УДК 342.2

Цехан Д. М.,
науковий співробітник
науково-дослідної частини
НУ «Одеська юридична академія»

ЦИФРОВІ ДОКАЗИ: ПОНЯТТЯ, ОСОБЛИВОСТІ ТА МІСЦЕ У СИСТЕМІ ДОКАЗУВАННЯ

Анотація. У статті на підставі аналізу наукових джерел досліджено інноваційні види доказів у кримінальному провадженні. Зокрема, автором визначено особливості цифрової інформації, які впливають на її використання у доказуванні. Обґрунтовано, у тому числі й з урахуванням міжнародного досвіду, необхідність використання цифрових доказів. Крім того, детально досліджено основні способи та засоби забезпечення їх допустимості у кримінальному процесі.

Ключові слова: докази, цифрова інформація, цифрове алібі, цифрові докази, коректність фіксації.

Постановка проблеми. Основним чинником трансформації сучасного суспільства є стрімка інформатизація, яка змінює усі сторони життєдіяльності, впливає на прийняття управлінських рішень і функціонування усталених суспільних інституцій, у тому числі й правових. Змінюючи усі сторони життя людства, динамічний розвиток високих інформаційних технологій торкнувся і сфери кримінального судочинства у контексті появи нових форм представлення інформації та необхідності визначення її місця у системі доказів.

Аналіз останніх досліджень та виокремлення нерозв'язаних проблем. Для нашої правової доктрини поняття «цифрових доказів» є досить новим, хоча й привертало увагу таких вчених як В. М. Бутузов, В. Б. Вехов, С. Й. Гонгало, М. А. Іванов, Т. Е. Кукарнікова, Л. Б. Краснова, А. В. Касаткін, Ю. М. Літвінов, В. В. Лисенко, В. О. Мещеряков, Д. В. Пашнєв, М. М. Федотов тощо.

Водночас, розроблені науковцями пропозиції та надані рекомендації не були враховані під час підготовки нового Кримінального процесуального кодексу України, що знову актуалізує цю проблему, яка вимагає комплексного вивчення та обговорення вченими із урахуванням нових реалій.

Метою статті є аналіз теоретико-прикладних підходів щодо розуміння цифрових доказів та визначення їх місця у системі засобів доказування.

Викладення основного матеріалу. Розпочинаючи аналіз необхідно акцентувати увагу на тому, що інформація, яка створена за допомогою високих інформаційних технологій має унікальні особливості, які відрізняють її від усіх форм представлення інформації, які існували раніше та є звичними для слідчих, зокрема:

– існує у нематеріальному вигляді;

– зберігається на відповідному носії, оперативній пам'яті ЕОМ або каналі зв'язку;

– для її сприйняття та дослідження необхідне використання програмно-технічних засобів;

– має здатність до дубляжу, тобто копіювання або переміщення на інший носій без втрати своїх характеристик [1].

– має особливий статус оригіналу і може існувати у такому статусі у декількох місцях [2, 13].

На початковому етапі розвитку комп'ютерної техніки проблема використання у доказуванні цифрової інформації виникла у США, де існували правила використання «нетрадиційних доказів» (novel evidence). З урахуванням особливостей англосаксонської системи права, джерелом таких правил став судовий прецедент у справі Фрай проти США (Frye vs United States), який стосувався використання у доказуванні нових даних та методик науки і складався із двох елементів: по-перше, суду необхідно визначити, до якої галузі наукового знання відноситься дані та методики, які покладені в основу доказу, а по-друге, чи визнається провідними вченими-фахівцями цієї галузі принцип, на основі якого сформований доказ.

У вітчизняній теорії кримінального процесу докази класифікуються за різними підставами. Розподіл доказів на види – це одна з класифікаційних систем, відповідно до якої вони розподіляються, виходячи із специфічних та найбільш суттєвих особливостей їх форми та змісту [3, 228]. При цьому, окремі види доказів утворюються у випадку, коли їх форма та зміст володіють специфічними характеристиками, що визначають спеціальний режим їх отримання чи використання у кримінальному процесі. Традиційно, вчені пропонують поділяти докази за механізмом формування на особисті та речові [4]. Ю. М. Грошевой та С. С. Стахівський зазначають, що за змістом формування докази доцільно поділити на дві групи та відносити до другої докази, що містяться в предметах і документах [5, 208].

У зв'язку з цим, практика діяльності правоохоронних органів склалась таким чином, що слідчий, виявивши на жорсткому диску чи в оперативній

пам'яті ЕОМ цифрову інформацію, що може містити сліди злочинної діяльності чи в інший спосіб сприяти вирішенню завдань кримінального судочинства, повинен відносити її до речових доказів, у випадку, передбаченому ст. 98 КПК України чи документів відповідно до ст. 99 КПК України.

Але це створює логічні суперечності та неузгодженості, оскільки речові докази – це, у відповідності до ст. 98 КПК України, матеріальні об'єкти. Крізь призму матеріальності об'єкта законодавець у ст. 99 КПК України визначив такий вид доказів як документи, деталізувавши, що до документів можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі й електронні).

Саме тому цифровий об'єкт, який є нематеріальним, не має відповідних якісних фізичних характеристик, має специфічну процедуру та середовище створення, здатний до копіювання та переміщення без втрати характеристик, сприймається людиною лише після обробки ЕОМ та виведення інформації на відповідний технічний пристрій (монітор), неможливо визнати матеріальним об'єктом і, як наслідок, речовим доказом чи традиційним документом. У даному випадку необхідно оцінювати власне інформацію, а не матеріальний об'єкт на якому вона зафіксована.

У наукових джерелах зарубіжних країн широкого застосування набув термін «digital evidence» (цифрові докази), під якими розуміють будь-які збережені дані або дані, що передаються з використанням комп'ютера і підтримують або спростовують намір чи алібі. Цифрові дані виявляються дуже корисними при розслідуванні злочинів, оскільки є текстовою, графічною, звуковою та відеоінформацію [6].

Експертами Scientific Working Group on Digital Evidence було запропоновано під терміном «цифрові докази» розуміти будь-яку інформацію доказового значення, яка зафіксована чи передана у цифровій формі [7].

Саме тому сьогодні можна говорити про існування «цифрових доказів», під якими розуміються фактичні дані, що представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія та після обробки ЕОМ стають доступними для сприйняття людиною. При цьому, обов'язковою ознакою цифрового доказу є конвергентність, під якою розуміється здатність одиничного доказу входити у сукупність інших доказів і набувати у зв'язку з цим доказового значення.

Необхідність підвищеної уваги до цифрових доказів зумовлюється тим, що, як слушно відзначає І. П. Пономарьов, у слідчій та судовій практиці останніх років, обґрунтовуючи своє алібі, учасники кримінального провадження все частіше посилаються на те, що під час вчинення злочину вони взаємодіяли з електронними системами (працювали з персональним комп'ютером, користувались мобільним телефоном, потрапляли у поле зору камер спостереження, авторизувались у системах контролю доступу до приміщень), які знаходяться в іншому місці [8, 437]. У зарубіжній практиці, як відзначає М. А. Іванов, такі пояснення отримали назву «цифрового алібі» (digital alibi), оскільки основою для їх підтвердження чи спростування є цифрова інформація, яка записана на матеріальних носіях [9]. При цьому дослідники звертають увагу на особливості перевірки такого алібі з урахуванням того, що, по-перше, доказова інформація, яка підтверджує чи спростовує «цифрове алібі», недоступна для безпосереднього сприйняття, і для її вивчення необхідно використовувати програмно-технічні засоби; по-друге, така доказова інформація є вкрай нестійкою, оскільки може бути легко знищена (у тому числі й некваліфікованими діями слідчого) [8, 438].

У кримінальному процесі доказ повинен відповідати двом вимогам, які висуваються до його змісту та форми, – відносності і допустимості. Закономірно, що такими ознаками повинен володіти і «цифровий доказ», що може забезпечуватись коректністю фіксації та подальшою незмінністю цифрової інформації. У зв'язку з цим, ґрунтовнішої уваги заслуговує процедура фіксації цифрової інформації та забезпечення її доказового значення. Сьогодні, під час виявлення цифрової інформації у слідчих виникають значні труднощі щодо її фіксації з урахуванням вимог, що висуває кримінально-процесуальне законодавство до доказів та подальшого використання у кримінальному судочинстві.

Можливість оперативно змінювати зміст сайту, фізичне розташування серверів на території інших держав, використання анонімних програмних пакетів є факторами, які суттєво ускладнюють можливість фіксації цифрової інформації. Особливої гостроти ця проблема набуває у зв'язку з тим, що встановлення факту такого порушення є чи не найвагомішою складовою процесу доказування у відповідних провадженнях. Серед прийомів для закріплення відомостей, розміщених в мережі Інтернет, з тим, аби їх можна було використати як докази, можна отримувати від провайдера копії файлів, що формують web-сайт. Відповідні носії таких файлів можливо долучити до матеріалів кримінального провадження як докази.

Проте, у даному випадку складно забезпечити цілісність збереження цифрової інформації, що створює підґрунтя для її спростування як доказу. Ключовим чинником у цьому випадку є коректна фіксація інформації, яка може здійснюватись автоматично за допомогою спеціального програмного забезпечення та за участю відповідного суб'єкта (експерта, спеціаліста). Сьогодні можна говорити про низький рівень підготовки слідчих до роботи із програмно-технічними комплексами та складними програмними

оболонками. Як зазначають вчені, з боку слідчих та працівників оперативних підрозділів було б самовпевнено розраховувати на власні сили у цій галузі, адже справжнім ІТ-професіоналом стають після навчання у ВНЗ і кількох років роботи за спеціальністю. Отримати еквівалентні знання, прочитавши книги, поспілкувавшись із спеціалістом і провівши розслідування десятка комп'ютерних злочинів, неможливо [10, 119]. У зв'язку з цим, залучення спеціаліста під час роботи з «цифровими доказами» є обов'язковим, оскільки найменша некваліфікована дія може призвести до втрати важливої доказової чи орієнтуючої інформації.

У кожній ситуації необхідним є висунення відповідних вимог до коректності фіксації інформації. Так, будь-яке програмне забезпечення може містити помилки, які можна розділити на систематичні та спорадичні, тобто епізодичні та нерегулярні. Аналіз роботи окремих видів програмного забезпечення свідчить, що ймовірність помилки у програмному забезпеченні залежить від її виробника. Саме тому необхідним є використання програмного забезпечення, яке сертифіковане, хоча це також не виключає можливість помилки. Проте, ймовірна можливість помилки програмного забезпечення не може апріорно слугувати фактором, що спростовує зафіксовану за його допомогою цифрову інформацію.

Виявлена помилка повинна відповідати трьом ключовим умовам:

– підтверджуватись службою технічної підтримки виробника програмного забезпечення, його уповноваженого представника або компетентної організації, яка займається вивченням та узагальненням помилок та недоліків програмного забезпечення;

– помилка повинна мати безпосереднє відношення до фіксації інформації і тому могла призвести до її модифікації, що підтверджується висновком експерта;

– модифікувала під час фіксації саме ту інформації, що має значення для доказування, що підтверджується висновком експерта.

Дещо інші вимоги до коректності фіксації інформації необхідно визначити у випадку покрокової фіксації необхідної інформації слідчим, у тому числі з використання відповідних програмних продуктів. Так, для закріплення у якості доказів цифрової інформації, яка отримана внаслідок проведення слідчих дій чи негласних слідчих (розшуковий) дій, потрібне виконання, принаймні, трьох умов. ***По-перше***, необхідно здійснити оформлення усіх необхідних документів, що підтверджують правові підстави, окреслюють коло суб'єктів та умови фіксації даних у відповідності до чинного законодавства України. ***По-друге***, при фіксації необхідно уникнути можливих фізичних дефектів відповідного носія та забезпечити максимально високу якість фіксації з метою можливості подальшого експертного дослідження такої інформації. ***По-третє***, у разі відсутності у слідчого необхідних спеціальних технічних знань та навичок роботи з апаратними засобами та програмним забезпеченням, повинні залучатись спеціалісти, здатні кваліфіковано поводитись з ними, і згодом підтвердити технічну можливість та факт отримання таких відомостей у судовому засіданні.

У практичній діяльності працівників оперативних підрозділів та слідчих можуть виникати тактичні ситуації, коли з технічних причин неможливо представити суду носій, на якому було зафіксовано цифрову інформацію, що отримана внаслідок проведення оперативно-розшукових заходів, слідчих дій чи негласних слідчих (розшукових) дій. У такому випадку можна формувати докази копіюванням інформації на даному носії із застосуванням відповідних технічних засобів. Копія означеного носія із супровідним документом, що містить відомості не лише про те, під час проведення якого оперативно-розшукового заходу чи слідчої дії був отриманий оригінал вказаного носія, але і про дату, місце, час копіювання, характеристики технічних засобів і носіїв, що використовувались при цьому, повинні бути надані суду.

У даному випадку гостро постає проблема збереження цілісності інформації. Існує декілька моделей апаратних та програмних копіювальників носіїв цифрової інформації. Так, до найбільш поширених програмних засобів можна віднести: «EnCase», «FTK», «SMART», «dd», «NED». При цьому, під копіюванням мається на увазі побітова копія, «сектор в сектор», «bitstream image». Аналогічні методики набули значного поширення закордоном. Так, у поліції Німеччини поширеним є метод Perkeo, важливою особливістю якого є надійне забезпечення цілісності інформації в ході документування злочинної діяльності та можливість її використання у кримінальному судочинстві, оскільки забезпечується копіювання інформації біт за бітом та завдяки цьому її модифікація не можлива.

У випадку, коли копіювання файлів проводиться за схемою «сектор в сектор», досить важливо, щоб цільовий носій, на який копіюється інформація, був попередньо очищений. Тобто усі його сектори без винятку повинні бути перезаписані нулями або випадковими бітами. В іншому випадку, під час дослідження такого носія, фахівець, досліджуючи копію одного диска, знайде там залишки попередньої копії. При цьому, факт очищення усіх секторів цільового носія доцільно фіксувати у протоколі. Окрім цього, під час копіювання корисно вираховувати хеш-функції або контрольні суми секторів, що копіюються і заносити їх до протоколу.

Звертаючи увагу на способи забезпечення допустимості «цифрових доказів», як позитивний досвід можливо використати досвід США, де суд

визначив, що для визнання доказу допустимим, він має відповідати двом критеріям: засновуватись на науковому знанні (scientific knowledge) та сприяти розумінню чи встановленню достовірності фактів суддею чи присяжними.

Дещо інші вимоги існують щодо визначення допустимості анімації та ілюстративних доказів (комп'ютерних моделей подій), які активно використовуються у кримінальних процесах зарубіжних країн. У даному випадку суд зобов'язаний встановити: правильність параметрів, введених у програму людиною; належність програми, якою оброблялись дані, тобто чи можна стверджувати, що створена цифрова реконструкція є точною.

В окремих слідчих ситуаціях, зокрема коли об'єкти сфери високих інформаційних технологій використовувались як засоби зв'язку злочинців, для розповсюдження порнографічних предметів, розміщення інформації про продаж заборонених товарів тощо, виникає необхідність надання статусу доказів інформації, яка розміщення в мережі Інтернет. На сьогодні, на фрагментарному рівні практикою вироблені окремі методи фіксації змісту web-сайту з метою подальшого використання у кримінальному судочинстві:

– роздруківка веб-сторінки через браузер;

– роздруківка та подання рапорту працівником міліції;

– огляд web-сайту слідчим у присутності понятих;

– аналогічний огляд разом із спеціалістом;

– відповідь провайдера на запит щодо змісту сайту.

З метою забезпечення допустимості «цифрових доказів» необхідно використовувати можливості сучасних судових техніко-криміналістичних експертиз, зокрема: експертизи комп'ютерної техніки і програмних продуктів, інформаційно-комп'ютерної експертизи та комплексної експертизи. При цьому увага експерта має зосереджуватись на виявленні ознак модифікації цифрової інформації, її способів та меж.

Прогресивними у контексті використання «цифрових доказів» у кримінальному провадженні є положення ст. 360 КПК України, якою дозволяються суду скористуватись під час дослідження доказів усними консультаціями чи письмовими роз'ясненнями спеціаліста, наданими на підставі його спеціальних знань, оскільки під час дослідження судом «цифрових доказів» існує необхідність пояснення особливостей алгоритму програмування чи обробки даних, а також специфіки комп'ютерної системи.

Висновки. Підсумовуючи викладене, відзначимо, що перманентне збільшення цифрової інформації та її систематичне використання у різних сферах життєдіяльності зумовлює необхідність вироблення оптимальних підходів щодо її використання у доказуванні в кримінальних провадженнях. З урахуванням існуючої нині концепції класифікації доказів цифрова інформація з урахуванням унікальних характеристик не може бути віднесена до жодної класифікаційної групи. Тому існує необхідність уведення категорії «цифрового доказу» під яким слід розуміти фактичні дані, представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія, що стають доступними для сприйняття людиною після обробки ЕОМ та на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

З урахуванням розповсюдження стандартизованого програмного забезпечення у багатьох країнах спостерігається тенденція до пом'якшення вимог до цифрових доказів.

Література:

1. Цехан Д. М. Правові аспекти використання цифрової інформації як доказу у кримінальному судочинстві / Д. М. Цехан // Процесуальні, тактичні та психологічні проблеми, тенденції та перспективи вдосконалення досудового слідства: матеріали міжнар. наук.-практ. конф. (Одеса, 30 травня 2008 р.). — Одеса, 2008. — С. 206 —209.
2. Гонгало С. Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку: автореф. дис. на здобуття наукового ступеня канд. юрид. наук.: спец. 12.00.09 — кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність / С. Й. Гонгало. — К., 2013. — 20 с.
3. Теория доказательств в советском уголовном процессе / отв. ред. Н. В. Жогин. — Изд. 2-е, испр. и доп. — М.: Юрид. лит., 1973. — 736 с.
4. Алексеев С. С. Обсуждение спорных вопросов теории доказательств в советском уголовном процессе / С. С. Алексеев, В. П. Божьев // Соц. законность. — 1965. — С. 95 —98.
5. Грошевий Ю. М. Докази і доказування у кримінальному процесі: наук.-практ. посіб. / Ю. М. Грошевий, С. М. Стахівський. — К.: КНТ, 2006. — 272 с.
6. Casey E. Digital evidence and computer crime: forensic scene, computer, and the Internet / Eoghan Casey. — 2nd ed. — Amsterdam: Elsevier Academic Press, 2004. — 690 p.
7. Scientific Working Group on Digital Evidence [Electronic resource]. — Electronic data (1 file). — Mode of access: http // www. swgde. org /. — Title from the screen.
8. Пономарев И. П. Цифровое алиби и его проверка / И. П. Пономарев // Вестник ВГУ. Серия: Право, 2011. — № 2 — С. 437-444
9. Иванов Н. А. Применение специальных знаний при проверке «цифрового алиби» / Н. А. Пономарев. [Електронний ресурс]. — Режим доступа: http: // www. infolaw. ru /lib /2006-4
10. Федотов Н. Н. Форензика — компьютерная криминалистика / Н. Н. Федотов. — М.: Юрид. мир, 2007. — 360 с.

Цехан Д. Н. Цифровые доказательства: понятие, особенности и место в системе доказывания

Аннотация. В статье на основе анализа научных источников исследованы инновационные виды доказательств в уголовном производстве. В частности,

автором определены особенности цифровой информации, влияющие на возможность ее использования в доказывании. Обосновано, в том числе и с учетом международного опыта, необходимость использования цифровых доказательств. Кроме того, детально исследованы способы и средства обеспечения их допустимости в уголовном судопроизводстве.

Ключевые слова: доказательства, цифровая информация, цифровое алиби, цифровые доказательства, корректность фиксации.

Tsekhan D. Digital evidence: concepts, characteristics and place in the proof system

Summary. In the article on the analysis of scientific sources the innovative types of evidence in criminal proceedings were investigated. In particular, author defines the peculiarities of digital information that affect it's use in proceeding. Besides, the basic ways and means to ensure this admissibility in criminal proceeding were investigated.

Keywords: evidence, digital investigation, digital alibi, digital evidence, the correctness of fixation.