УДК 343.14
DOI https://doi.org/10.32782/2524-0374/2024-2/111

ПРОБЛЕМНІ АСПЕКТИ СПОСОБІВ ЗБИРАННЯ ЦИФРОВИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

PROBLEMATIC ASPECTS OF METHODS OF COLLECTING DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS

Метелев О.П., доктор філософії у галузі права,
завідувач кафедри
Інститут підготовки юридичних кадрів для Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого

В даній статті досліджуються специфіка та особливості способів збирання і формування цифрових доказових відомостей в досудовому та судовому провадженнях, аналізується сучасний стан наукової розробки цієї проблеми. Проведений автором аналіз показав, що доказові відомості у цифровому вигляді, особливо в умовах збройної агресії рф проти України, складають значну частку доказового матеріалу кримінальних проваджень. Такий стан речей безумовно вимагає впровадження у кримінальний процес якісно нового підходу до використання у доказуванні цифрових доказів. Автор акцентує увагу, що процес збирання (отримання) і формування доказів у кримінальному провадженні здійснюється суб'єктами доказування (стороною обвинувачення і стороною захисту) в особливій процесуальній формі. Суб'єкт доказування, який встановлює через докази обставини у кримінальному провадженні, переходить від сприйняття окремих фактів, інформації про них під час проведення процесуальних дій (чуттєво-практичний аспект пізнання) до логічного осмислення сприйнятого (гносеологічний аспект пізнання). У статті зазначається, що структура процесу доказування повинна включати в себе різні елементи, які властиві як інформаційному, так і іншим підходам до теорії доказів: збирання, закріплення, перевірку, оцінку, логічне обґрунтування і т.п. Наголошується на невідворотності адаптації класичної кримінально-процесуальної системи до цифрової реальності.

Автором робиться висновок, що у кримінальному процесуальному законодавстві не врегульовані деякі питання щодо порядку та особливостей збирання та способів дослідження і формування цифрових доказових відомостей, які за умови належності та допустимості в подальшому набудуть статусу судових доказів. Це, в свою чергу, значно ускладнює практичне використання цифрової інформації у процесі доказування ретроспективних обставин вчиненого кримінального правопорушення. Автором пропонується з огляду на особливу гносеологічну та правову природу цифрових (електронних) доказів, виділити способи їх збирання (отримання) в окрему процесуальну категорію.

Ключові слова: кримінальне провадження, цифрові докази, способи збирання доказів.

The given article studies specifics and peculiarities of the ways and methods used to gather and form digital evidence data in pre-trial investigation and trial proceeding, as well as analyses the status of current scientific elaboration of the problem.

The analysis carried out by the author of the article shows that evidence in digital form, particularly during the russian aggression against Ukraine, comprises a significant part of evidence materials in criminal proceedings. Under such circumstances, it is required to introduce a more efficient approach to digital evidence use in criminal procedure. The author emphasizes that gathering (obtaining) and forming of evidence in criminal proceeding is performed by probative subjects (a prosecution party and a defence party) in a specific form of action. In the course of legal proceedings, a probation subject, while establishing the circumstances (facts) in criminal proceeding through the evidence, is moving from perceiving some facts, information about them (the sensual and practical aspect of cognition) to logical comprehending the perceived information (gnoseological aspect of cognition). The article states that the probation process must include different elements, common for information as well as other approaches to the theory of proofs: gathering, consolidation, verification, assessment, logical justification, etc. It also stresses on inevitable tailoring of classical criminal and procedural system to digital reality.

The author concludes that some issues related to the procedure and peculiarities of gathering evidence as well as methods of examining and forming digital data, which further will gain the trial evidence status, have not been regulated in the criminal and procedural legislation. This drawback greatly complicates practical use of digital information while establishing retrospective circumstances of a criminal offence. Taking into consideration a specific gnoseological and legal nature of digital (electronic) evidence, the author offers to distinguish its gathering (obtaining) methods in a separate procedural category.

Key words: criminal proceeding, digital evidence, evidence gathering methods.

Постановка проблеми. Інститут доказування в кримінальному процесі постійно розвивається. Зважаючи на стрімку комп'ютеризацію суспільства і значне збільшення кількості правовідносин в площині інформаційного простору, з'явився якісно новий вид кримінальних доказів – цифрові докази, основою яких є інформація представлена в дискретному вигляді. Так, Н. В. Глинська зазначає, що «значну долю інформаційного сегменту сучасного кримінального провадження складає саме цифрова інформація, що обумовлює необхідність формування якісно нового підходу до використання у доказуванні цифрових (електронних) доказів. Водночас, як констатується сучасною науковою спільнотою та практиками, чинне кримінальне процесуальне законодавство містить лише загальні правила щодо застосування електронних доказів, залишаючи не врегульованими низку питань щодо специфіки порядку їх збирання та способів дослідження» [1, с. 18].

Саме тому законодавче врегулювання способів та процедури збирання (отримання) цифрових доказів у кримінальному процесі, їх використання, з урахуванням дотримання вимог їх належності, допустимості, достовірності та достатності є нагальною теоретичною і практичною проблемою.

Аналіз останніх досліджень і публікацій. Доказування, як інститут кримінального провадження, цікавило науковців практично на всіх етапах розвитку кримінальної процесуальної науки. Свої праці дослідженню актуальних проблем доказового права, зокрема питань доказування, присвятили такі вчені, як: Н. В. Глинська, Ю. М. Грошевий, В. П. Гмирко, О. В. Капліна, М. М. Михеєнко, В. Т. Нор, М. А. Погорецький, Д. Б. Сергєєва, С. М. Стахівський, В. М. Тертишник, Л. Д. Удалова, М. Є. Шумило та інші.

Не дивлячись на те, що поняття «цифрових доказів» в правовій доктрині є достатньо новим, а наукова розробка способів збирання (отримання) цифрових даних, які мають доказове значення для кримінального провадження у вітчизняній правовій науці знаходиться на даний час на початковій стадії, досить багато науковців звертали увагу на важливість і необхідність визначення їх гносеологічної і правової природи, зокрема: Т. В. Авер'янова, Н. Н. Ахтирська, К. Браун (Christopher Brown), В. В. Білоус, В. М. Бутузов, С. Й. Гонгало, І. Г. Каланча, Е. Кейси (E.Casey), І. О. Крицька, А. В. Скрипник, А. В. Столітній, Дж. Чизам (J. W. Chisum), Д.М. Цехан, М.Г. Щербаковський, О. Г. Яновська та інші.

Мета статті. Спираючись на аналіз наукових публікацій та норм вітчизняного і зарубіжного кримінально-процесуального законодавства, дослідити способи збирання (отримання) цифрових доказів та визначити чи можливо виділити їх в окрему процесуальну категорію.

Виклад основного матеріалу. У кримінальному провадженні основою процесу пізнання є загальні гносеологічні, соціальні та психологічні закономірності. Основною метою кримінально-процесуального пізнання є отримання знання про факти, що підлягають встановленню у кримінальному провадженні. В свою чергу, предметом доказування є подія минулого – вчинене кримінальне правопорушення, саме воно визначається як різновид соціального пізнання (безпосереднього та опосередкованого). Д. Б. Сергєєва справедливо вказує, що «кримінальне правопорушення є центральним елементом предмета доказування, визначеним п. 1 ч. 1. ст. 91 КПК України. Одночасно, у органів досудового розслідування часто виникають проблеми з визначенням кола питань, пов'язаних з доведенням кримінального правопорушення, з урахуванням норм КК України та КПК України, а також обставин конкретного кримінального правопорушення» [2, с. 41].

Ця обставина обумовлена тим, що за своєю природою кримінально-процесуальне доказування є пізнавальною діяльністю ретроспективних подій. Так, М. А. Погорецький зазначає, що доказування – це нерозривний цілісний процес, що полягає в отриманні доказів (пошуку і виявленні (вилученні) фактичних даних та їх джерел; перевірці, оцінці фактичних даних і їх джерел, їх процесуальному оформленні (закріпленні) й наданні фактичним даним та їх джерелам значення доказу у кримінальному провадженні) та їх використанні для встановлення фактів та обставин, що мають значення для кримінального провадження, в обґрунтуванні доказами своєї правової позиції сторонами кримінального провадження [3, с. 22]. Наслідком здійснення пізнавальної діяльності по доказуванню є формування суб'єктивного образу об'єктивної дійсності про подію минулого, а за характером вона являє собою складноструктуровану діяльність і має розглядатися:

1) як встановлення та дослідження обставин справи, що входять до предмета доказування (ст. 91 Кримінального процесуального кодексу України (далі – КПК)), тобто діяльність відповідних державних органів і учасників процесу зі збирання (формування), перевірки й оцінки доказів, з одного боку [4];

2) як логічне формулювання та обґрунтування певної тези, висновків процесуальних рішень у кримінальному провадженні – з другого боку.

Отже, процес збирання (отримання) і формування доказів у кримінальному провадженні здійснюється суб'єктами доказування (стороною обвинувачення і стороною захисту) в особливій процесуальній формі. Суб'єкт доказування, який встановлює через докази обставини у кримінальному провадженні, переходить від сприйняття окремих фактів, інформації про них під час проведення процесуальних дій (чуттєво-практичний аспект пізнання) до логічного осмислення сприйнятого (гносеологічний аспект пізнання).

Сучасне законодавство передбачає структуру доказування, яка включає в себе збирання (отримання), перевірку і оцінку доказів. Така нормативна конструкція наслідувана з інформаційної теорії доказів, де під доказами розумілися відомості (інформація) і доказування ототожнювалось виключно з пізнавальною діяльністю. При цьому повністю ігнорується логічна і психологічна основа процесу доказування. У зв'язку з цим сучасна кримінально-процесуальна доктрина потребує конструктивного перегляду і в науковому середовищі це питання обговорюється вже давно. Зокрема, В. П. Гмирко запропонував юридичну конструкцію доказу, яка складається з нормативно-процедурного, інформаційного та фактовстановлювального сегментів [5, с. 34]. Зважаючи на вимоги ч. 2 ст. 23 КПК України, М. Є. Шумило запропонував доповнити дану конструкцію ще двома сегментами – судово-інтерпретаційним та судово-констатуючим, тим самим підкреслюючи участь сторони захисту у формуванні судових доказів [6, с. 102].

Таким чином, структура процесу доказування повинна включати в себе різні елементи, які властиві як інформаційному, так і іншим підходам до теорії доказів: збирання (отримання), закріплення, перевірку, оцінку, логічне обґрунтування і т.п.

Зупинимось більш детально на збиранні (отриманні) доказів – найважливішому початковому елементу доказування, який властивий для пізнавальної діяльності слідчого, детектива, прокурора, слідчого судді та полягає в знаходженні, сприйнятті і фіксації в установленому законом порядку відомостей, які мають значення для кримінального провадження. Збирання доказів – достатньо стала категорія, яка як елемент доказування закріплена нормативно в ст. 93 КПК та підтримується більшістю науковців. Проте, в кримінально-процесуальній науці існує не менш авторитетна позиція щодо ототожнення першого етапу доказування з процесом формування доказів, під яким розуміється весь процес перетворення доказової інформації у форму доказів, передбачених кримінально-процесуальним законом, який включає в себе як пізнавальні (вилучення інформації зі слідів), так і посвідчувальні елементи (об'єктивізація сприйнятих відомостей за допомогою засобів фіксації). Це, наприклад, формування показань, експертних висновків, протоколів слідчих дій тощо. Проте, в кримінальному процесі передбачені і інші види доказів: речові докази, інші документи, висновок спеціаліста. Такі докази отримуються суб'єктами доказування вже в готовому, остаточному вигляді і процесуальному формуванню не підлягають. Таким чином, можна вважати, що перший етап процесу доказування може здійснюватися як шляхом їх збирання, так і шляхом їх формування.

Отже, для того, щоб будь-які докази могли бути використані в кримінальному провадженні, їх слід зібрати, тобто тим чи іншим шляхом отримати в розпорядження суб'єкта доказування (слідчий, детектив, прокурор, слідчий суддя тощо) саме як докази, виділити із усього значного обсягу фактичних даних за ознакою їх значення для справи.

Збирання (отримання) доказів здійснюється сторонами кримінального провадження у порядку, передбаченому КПК. Зокрема, сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених КПК.

У той самий час, сторона захисту та потерпілий здійснює збирання доказів шляхом витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб речей, копій документів, відомостей, висновків експертів, висновків ревізій, актів перевірок; ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій, а також шляхом здійснення інших дій, які здатні забезпечити подання суду належних і допустимих доказів. Ініціювання стороною захисту, потерпілим проведення слідчих (розшукових) дій здійснюється шляхом подання слідчому, прокурору відповідних клопотань, які розглядаються в порядку, передбаченому ст. 220 КПК.

Докази можуть бути одержані на території іноземної держави в результаті здійснення міжнародного співробітництва під час кримінального провадження. Слідчий, прокурор, слідчий суддя, суд за своїм внутрішнім перекo-

нанням, яке ґрунтується на всебічному, повному й неупередженому дослідженні всіх обставин кримінального провадження, керуючись законом, оцінюють кожний доказ з точки зору належності, допустимості, достовірності, а сукупність зібраних доказів – з точки зору достатності та взаємозв'язку для прийняття відповідного процесуального рішення. Жоден доказ не має наперед встановленої сили (ст. 94 КПК).

Використання цифрових доказів у кримінальному судочинстві стало одним із самих перспективних напрямів розкриття і розслідування кримінальних правопорушень. Цифрові докази в певних випадках є єдиними доказами винуватості особи в скоєнні злочину. Відповідно, значення цифрових доказів в кримінальному судочинстві стає очевидним. На шляху до побудови нової теорії доказування змагального кримінального процесу стає очевидною невідворотність адаптації традиційної кримінально-процесуальної системи до цифрової реальності та впровадженням ефективного кримінально-правового механізму, заснованого на класичних основах справедливого суду і озброєного цифровими технологіями.

Слідчі (розшукові) дії (гласні і негласні), що являють собою найбільш досконалий механізм збирання та отримання доказової інформації і відображення її в матеріалах кримінальної справи, є основним способом збирання цифрових доказових відомостей. Процедура кожного з них детально врегульована законом.

Широкі можливості застосування інформаційних технологій в усіх сферах суспільних відносин іноді настільки стрімко змінюють їх характер, що право, як регулятор суспільної поведінки, не завжди своєчасно реагує на це. Необхідно зазначити, що збирання (отримання) цифрової інформації і цифрових носіїв інформації на сучасному етапі розвитку кримінально-процесуальної науки недостатньо врегульоване. Крім того, законодавцем досі не розроблені необхідні процесуальні гарантії щодо захисту громадян від надмірної зацікавленості з боку правоохоронних органів під час проведення процесуальних дій.

Так, в результаті правового аналізу, можна встановити, що цифрова інформація і цифрові носії інформації можуть бути отримані в рамках процедур вилучення під час обшуку (ст. 234 КПК), огляду (ст. 237 КПК), витребування документів і предметів (ст. 93 КПК) та негласних слідчих (розшукових) дій (глава 21 КПК).

Власне, сама процедура вилучення цифрової інформації, під час проведення обшуку та огляду має здійснюватися шляхом її копіювання із інформаційного простору або цифрового носія інформації і проходити в кілька етапів: 1) вилучення (копіювання) цифрової інформації з місця її виявлення на цифровий носій інформації; 2) пред'явлення виявленої цифрової інформації понятим, спеціалісту та іншим учасникам слідчих дій; 3) відображення у протоколі слідчих дій часу, місця і обстановки виявленої інформації; 4) пакування та опечатування цифрових носіїв інформації, які містять шукану цифрову інформацію.

Проте, на відміну від процедур вилучення речей та документів, вищеозначена процедура вилучення цифрових носіїв інформації в ході обшуку і огляду законодавцем не формалізована та не визначена, що може призвести до зловживань, зокрема, з боку правоохоронців, які при отриманні доступу до того чи іншого цифрового носія інформації, стають власниками особистої значущої інформації (тексти повідомлень в соціальних мережах, паролі систем електронних платежів і т.п.).

Розглянемо цю проблему більш детально. Відповідно до чинного законодавства обшук, огляд в житловому приміщенні може бути здійснений тільки за відповідною санкцією суду. Недоторканість житла – один із основних правових принципів демократичного суспільства, оскільки житло представляє собою найбільш важливе джерело відомостей про осіб, які там проживають. Раніше, низький рівень інформаційних технологій обумовлював особливий правовий статус житла. Там найчастіше зберігались відомості (листи, особисті записи, документи, цінності і т.п.), які могли б мати доказове значення для кримінального провадження, і зберігались вони у вигляді речей і документів. Отже, з точки зору ефективності збирання (отримання) доказів, саме приватна інформаційна значимість житла для людини стала правовою підставою для захисту її з боку держави від несанкціонованого проникнення, у тому числі і суб'єктів доказування.

Водночас, розвиток інформаційних технологій зумовив ситуацію, коли більша частина особистої інформації про особу стала зберігатись в електронному (цифровому) вигляді на цифрових пристроях зберігання і обробки інформації (персональних комп'ютерах, серверах, жорстких дисках, флеш-носіях і т.п.), які стали спроможні, в рамках невеликих просторових межах, контури яких співпадають з фізичними межами цих цифрових пристроїв, зберігати великі об'єми особистої інформації [7, с. 26].

Тобто, ще донедавна можливо було стверджувати, що цифровий пристрій (персональний комп'ютер, ноутбук і т.п.) знаходиться в приміщенні і, відповідно, може вважатись як його невід'ємна частина, як і інформація, яка на ньому міститься. Однак, мініатюризація електронних компонентів призвела до того, що з'явилась велика кількість ультрапортативних цифрових пристроїв, і тому вищеозначені доводи більше не можуть визнаватись як беззаперечні.

Тому, на даний час можливо поставити під сумнів належність і достовірність цифрових доказів, зібраних (отриманих) під час проведення такої слідчої дії як огляд персонального комп'ютера. Під оглядом розуміється лише візуальне обстеження місцевості, приміщення або речі, які знаходяться у вільному доступі, без активного пошукового впливу на них. Однак, органами, які проводять слідчі дії у формі огляду, в рамках цього заходу проводяться операції по відкриттю папок з файлами та самих файлів, вивчення їх вмісту та властивостей, які по суті своїй є цілеспрямованим пошуком інформації, тобто обшуком – примусовою дією, санкціонованими слідчим суддею, по виявленню відомостей, що мають доказове значення для кримінального провадження, які цікавлять слідство, а також їх конфіскацію.

Неурядова правозахисна організація «Асоціація українських моніторів дотримання прав людини в діяльності правоохоронних органів» («Асоціація УМДПЛ»), досліджуючи проблеми правового огляду особи та її речей, а також практику його здійснення (правозастосування) нарахувала у вітчизняному законодавстві п'ять різних понять стосовно проведення такої дії, як огляд особи та її речей: «особистий огляд і огляд речей», «зовнішній огляд одягу та речей», «огляд особи», «особистий обшук», «обшук особи» [8]. Це створювало плутанину щодо порядку та підстав його проведення. На теперішній час ситуація не змінилась – у вітчизняному законодавстві ми також маємо п'ять понять, що позначають один інститут особистого огляду. Лише зникло поняття «зовнішній огляд», яке було закріплене в Статуті патрульно-постової служби. Йому на зміну прийшов інститут «поверхневої перевірки» (ст. 34 Закону України «Про Національну поліцію»), який схожий за назвою, але інший за змістом. В кримінальному процесі «огляд» отримав назву «обшук особи» (ч. 3 ст. 208, ч. 5 ст. 236 КПК) / «особистий обшук» (ч. 8 ст. 191, ч. 6 ст. 208 КПК). Сучасне нормативне регулювання обшуку особи має неповний і несистемний характер, що підкреслюється низкою науковців та практиків. Так, «…закон, на жаль, не містить ніяких критеріїв, за наявності яких таке рішення може бути прийняте (мається на увазі рішення про проведення обшуку особи під час проведення обшуку житла або іншого володіння особи). Не встановлено також, яким повинне бути це рішення, як воно має бути оформлене» [9].

Користуючись такою законодавчою невизначеністю, правоохоронні органи під час проведення слідчих дій часто по відношенню до збирання цифрових доказів самостійно оцінюють свої дії як огляд, фактично здійснюючи обшук, на власний розсуд визначають необхідність обшуку особи (з метою вилучення та вивчення вмісту мобільних телефонів, інших цифрових пристроїв, накопичувачів інформації тощо), обираючи для себе найбільш сприятливий процесуальний режим отримання цифрових доказів, нехтуючи правами громадян та принципами, закріпленими кримінальним процесуальним законодавством.

В продовження даної теми, розглянемо, наприклад, іншу процесуальну дію – дослідження вмісту мобільного телефону затриманої особи в рамках особистого обшуку на підставі ч. 3 ст. 208 КПК. З точки зору законодавця, проведення уповноваженою службовою особою особистого обшуку при затриманні (без отримання нею ухвали слідчого судді на ці дії) зумовлено, по-перше, доцільністю збирання доказів «по гарячих слідах», що унеможливлює знищення доказів, а по-друге, незначними розмірами тих речей, які можливо знайти при особистому обшуку у затриманого. Хочеться зазначити, що до недавнього часу, до появи інформаційних технологій в повсякденному житті, невеликий розмір речей (об'єктів), який могла мати при собі особа, суттєво обмежував її в можливостях по збереженню і передачі інформації. Матеріальні, письмові джерела відомостей мали займати певний об'єм, що напевно обмежувало здатність людини до їх зберіганню і переміщенню у просторі. Враховуючи ці факти, законодавець допустив можливість проведення особистого обшуку без отримання ухвали слідчого судді. Проте, виходячи з реальних тенденцій у інформаційних технологіях до постійного зменшення розмірів цифрових пристроїв, наявність у затриманої особи смартфону, в якому може міститись особиста інформація, за своїм об'ємом еквівалентна вмісту кількох традиційних бібліотек, дозволяє правоохоронцям отримати доступ до цього масиву даних без належної процесуальної процедури отримання ухвали слідчого судді. Крім того, збереження відомостей в фізичній формі у вигляді письмових документів або на будь-якому іншому матеріальному носії інформації завжди дозволяло точно визначити, де саме знаходяться ті чи інші відомості, які можуть мати доказове значення для кримінального провадження. Але, сучасні цифрові технології дозволяють:

– підключення електронних пристроїв до глобальної мережі Інтернет, до інших інформаційно-телекомунікаційним мереж і систем;

– постійно знаходитись з ними на мережевому зв'язку і здійснювати обмін інформації як режимі «запит-відповідь», так і у «фоновому» (автоматичному) режимі без безпосередньої участі користувача.

Тобто, інформація на смартфонах може зберігатись не тільки фізично на самому пристрої, але і в так званих «хмарних» сховищах («iCloud», «Dropbox», «Google диск», «eDisk-UKR.net» і т.п.), при цьому пересічному користувачу не буде очевидна різниця де знаходиться шукана інформація, на локальному машинному носії інформації чи в мережі («хмарному» сховищі).

У таких випадках, з процесуальної точки зору, незрозуміло, до якої межі допускається аналогія фізичного предмета (речі) і цифрового пристрою (комп'ютера, ноутбука, електронної книги тощо), оскільки предмет може містити в собі тільки те, що в нього поклали, а комп'ютер може звернутися до даних, які не містяться в його пам'яті та машинних носіях інформації, а знаходяться, прикладом, на серверах, які знаходяться за кордоном [10, с. 31].

Не дивлячись на те, що вищевказані проблеми давно вже стали вже реальністю на практиці, КПК не дає чіткої відповіді, чи необхідно отримувати ухвалу суду на проведення обшуку мобільного телефону, або іншого цифрового пристрою затриманого. Разом з тим ст. 14 КПК передбачає, що втручання у таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування, можливе лише на підставі судового рішення. Враховуючи вищевказані протиріччя процесуальних норм, стає незрозумілим, якою з них повинен керуватись правоохоронець, здійснюючи вивчення вмісту мобільного телефону при особистому обшуку затриманого.

Як вже було зазначено раніше, огляд – це безпосереднє візуальне дослідження об'єкта шляхом її особистого сприйняття. Щодо цифрових носіїв інформації, то їх огляд спрямований на встановлення стану предмету, призначення, наявність ознак, які вказуються на зв'язок зі злочинним діянням, а також відомостей, що мають відношення до кримінального провадження. На практиці, процедуру огляду цифрового (електронного) носія інформації, засобів стільникового зв'язку (мобільних телефонів, модемів і т.п.) зазвичай розділяють на кілька етапів:

– зовнішній огляд матеріального носія (найменування пристрою, зовнішні ознаки);

– конструктивний огляд (наявність елементів живлення. карт пам'яті, SIM-карт і т.п.);

– огляд інформаційної середовища (огляд і фіксація відомостей, які містяться на цифровому носії інформації).

На особливу увагу заслуговує саме огляд інформаційного середовища цифрового носія інформації. В ході цієї процесуальної дії може виникнути необхідність щодо фіксації та копіювання інформації, яка на ньому міститься. На переконання переважної більшості науковців і експертів копіювання інформації необхідно проводити лише під час судової експертизи лабораторних умовах з метою забезпечення її належності і достовірності.

Отже, виникає закономірне питання, чи властиві «огляду інформаційного середовища» та «копіюванню цифрової інформації» ознаки самостійних слідчих дій і чи не є збирання цифрової інформації окремим способом отримання доказів під час кримінального провадження.

Аналіз численних наукових розвідок процесуалістів стосовно механізмів формування слідчих дій та способів отримання доказів у кримінальному процесі дозволяє зробити обґрунтований висновок, що нова слідча дія повинна відповідати таким критеріям:

а) загальним принципам кримінального судочинства як системи більш високого рівня;

б) загальним принципам функціонування системи (оригінальність, пристосовуваність до досягнення специфічної мети певними прийомами відображення слідів).

Крім того, з урахуванням перспективи цифровізації кримінального процесу, цілком ймовірно, що кримінально-процесуальне законодавство матиме наступні перспективні напрями розвитку:

1) розширення меж допустимості доказів і поява нових фактичних даних;

2) розширення кола слідчих дій, поява додаткових гарантій прав і свобод при їх провадженні;

3) використання новітніх експертних систем під час прийняття процесуально важливих рішень.

Таким чином, з огляду на розвиток інформаційних технологій, було б доцільно передбачити у кримінальному процесі комплекс слідчих (розшукових) дій, які аналогічні допиту, обшуку, вилученні речей і слідчому експерименту, але пов'язані з вивченням цифрової інформації, які використовують інтелект цифрових систем. І крім того, передбачити особливий порядок початку досудового розслідування на підставі повідомлень, розміщених в мережі Інтернет, а також виділити в окремі слідчі (розшукові) дії «цифровий (електронний) огляд інформаційного середовища» і «цифрове (електронне) копіювання».

Особливостями провадження таких слідчих (розшукових) дій пропонується вважати:

– «місце» проведення – інформаційне середовище;

– методи і способи провадження – спеціальні, характерні тільки для роботи з цифровими доказами;

– об'єкт дослідження, отримані відомості – цифрова інформація;

– знаряддя провадження – спеціальні засоби отримання, дослідження та оцінки отриманих цифрових даних (оскільки сприйняти цифрову інформацію можливо тільки за допомогою спеціальних цифрових приладів відображення та обробки інформації);

– суб'єкти провадження – обов'язкове залучення до роботи з цифровими доказами спеціалістів, які володіють спеціальними знаннями в сфері інформаційно-цифрових технологій;

– умови збереження отриманих масивів даних – для гарантованого збереження цифрових доказів необхідно забезпечити спеціальні умови: відсутність в найближчому оточенні цифрового сховища магнітних і електричних полів, відсутність значних коливань напруги та струму, стабільний температурний режим, відсутність механічних потрясінь, обмеження як безпосереднього фізичного доступу до носіїв цифрової інформації, так і захист найближчого оточення сховища для унеможливлення віддаленого впливу магнітними і електричними полями на цілісність цифрової інформації.

Висновки. З урахуванням специфічної «нематеріальної» природи цифрових (електронних) доказів, які: а) існують у штучно створеному інформаційному середовищі; б) мають особливий статус оригіналу і можуть існувати у такому статусі у декількох місцях; в) сприймаються та досліджуються за допомогою спеціальних програмно-технічні засобів; г) зберігаються на відповідному носії інформації, в оперативній (тимчасовій) пам'яті ЕОМ або каналі зв'язку – вбачається за доцільне виділити в окремі слідчі дії «цифровий (електронний) огляд інформаційного середовища» і «цифрове (електронне) копіювання» та відокремити збирання (отримання) цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження, з опрацюванням і визначенням особливих процесуальних правил та стандартів, зміст яких би врахував сучасні зміни, які відбулися в інформаційному суспільстві.

ЛІТЕРАТУРА

1. Глинська Н.В. Щодо використання цифрової інформації в кримінальному провадженні: окремі аспекти. *Використання цифрової інформації в розслідуванні кримінальних правопорушень:* матеріали міжнар. наук.-практ. круглого столу (м. Харків, 12 грудня 2022 року), Харків, 2022. С. 18–21.

2. Pohoretskyi M., Serhieieva D., Toporetska Z. The proof of the event of a financial resources fraud in the banking sector: problematic issues. *Financial and credit activity problems of theory and practice*.. Kyiv, 2019. № 28 (1). P. 36-45.

3. Погорецький М.А. Теорія кримінального процесуального доказування: проблемні питання. *Право України.* 2014. № 10. С. 12–25.

4. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon5.rada.gov.ua/laws/show/4651-17 (дата звернення: 15.02.2024).

5. Гмирко В.П. Кримінально-судові докази: юридичне поняття чи дефініція? *Право України.* 2014. № 10. С. 26–35.

6. Шумило М.Є. Поняття доказів у кримінальному процесі: пролегомени до розуміння «невловного» феномену доказового права. *Вісник кримінального судочинства*. 2015. № 3. С. 95–104.

7. Kessler G. Judge` Awareness, Understanding, and Application of Digital Evidence. A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computing Technology in Education. Nova Southeastern University. 2010. 182 c.

8. Крапивін Є. Особистий огляд та поверхнева перевірка: експертний аналіз. URL: http://umdpl.info/police-experts.info/2016/05/18/inspection/ (дата звернення 18.02.2024).

9. Фаринник В. Які хитрощі можуть застосовуватися стороною обвинувачення для обмеження прав громадян, у котрих проводиться обшук? URL: https://zib.com.ua/ua/print/113888-scho_potribno_znati_gromadyanam_pro_ poryadok_provedennya_obs.html (дата звернення 18.02.2024).

10. Adam M. The iphone meets the fourth amendment. *UCLA Law Review 27*, 2008. P. 27–58.