law enforcement officers, it is electronic data that often allows us to reconstruct the algorithm of illegal actions, determine the method of masking illegal activities, establish the role of each participant and confirm their involvement in illegal behavior. In this context, the review of computer data is an extremely important investigative (search) action that requires a clear organization, special technical knowledge and appropriate procedural support.

The work emphasizes that modern electronic information carriers are characterized by a variety of formats, a high speed of data update, instability of some digital information, as well as high vulnerability to modification. That is why the timeliness and correctness of the investigator's actions, as well as the ability of authorized persons to ensure data integrity, are a key condition for preserving the evidentiary value of information.

The article analyzes the regulatory basis for conducting a review of computer data, defined in Art. 237 and Art. 99 of the Code of Criminal Procedure of Ukraine. It is emphasized that the law considers computer data as a type of document, which gives the investigator the right to inspect them in a general manner, and to record the results of the inspection in a protocol using electronic recording devices.

Considerable attention is paid to the issue of involving a specialist during the inspection of computer equipment and computer data. The article draws attention to different levels of access to data: local (direct connection to the device) and remote (access via the network, cloud services, web interfaces).

The author emphasizes that a significant part of digital information that has forensic significance remains invisible to the user and requires special detection methods. The article also pays attention to the importance of recording the audiovisual expression of computer data – that is, information that the device displays on the monitor or reproduces in the form of sound or image.

Key words: *digital evidence, computer data, computer data inspection, corruption offenses, law enforcement officers, forensic traces, digital forensics.*

Постановка проблеми. Цифровізація суспільства кардинально змінила криміналістичні підходи до фіксації доказів. При розслідуванні корупційних кримінальних правопорушень, вчинених працівниками правоохоронних органів, електронні (цифрові) сліди є ключовим джерелом доказової інформації, проте залишаються надзвичайно вразливими. Водночас, такий вид огляду є відносно новим та вимагає від науковців розроблення криміналістичних рекомендацій реалізації даної слідчої (розшукової) дії.

Аналіз останніх досліджень і публікацій. Загальні перспективи цифровізації науки криміналістики досліджувались у наукових роботах В. М. Шевчука [1], Р. Л. Степанюка і С. І. Перліна [2]. Окремі питання дослідження комп'ютерної техніки та комп'ютерних даних під час досудового розслідування досліджувались у публікаціях таких авторів: О. В. Захарова [3], О. В. Манжай [4], О. В. Одерій, С. О. Корона, С. В. Самойлов [5].

Криміналістичні рекомендації щодо тактики огляду комп'ютерних даних розробляли такі вчені як П. Є. Антонюк, А. В. Гутник, А. В. Коваленко [6], Г.Ю. Нікітіна-Дудікова [7], В.Г. Хахановський [8], Ю.М. Чорноус [9] та ін.

Метою статті є розкриття процесуальних та криміналістичних особливостей огляду комп'ютерних даних під час розслідування корупційних кримінальних правопорушень, учинених працівниками правоохоронних органів.

Виклад основного матеріалу. При розслідуванні корупційних кримінальних правопорушень, учинених працівниками правоохоронних органів слід враховувати, що сьогодні цифрові технології стали невід'ємною складовою життя людини та її соціальної реалізації, а тому, під час огляду місця події як окремої слідчої (розшукової) дії, слідчому доцільно звертати увагу не лише на предмети неправомірної вигоди та об'єкти, які містять матеріальні сліди кримінального правопорушення, але й на носії електронної (цифрової) інформації, що можуть зберігати в собі комп'ютерні дані.

Найбільш очевидними та поширеними джерелами даних є настільні комп'ютери, сервери, мережеві пристрої зберігання даних та ноутбуки. Ці системи зазвичай мають внутрішні накопичувачі, які приймають носії, такі як компакт-диски та DVD-диски, а також кілька типів портів (наприклад, USB, Firewire, Міжнародна асоціація карт пам'яті персональних комп'ютерів [PCMCIA]), до яких можна підключати зовнішні носії та пристрої для зберігання даних.

Прикладами зовнішніх форм зберігання, які можуть бути джерелами даних, є флеш-накопичувачі, карти пам'яті та флеш-карти, оптичні диски та магнітні диски. Стандартні комп'ютерні системи також містять нестабільні дані, які доступні тимчасово (тобто до вимкнення або перезавантаження системи). Окрім комп'ютерних пристроїв, багато типів портативних цифрових пристроїв (наприклад, КПК, мобільні телефони, цифрові камери, цифрові диктофони, аудіоплеєри) також можуть містити дані [10].

Виявлення, локалізація та збереження технічних засобів, які можуть містити в собі електронні (цифрові) сліди вчинення корупційного кримінального правопорушення, вчиненого працівниками правоохоронних органів, має важливе значення, адже комп'ютерні дані становлять цінне джерело доказової інформації, проте водночас є високовразливими – можуть бути легко змінені, пошкоджені чи повністю видалені. Саме тому забезпечення їхньої цілісності та автентичності вимагає від слідчого не лише оперативності у виявленні й вилученні таких носіїв, але й застосування спеціальних криміналістичних прийомів і технічних засобів для запобігання втраті чи спотворенню даних.

Під час огляду місця події при розслідуванні досліджуваного виду кримінальних правопорушень слідчий повинен розпізнавати можливі джерела даних, особливо електронні (цифрові) сліди, які можуть містити у собі доказову інформацію. Алгоритм дій під час виявлення таких слідів полягає у визначенні місць їх зберігання. Зокрема, такі дані можуть зберігатися в інших підрозділах організації (логи мережевої активності, використання застосунків) або в сторонніх організаціях (наприклад, журнали провайдерів Інтернет-послуг).

При виявленні комп'ютерної техніки чи інших об'єктів, які можуть містити цифрові дані, слід вжити заходів збереження інформації, якими є захист периметра навколо комп'ютера та обмеження доступу до нього під час огляду, щоб гарантувати, що інформація не буде змінена.

Також слід з'ясувати перелік всіх користувачів, які мають доступ до комп'ютера працівника правоохоронного органу, який підозрюється у вчиненні корупційного кримінального правопорушення, оскільки ці особи можуть надати паролі або інформацію про те, де знаходяться певні дані. Якщо технічні засоби підключено до мережі інтернет, відключення мережевих кабелів, підключених до технічних засобів, може запобігти зміні даних віддаленими користувачами. Якщо технічні засоби використовують бездротове мережеве підключення, то необхідно вжити заходів щодо відключення зовнішнього мережевого адаптеру або вимкнення внутрішнього мережевого адаптеру з метою розірвати мережеве підключення. У випадку, якщо жоден з цих варіантів неможливий, то доцільним є вимкнення точки доступу до бездротової мережі, яку використовують технічні засоби. Слід враховувати, що у технічних засобах може бути більше однієї точки доступу, а деякі бездротові мережеві адаптери автоматично намагаються підключитися до інших точок доступу, коли основна точка доступу недоступна, тому для запобігання знищення чи зміні комп'ютерних даних може знадобитися відключення кількох точок доступу.

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 [11, с. 115].

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 [6, с. 185]. 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 [12, с. 55].

Крім того, до такого виду огляду слід залучати спеціаліста, оскільки саме за допомогою нього можна більш повно виявити, вилучити та зафіксувати слідову інформацію з метою уникнення її зміни та знищення або пошкодження.

Стаття 237 КПК України містить положення, згідно з яким огляд комп'ютерних даних проводить слідчий, прокурор шляхом відображення в 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 в паперовій формі). Водночас ст. 99 КПК України відносить комп'ютерні дані до документів, тож огляд комп'ютерних даних необхідно проводити на підставі процесуальних вимог до огляду документів, надаючи можливість фіксації та копіювання інформації (зокрема комп'ютерних даних), що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, прирівнюючи такі копії до оригіналу.

Однак, серед науковців простежується дискусія щодо правильності такого підходу: висловлюється думка, що огляд комп'ютерних даних виходить за межі ст. 237 КПК України та потребує спеціального процесуального врегулювання.

На думку П.Є. Антонюк та К. Кахнич, визначення комп'ютерних даних дає чітке уявлення про їх сутність – інформація, що існує в електронній (цифровій) формі, така, що обробляється комп'ютерною системою, а також сама програма, що забезпечує роботу системи. Тобто, враховуючи об'єктивну дійсність, людині така інформація не доступна для безпосереднього сприйняття, а доступним є лише опосередковане (оброблене комп'ютерною системою) відображення певної її частини. Таким чином, відповідно до визначеного КПК України порядку, комп'ютерні дані в результаті «огляду» перетворюються в інформацію, яку містять комп'ютерні дані, а отже перестають ними бути, тобто відбувається підміна понять, про що ми вже неодноразово зазначали [13, с. 35]. Продовжуючи свою думку, дослідники зазначають, що в подальшому, процесуальним джерелом доказів стають не комп'ютерні дані і не інформація, яку вони містять, а копія комп'ютерних даних, виготовлена слідчим, прокурором із залученням спеціаліста. А зміст інформації, яку містять комп'ютерні дані, переданий слідчим, прокурором при складанні протоколу в ході огляду комп'ютерних даних як в самому протоколі, так і у вигляді додатків до нього (фотографій, скриншотів тощо), без збирання комп'ютерних даних (виготовлення їх копії) носить суб'єктивний та ситуативний характер, не забезпечує збереження комп'ютерних даних та можливість їх подальшого дослідження, а також багаторазового об'єктивного відображення їх змісту для всіх учасників кримінального провадження. Тобто в передбачений порядок не забезпечується збирання належних і допустимих доказів [14, с. 46].

А тому, у своїх дослідженнях П.Є. Антонюк, К. Кахнич приходять до висновку, що комп'ютерні дані не можуть бути об'єктом огляду як слідчої (розшукової) дії, порядок проведення якої передбачений ст. 237 КПК України. В ході дослідження матеріального середовища (огляду) з метою виявлення та фіксації відомостей щодо обставин кримінального правопорушення, на думку дослідників, можна вести мову лише про збирання комп'ютерних даних. А пізнання й сприйняття їх змісту має реалізовуватися шляхом проведення експертизи спеціально уповноваженим суб'єктом – судовим експертом [13, с. 36; 15, с. 129].

Проаналізувавши зазначений підхід, зауважимо, що він не позбавлений певних недоліків та не повною мірою узгоджується з положеннями чинного КПК України. Зокрема, ст. 99 КПК України прямо відносить комп'ютерні дані до документів у кримінальному провадженні. Відтак комп'ютерні дані є об'єктом криміналістичного дослідження нарівні з іншими матеріальними носіями. Крім того, ст. 237 КПК України не встановлює обмежень щодо характеру об'єктів огляду – огляду можуть підлягати як речі, документи, так і комп'ютерні дані, а отже, їх огляд можливий і передбачений процесуальним законом, а проведення експертизи не виключає можливості огляду: ці процесуальні дії мають різне призначення. Огляд забезпечує фіксацію виявлених даних у момент їх знаходження та підтверджує їх цілісність і незмінність. Експертиза ж спрямована на використання спеціальних знань для вирішення ідентифікаційних та діагностичних завдань. Таким чином, висновок експерта не може замінити протокол огляду як самостійне джерело доказів.

Отже, комп'ютерні дані можуть і повинні бути об'єктом огляду як слідчої (розшукової) дії. Особливого значення комп'ютерні дані та їх огляд мають при розслідуванні корупційних кримінальних правопорушень, вчинених працівниками правоохоронних органів.

А. В. Коваленко визначає огляд комп'ютерних даних 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 [12, с. 56].

Слід зауважити, що огляд комп'ютерної техніки та комп'ютерних даних не є тотожними між собою поняттями. Вони можуть проводитися як водночас, так і окремо. У випадку одночасного проведення огляд комп'ютерних даних виступає складовою частиною огляду комп'ютерної техніки.

Якщо розглядати комп'ютерну та мобільну техніку, за допомогою якої вчинено чи на якій залишилися сліди вчинення кримінального правопорушення, зокрема, корупційних кримінальних правопорушень, вчинених працівниками правоохоронних органів, то найінформативнішими є відомості, отримані з мобільних телефонів і смартфонів правопорушника: про осіб з кола спілкування та зміст листування з ними (в адресній книзі, електронній пошті, соціальних мережах, месенджерах, текстових документах тощо); придбані електронні квитки на різні види транспорту, факти використання сервісів пошуку попутників для поїздок (BlaBlaCar); фінансові транзакції, здійснені за допомогою банківських й електронних платіжних систем, пов'язаних, наприклад, із придбанням туристичних путівок (з метою переховатися від правоохоронних органів), бронюванням готелів, наймом житла (для тимчасового перебування там), орендою автотранспорту (для пересування); файли фотографій, що містять відомості про місце та час здійснення зйомки; інші використані такими особами електронні пристрої, які пов'язані й синхронізуються з досліджуваним комп'ютером тощо, які можливо безпосередньо використовувати для встановлення обставин розслідуваної події; транспортні засоби, обладнані автосигналізацією із функцією супутникового охоронно-моніторингового сервісу та синхронізовані з досліджуваним комп'ютерним пристроєм. Така сама інформація може бути отримана зі смартфонів, які підтримують додатки, що дають змогу здійснювати комунікацію в мережі Інтернет і зберігати необхідну інформацію [16, с. 113–114].

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 [12, с. 56].

Важливим етапом підготовки до огляду комп'ютерних даних є складання плану їх отримання. Це має важливе значення, оскільки зазвичай у технічному засобі існує кілька місць, які можуть містити в собі джерела доказової інформації. Слідчий або спеціаліст повинен сформувати план, який визначає пріоритетність цих джерел та послідовність їх дослідження. Виходячи з цього, необхідно визначити яке саме джерело даних може містити найбільш значущу для розслідування інформацію (соціальні мережі, журнали дзвінків, смс-листування між абонентами, історії браузерів тощо).

Крім того, слід враховувати, що деякі оперативні дані зникають після вимкнення або перезавантаження комп'ютера, тому їх фіксація повинна мати пріоритет перед роботою з енергонезалежними носіями. Водночас останні теж можуть змінюватися (наприклад, журнали подій, які постійно перезаписуються) [10].

З урахуванням зазначених факторів визначається послідовність дій під час огляду, що забезпечує обґрунтоване виокремлення пріоритетів та підвищує ефективність проведення 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 [17].

Отримання комп'ютерних даних може здійснюватися локально або віддалено через мережу. Локальне вилучення зазвичай є пріоритетним, оскільки забезпечує більший контроль над системою та збереженням даних. Водночас не у кожному випадку воно можливе – наприклад, коли технічний засіб розташований у приміщенні з обмеженим доступом або фізично знаходиться в іншому місці.

У випадку проведення огляду віддалено, 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 веб-версії – з використанням програми-клієнта такого месенджера [18, с. 184].

Загальний порядок виявлення та дослідження комп'ютерних даних, що зберігаються на носіях можна визначити наступним алгоритмом: 1) аналіз доступних (відкритих) файлів шляхом контекстуального пошуку за ключовими фразами; 2) пошук прихованих і зашифрованих, тимчасових, специфічних даних; 3) спроба відновлення видалених файлів [4, с. 113].

Особливе криміналістичне значення під час розслідування корупційних кримінальних правопорушень, вчинених працівниками правоохоронних органів має той факт, що файлові системи можуть зберігати дані видалених файлів чи попередніх версій існуючих файлів, які стають важливим джерелом доказової інформації. Зокрема, у більшості випадків після видалення файл фактично не стирається з носія. Змінюється лише службова інформація у структурі каталогу: вона позначає відповідний файл як видалений. Таким чином, сам файл продовжує існувати на носії, але операційна система більше не відображає його в системі каталогів. Простір, який він займає, вважається вільним і може бути перезаписаний у будь-який момент частково чи повністю. Це створює можливості для подальшого криміналістичного відновлення таких даних [10].

Виявлення та відновлення видалених файлів традиційно відносять до завдань експертизи комп'ютерної техніки та програмних продуктів [19, с. 24], отже, є складовою частиною експертного дослідження комп'ютерних даних. Водночас, як зазначає А.В. Коваленко, 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 [18, с. 185].

Під час огляду комп'ютерних даних уповноважені особи зобов'язані безпосередньо ознайомитися зі змістом їх аудіовізуального виразу та зафіксувати його у протоколі процесуальної дії й додатках до нього у формі, доступній для сприйняття іншими учасниками провадження. Для цього текстові файли, зображення, звукові чи інші аудіовізуальні форми інформації відтворюються за допомогою пристроїв виведення (монітора, акустичних систем, принтера тощо), а програмний код може бути запущений для демонстрації алгоритму його роботи. Доцільно кожний файл, що містить дані, важливі для кримінального провадження, одразу після його дослідження зберігати та фіксувати у протоколі. Такий підхід частково нівелює традиційний поділ огляду на робочу та заключну стадії, однак забезпечує належне документування результатів, які мають бути зафіксовані у протоколі.

Висновок. Огляд є основною слідчою (розшуковою) дією, яка спрямована на фіксацію обстановки вчинення корупційного кримінального правопорушення працівниками правоохоронних органів. Особливу доказову вагу набуває огляд комп'ютерних даних, що, за умови залучення спеціаліста, забезпечує повноту виявлення й фіксації електронних (цифрових) слідів без ризику їх спотворення. За допомогою використання можливостей огляду орган досудового розслідування має можливість відтворити механізм вчинення корупційного кримінального правопорушення та встановити взаємозв'язок між елементами його криміналістичної характеристики.

Список використаних джерел:

1. Shevchuk V. Innovative Essence of Criminalistic and Prospective Directions of Its Development. Malewski H., Matulienė S., Shepitko V. та ін. (ред.) Developments of Criminalistics Theory and Future of Forensic Expertology: Liber Amicorum Prof. Egidijus Vidmantas Kurapka. Вільнюс: Mykolas Romeris University, 2022. P. 152–168.

2. Степанюк Р.Л., Перлін С.І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка. 2022. № 3 (99). С. 283–284. DOI: https://doi.org/10.33766/2524-0323.99.283-284.

3. Захарова О.В. Особливості проведення огляду вилученої комп'ютерної техніки під час розслідування комп'ютерних злочинів. Слідча практика. 2012. № 3. С. 169–175.

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

5. Одерій О.В., Корона С.О., Самойлов С.В. Тактика слідчого огляду комп'ютерних систем та їх елементів. Донецьк, 2010. 88 с.

6. Коваленко А.В. Організація і тактика проведення огляду комп'ютерних даних. Науковий вісник Херсонського державного університету. Серія «Юридичні науки». 2023. № 4. С. 53–58. DOI: 10.32999/ksu2307-8049/2023-4-9.

7. Нікітіна-Дудікова Г.Ю. Електронні (цифрові) сліди у злочинах проти статевої свободи та статевої недоторканості дітей. Правове регулювання суспільних відносин: перспективні напрями на шляху до сталого розвитку: матеріали міжнар. наук.-практ. конф. (Київ, 14–15 трав. 2021 р.). Київ, 2021. С. 100–104.

8. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін. ; за заг. ред. О.В. Корнейка. 2-ге вид., доповн. Київ: Нац. акад. внутр. справ, 2020. 104 с.

9. Чорноус Ю.М., Дульський О.Л. Методико-криміналістичне забезпечення збирання доказів у кримінальному провадженні. Нове українське право. 2023. Вип. 4. С. 191–198. DOI: https://doi.org/10.51989/NUL.2023.4.25.

10. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response (NIST Special Publication 800-86). Гейтерсберг: National Institute of Standards and Technology, 2006. DOI: https://doi.org/10.6028/NIST.SP.800-86.

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

12. Коваленко А.В. Організація і тактика проведення огляду комп'ютерних даних.Науковий вісник Херсонського державного університету. Серія «Юридичні науки». 2023. № 4. С. 53–58. DOI: 10.32999/ksu2307-8049/2023-4-9. URL: https://lj.journal.kspu.edu/index.php/lj/article/view/393

13. Антонюк П., Кахнич К. Комп'ютерні дані як об'єкт огляду в кримінальному провадженні: проблемні аспекти. Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності: зб. матеріалів міжнар. наук.-практ. конф. (Кропивницький, 23 вересня 2022 р.). Кропивницький: ТОВ «Центрально-Українське видавництво», 2022. С. 34–37.

14. Антонюк П.Є. Огляд комп'ютерних даних як засіб збирання доказів у кримінальному провадженні. Кримінальне судочинство: сучасний стан та перспективи розвитку: зб. наук. праць. Київ: Нац. акад. внутр. справ, 2023. С. 45–49.

15. Антонюк П., Кахнич К., Улещенко О. Огляд комп'ютерних даних: криміналістичні рекомендації. Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності: зб. матеріалів міжнар. наук.-практ. конф. (Кропивницький, 10 жовтня 2023 р.). Кропивницький: ТОВ «Центрально-Українське видавництво», 2023. С. 128–131.

16. Климчук М.П., Кунтій А.І. Виявлення та вилучення слідів кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку. Соціально-правові студії. 2020. Вип. 3 (9). С. 111–118. URL: https://sls-journal.com.ua/web/uploads/pdf/S&LS_2020_Vol.%203,%20No.%203_111-118.pdf

17. 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. 2017. № 1 (88). С. 182–191.

18. 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.