Метелев О. П.,
аспірант кафедри кримінального права
та кримінального процесу
Національної академії Служби безпеки України
ORCID ID: *0000–0003–2969–8388*

Науковий керівник:
М. Є. Шумило*, доктор юридичних наук, професор,*
професор кафедри правосуддя юридичного факультету
Київського національного університету імені Тараса Шевченка

DOI: *https://doi.org/10.17721/2413-5372.2019.3/224-238*

УДК:343.14

ПРОБЛЕМИ ВИЗНАЧЕННЯ ДОПУСТИМОСТІ І НАЛЕЖНОСТІ ЦИФРОВИХ (ЕЛЕКТРОННИХ) ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ

Анотація. *Розвиток інформаційних технологій разом із безперечними своїми перевагами привніс в наше життя цілу низку негативних явищ, які пов'язані з протиправним використанням засобів електронно-обчислювальної техніки і телекомунікації. Проте питання використання цифрової інформації як доказів у кримінальному процесуальному законодавстві України є майже не врегульованим, зокрема, залишається не визначеним місце цифрових доказів у системі процесуальних джерел доказів (цифрові докази важко однозначно віднести до речових доказів або документів), крім того, під час проведення кримінального провадження виникають проблеми щодо правильної оцінки цифрових (електронних) доказів на предмет їх належності та допустимості, що, безумовно, не сприяє ефективному використанню цифрових технологій та джерел інформації у національному судочинстві.*

Мета статті: *аналіз проблемних питань визначення належності та допустимості цифрових (електронних) доказів під час проведення кримінального провадження, а також визначення і розкриття окремих принципів для їх правильної процесуальної оцінки.*

У роботі розглядається сучасний стан теоретичних досліджень питання належності і допустимості цифрових доказів як в українській кримінально-процесуальній науці, так і за кордоном. Аналізуються особливості вимог щодо оцінки традиційних доказів і цифрових доказів у кримінальному процесі. Автором визначені особливості отримання (збирання) цифрових доказів з огляду на їх складну нематеріальну природу з метою їх подальшої позитивної оцінки за критеріями допустимості та належності.

Спираючись на міжнародний досвід, автор доходить висновку, в якому доводиться необхідність виділення окремих принципів допустимості та належності для цифрових доказів, розкривається їх зміст.

Обґрунтовується нагальна необхідність урегулювання цього питання як на законодавчому рівні, так і шляхом відповідних судових роз'яснень. Наголошується, що з огляду на специ-

фіку природи цифрових (електронних) доказів забезпечення їх належності та достовірності в кримінальному провадженні пов'язане з оперативністю проведення слідчих (розшукових) дій, обов'язковим залученням спеціаліста, фаховою підготовкою всіх суб'єктів доказування та неухильним дотриманням ними рекомендацій роботи з цифровими доказами.

Ключові слова: *кримінальний процес, цифрова інформація, цифрові (електронні) докази.*

Постановка проблеми. Інформатизація суспільства і, зокрема, розвиток цифрових технологій привело до необхідності розгляду в кримінальних справах нового виду кримінальних доказів – цифрових (електронних) доказів, яких раніше не існувало. Суттєва складність їх застосування в кримінальному судочинстві полягає в тому, що вони мають складну технічну природу, оскільки містять у собі досить абстрактні технічні і математичні моделі, а також мають специфічні умови виникнення, існування, копіювання та зберігання. Тому їх важко однозначно віднести до речових доказів або документів. Крім того, виникають певні труднощі з їх візуалізацією та гарантованим зберіганням. Проте в сучасному цифровому світі, який охоплює все більше сфер суспільного життя, цифрові докази іноді стають єдиною можливістю здійснити правосуддя. І саме тому правильна оцінка цифрових доказів під час проведення кримінального провадження на предмет належності та допустимості стає першочерговим завданням для процесу доказування.

Аналіз останніх досліджень і публікацій. Проблематика оцінки доказів як важливої частини теорії доказування в кримінально-процесуальній науці завжди привертала увагу науковців. Зокрема цьому питанню присвячували свої праці А. С. Александров, А. Р. Бєлкін, Р. С. Бєлкін, В. В. Вапнярчук, Л. Є. Владимиров, В. П. Гмирко, Г. Ф. Горський, Ю. М. Грошевий, В. Я. Дорохов, А. І. Дубинський, О. Ф. Коні, М. М. Михеєнко, Ю. К. Орлов, М. А. Погорецький, О. С. Степанов, М. С. Строгович, І. Я. Фойницький, В. Н. Шпілєв, М. Є. Шумило та інші. Щодо оцінки цифрових доказів, то цією проблематикою займалися в різні часи такі вчені, як В. Б. Вехов, Н. А. Зігура, М. А. Іванов, С. В. Калітін, В. В. Марков, В. А. Мещеряков, П. С. Пастухов, М. С. Сергєєв та інші. Серед зарубіжних науковців, які у своїх роботах розглядали окремі аспекти цієї проблематики, такі вчені як Henry C. Lee, Elaine M. Pagliaro, M. Miller, Alan Pendleton, J. Peterson, Peter Sommer та ін.

У той час, як вітчизняними науковцями досить ретельно були досліджені питання визначення поняття та принципів належності і допустимості доказів у кримінальному процесі, все ж необхідно зазначити, що теоретичних досліджень питання належності і допустимості цифрових доказів в українській кримінально-процесуальній науці обмаль. У свою чергу, М. Є. Шумило, аналізуючи еволюційні тенденції інституту доказу, зазначає, що «конструкція доказового розділу КПК України дає змогу стверджувати, що у вітчизняній процесуальній науці та законодавстві відбувається процес зміни методологічної парадигми», і з ним слід погодитись, бо зміни дійсно, як кажуть, «на порозі»[1].

Метою статі є аналіз проблемних питань визначення належності та допустимості цифрових (електронних) доказів під час проведення кримінального провадження, а також визначення і розкриття окремих принципів для їх правильної процесуальної оцінки.

Виклад основного матеріалу дослідження та його основні результати. Відомо, що з процесуального погляду будь-які відомості перед тим, як набути

[1] М Шумило, 'Гносеологічна і процесуальна природа доказів у кримінальному процесуальному кодексі України' (2016) *Актуальні питання кримінального процесуального законодавства України: збірник матеріалів міжвузівської наукової конференції* (26 квітня 2013 року) (Київ, Національна академія прокуратури України) 25.

статусу доказів, мають бути оцінені з огляду на належність, допустимість, достатність та достовірність. Змісту доказів властиві достовірність і належність, а процесуальній формі – допустимість, у той час як ознакою достатності характеризуються ті докази, яким вже властиві допустимість, належність і достовірність. За відсутності будь-якої з вказаних вище ознак немає і доказу. Так, М. Є. Шумило, обґрунтовуючи в своїх роботах необхідність розуміння доказу як складної юридичної конструкції системного характеру, зазначає, що «…правознавцю для кваліфікованої юридичної роботи з доказами треба мати напохваті спеціальний процесуальний засіб (знаряддя) – юридичну конструкцію «склад доказу». З його допомогою можна «просканувати» той матеріал, що подається (може бути поданий) у суді як доказ на предмет виявлення його юридичних «властивостей» – належності, допустимості, ступеня достовірності, вагомості, переконливості, а також визначення перспектив і способів його використання для формування і обстоювання власної правої позиції в суді»[1].

В юридичній науці вважають, що допустимість доказів – це один із елементів процесуальної форми, під якою розуміють «сукупність умов, передбачених законодавством для вчинення процесуальних дій, їх послідовність, порядок закріплення і оформлення процесуальних дій, процесуальні строки»[2]. Допустимість доказів – це придатність їх для використання у кримінальному процесі за формою, на відміну від їх належності – придатність для використання за змістом. Діалектично форма не має значення, якщо вона не відповідає його змістовній суті. І, відповідно, зміст без форми не може існувати. Форма судового доказу має істотне значення, оскільки зміст його залежить від об'єктивних властивостей фактів і обставин, що підлягають доказуванню, проміжних і побічних фактів, від якості джерел, об'єктивних і суб'єктивних факторів, що впливають на формування доказів[3]. Н. М. Кіпніс писав, що інститут допустимості доказів відображає пріоритет законодавця, що стоїть перед вибором між встановленням істини будь-якою ціною і свідомою готовністю знизити ймовірність її досягнення, щоб зменшити ризик обвинувачення невинуватого, а також звузити сферу обмеження конституційних прав громадян[4].

Що стосується дефініції допустимості доказів, то єдиної думки щодо цього у вчених немає. Зокрема, М. С. Строгович зазначав, що «допустимість доказів – це їх здатність як джерела відомостей про факти бути засобом встановлення цього факту»[5]. В свою чергу, С. А. Шейфер вбачає під допустимістю доказів якість цього доказу, пов'язану з його належною процесуальною формою[6]. М. А. Погорецький під допустимістю доказів розуміє таку внутрішньо властиву їм якість, унаслідок якої ці докази здатні встановити обставини, що необхідні для повного і правильного вирішення певної справи, а вимога належності охоплює не весь доказ у цілому, а лише його змістовну частину – фактичні дані. Сукупність вимог, що висуваються законом до процесу отримання доказів, становить інститут процесуальної допустимості, який полягає в тому, що

[1] М Шумило, 'Поняття доказів у кримінальному процесі: пролегомени до розуміння «невловного» феномену доказового права' (2015) 3 *Вісник кримінального судочинства* 102.

[2] В Шпилев, '*Содержание и формы уголовного судопроизводства'* (Минск 1974) 102.

[3] О Бандурка, Є Блажівський, Є Бурдоль та ін., *Кримінальний процесуальний кодекс України. Науково-практичний коментар у 2 т.* (Право 2012) <https://pidruchniki.com/1250071149245/ pravo/dopustimist_dokazu#888/> дата звернення 10.09.2019.

[4] Н Кипнис, '*Допустимость доказательств в уголовном судопроизводстве*' (Москва 1995) 5.

[5] М Строгович, '*Курс советского уголовного процесса*' (Москва 1968) т 1, 392.

[6] С Шейфер, '*Сущность и способы собирания доказательств в советском уголовном процессе*' (Москва 1972) 34.

належні до справи фактичні дані повинні бути одержані із встановленого законом джерела уповноваженим на це суб'єктом кримінального процесу (органом дізнання, слідчим чи судом) і закріплені у спосіб, передбачений у кримінально-процесуальному законі[1].

Відповідно до ст. 86 КПК доказ визнається допустимим, якщо він отриманий у порядку, встановленим Кримінальним процесуальним кодексом. Недопустимий доказ не може бути використаний при прийнятті процесуальних рішень, на нього не може посилатися суд при ухваленні судового рішення[2]. Разом із тим у законі визначені окремі ознаки недопустимих доказів і зазначені безумовні ознаки недопустимих доказів: це докази, отримані внаслідок істотного порушення прав та свобод людини, гарантованих Конституцією та законами України, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також будь-які інші докази, здобуті завдяки інформації, отриманій внаслідок істотного порушення прав і свобод людини (ст. 87 КПК).

До того ж, статтею 223 КПК передбачена норма, згідно з якою будь-які слідчі (розшукові) або негласні слідчі (розшукові) дії після закінчення строків досудового розслідування (крім їх проведення за дорученням суду) визнаються недійсними, а встановлені внаслідок них докази – недопустимими.

Крім того, згідно з КПК умовно допустимими є докази щодо судимостей підозрюваного, обвинуваченого або вчинення ним інших правопорушень, що не є предметом цього кримінального провадження, а також відомості щодо характеру або окремих рис характеру підозрюваного, обвинуваченого (ст. 88 КПК), показання з чужих слів (ст. 97 КПК), докази, отримані в результаті обшуку до постановлення ухвали слідчого судді з цього приводу (ч. 3 ст. 233 КПК), докази кримінального провадження, що перейняте від іншої держави (ст. 598 КПК). У разі встановлення очевидної недопустимості доказу під час судового розгляду суд визнає цей доказ недопустимим, що, в свою чергу, означає неможливість дослідження цього доказу або припинення його дослідження в судовому засіданні, якщо таке дослідження було розпочате. О. С. Ткачук, аналізуючи зміст КПК, дійшов висновку, що загалом під допустимістю доказів у кримінальному процесі законодавець передбачає оцінку сукупності кримінально-процесуальних дій, спрямованих на захист прав і свобод громадян[3].

Науковці традиційно виділяють наступні вимоги щодо допустимості доказів:

1. Законність джерела. Вважається, що не можуть бути доказами фактичні дані, отримані з анонімних джерел, чуток тощо. Згідно з ч. 2 ст. 84 КПК процесуальними джерелами доказів можуть бути: показання, речові докази, документи, висновки експертів. Особливості джерела доказів впливають на його зміст і форму. Ідея об'єктивної можливості перевірки доказів полягає в тому, що без знання джерела не можна судити про якості доказу, його здатність встановлювати шукані факти.

2. Законність способу отримання доказів. Способи отримання доказів формалізовані та визначені в КПК. Так, у ст. 223 КПК сформульовані загальні вимоги щодо проведення слідчих (розшукових) дій. Статті 224–232 КПК містять норми щодо умов і процесуального порядку проведення таких слідчих (розшукових) дій, як допит, пред'явлення особи для впізнання, пред'явлення речей (трупа) для впізнання, проведення допиту, впізнання в режимі відеоконференції під час досудового розслідування, обшу-

[1] М Погорецький, '*Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі*' (Харків 2007) 479, 492–493.

[2] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI <http://zakon5.rada.gov.ua/laws/show/4651–17> дата звернення: 19.09.2019.

[3] О Ткачук, 'Визнання доказів допустимими за кримінальним процесуальним законодавством' (2013) 1 (10) *Часопис цивільного і кримінального судочинства* 89

ку, огляду, залучення експерта та проведення експертизи.

Якщо розглядати цифрові докази, то беручи до уваги їх особливу нематеріальну природу, особливості їх виникнення та існування, копіювання й дублювання, зберігання і візуалізації – вбачається за доцільне виділити в окремі слідчі дії «електронний огляд інформаційного середовища» і «електронне копіювання» та відокремити збирання (отримання) електронної інформації як окремий спосіб отримання доказів під час кримінального провадження.

При збиранні цифрової інформації, яка має доказове значення для кримінального провадження, закономірно виникають наступні проблемні питання:

– правова регламентація участі спеціаліста;

– оформлення процесуальних рішень;

– технічне забезпечення слідчих;

– достовірність отриманої цифрової інформації;

– правовий статус відомостей, отриманих із інформаційно-телекомунікаційних мереж, зокрема глобальної мережі Інтернет.

Для вирішення цих проблемних питань необхідно виділити у відповідних явищах дійсності (інформаційних технологіях) ті ознаки, які мають юридичне значення і підлягають кодифікації законодавцем під час опрацювання нових процесуальних правил стосовно цифрових доказів. До них будуть відноситись, звичайно, загальні ознаки, які властиві всім без винятку доказів, а також спеціальні, які характерні тільки цифровим доказам.

З огляду на специфічну природу цифрових доказів можливо узагальнити та визначити їх критерії, а саме:

– вони існують у нематеріальному вигляді;

– зберігаються на відповідному носії (машинному носії інформації), в оперативній пам'яті ЕОМ або каналі зв'язку;

– для їх сприйняття та дослідження необхідні програмно-технічні засоби, тобто «посередники» між програмним кодом (цифровим сигналом) та людиною;

– вони мають здатність до дубляжу (копіювання/переміщення) на інший носій без втрати своїх характеристик, причому якість копіювання знаходиться на такому рівні, що єдиною відмінністю оригіналу від копії може бути час створення файлів;

– мають особливий статус оригіналу і можуть існувати у такому статусі у кількох місцях;

– здатні зберігати великі об'єми відомостей (це робить цифрові пристрої найбільш інформативним джерелом відомостей про власника, що підлягає обліку при забезпеченні прав громадян на особисте життя);

– можливість отримання інформації, яка зберігається в пам'яті самого пристрою, так і в інформаційно-телекомунікаційній мережі Інтернет, або в будь-якій іншій комунікаційній системі (ця особливість цифрової інформації, як було показано вище, підриває діючі правові стандарти, наприклад, у частині обґрунтованості застосування процедури особистого обшуку, яка завжди виходила з того, що об'єкт матеріального світу містить лише ті відомості, які зберігає в собі, в той час як цифровий пристрій може надавати інформацію ззовні);

– відносність і неочевидність вмісту цифрових даних (наприклад, більша частина інформації, що зберігається на електронних носіях, є метаданими, про існування яких користувач, як правило, не здогадується, проте метадані можуть містити важливу інформацію про операції користувача з файлами, а доступ до них користувачу іноді може бути обмежений правами адміністратора операційної системи). Зазначена особливість цифрової інформації дає можливість досліджувати ті дані електронної активності людини, про існування яких вона і не здогадувалась (службові команди; звіти про користувача і системні зміні, про наявне програмне забезпечення;

дані тріангуляції і геопозиції, які пересилають цифрові пристрої в «фоновому» режимі; історію мережевого підключення тощо).

Саме тому до цифрових доказів повинні пред'являтись більш жорсткі вимоги, оскільки для їх оцінки потрібні спеціальні пристрої, а також особи, які володіють вузькоспеціалізованими науковими знаннями. А. Р. Бєлкін уважав, що «… законодавець справедливо взяв до уваги ту обставину, що вилучення електронного носія інформації в ході обшуку і вилучення може представляти собою завдання, яке потребує професійних знань у сфері інформації»[1]. До того ж, цифрові докази можуть легко бути змінені або знищені. Відповідно вкрай важлива своєчасна і правильна фіксація цифрової інформації.

Тому існують певні особливості отримання (збирання) цифрових доказів з метою їх подальшої позитивної оцінки за критеріями допустимості та належності, а саме:

– висока оперативність під час збору цифрових доказів;

– обов'язкова участь компетентної особи, яке володіє достатніми знаннями;

– наявність спеціальних пристроїв, які мають необхідні функції для збирання цифрових доказів (персональний комп'ютер, мобільний пристрій тощо).

До недавнього часу використання цифрових доказів у кримінальному судочинстві було новим, проте тепер цей вид доказів досить широко використовуються в доказуванні у кримінальному провадженні.

У світовій практиці боротьби зі злочинністю робота з цифровими доказами (digital evidence) ведеться ще з середини 80-х років минулого століття і переважно нормативно закріплена в національних законодавствах. Зокрема, в законодавстві США (країні, в якій дуже серйозно ставляться до питання відповідності законодавства реаліям життя суспільства і держави) вже наприкінці XX ст. цифрові докази були виділені в окрему групу доказів. Для цього у процесуалістів було кілька причин: по-перше, вважалось, що це особлива форма доказів, створення яких пояснюється використанням апаратно-програмних засобів цифрової техніки; по-друге, доступ. Аналіз і дослідження інформації, яка зафіксована на машинних носіях (локальних або мережевих), не можливі без використання апаратно-програмних засобів цифрової техніки; по-третє, пошук, вилучення, дослідження та зберігання цифрових доказів потребує застосування особливих і спеціальних технологій; по-четверте, необхідні спеціальні підходи щодо оцінки їх допустимості і достовірності в рамках кримінального судочинства.

В 1995 році за ініціативою правоохоронних органів США, Канади і кількох європейських країн була створена Міжнародна організація по комп'ютерним доказам (International Organization on Computer Evidence –IOCE)[2]. Пізніше була створена Наукова робоча група по дослідженню цифрових доказів (Scientific Working Group on Digital Evidence – SWGDE)[3].

Вказаною робочою групою (SWGDE) були сформульовані основні принципи і стандарти роботи з цифровими доказами, які базуються на положенні, що для забезпечення процесуальних процедур, з метою забезпечення належності доказів правоохоронними і судовими органами повинні створюватись ефективні системи відстеження якості цифрових доказів[4]. Відповідно до цих принципів стандартні операційні процедури повинні становити собою документально зафіксовані рекомендації щодо контролю

[1] А Белкин 'Новеллы уголовно-процессуального законодательства – шаги вперед или возврат на проверенные позиции?' (2013) 3 *Уголовное судопроизводство* 5.

[2] International Organization on Computer Evidence <http://www.ioce.org/> дата звернення 10.07.2019.

[3] Scientific Working Group on Digital Evidence <https://www.swgde.org/> дата звернення 10.07.2019.

[4] G Kessler, Judge. Awareness, Understanding, and Application of Digital Evidence (Miami Nova Southeastern University 2010) 182

якості роботи з цифровими доказами, які підтверджуватимуться відповідними нотатками в матеріалах справи і проводитимуться з використанням загальнопоширених методів, обладнання та матеріалів. Також вся діяльність, яка пов'язана з отриманням, зберіганням, дослідженням та передачею цифрових доказів, повинна бути зафіксована в письмовому вигляді і бути доступною для ознайомлення усіма учасниками судового процесу. Крім того, будь-які дії, результатом яких може стати порушення цілісності цифрових доказів, пошкодження або знищення вихідних доказів, повинні виконуватись винятково кваліфікованим персоналом і тільки із застосуванням експертно-обґрунтованих методів і процедур.

У свою чергу, враховуючи досвід західних колег, Н. А. Зігура пропонує на етапі перевірки комп'ютерної (цифрової) інформації вказані принципи доповнити наступними правилами:

1. За можливістю встановити технічний засіб, з якого була отримана або скопійована цифрова інформація.

2. Перевірити відповідності типу, моделі, фірми виробника матеріального носія цифрової інформації з параметрами, вказаними в протоколі слідчої дії, у висновку спеціаліста.

3. Встановити програмні засоби, за допомогою яких була отримана цифрова інформація[1].

Таким чином, беручи до уваги вказані загальні положення та рекомендації, для забезпечення достовірності цифрових доказів в інтересах кримінального провадження необхідно встановити:

Яке програмне забезпечення використовувалось для формування (створення) доказово значущої цифрової інформації (наприклад, автоматичне створення журналів системних подій відбувається під час роботи операційних систем WINDOWS, UNIX, ANDROID, iOS тощо).

Який програмний засіб використовувався для копіювання, якщо цифрова інформація скопійована на інший машинний носій інформації.

Яким апаратно-програмним засобом необхідно буде скористатись для відтворення цифрової інформації.

Вказати в протоколі слідчих дій характеристики апаратних та програмних засобів (тип та параметри операційної системи, серійні номери апаратних та інтерфейсних складових ПЕОМ, MAC-адреси мережевих компонентів тощо).

Визначити реквізити цифрової інформації яка знаходиться на машинному носії зберігання та обробки інформації (тип файлу, об'єм, час створення, час редагування, час відкриття, відомості про користувача тощо).

Встановити, яким чином була забезпечена вимога цілісності (незмінності) даних. Вказати в протоколі слідчих дій, які саме засоби (програмні, апаратні тощо) використовуються для забезпечення цілісності цифрової інформації.

Щодо збереження цілісності цифрових доказів, то поряд з апаратними і фізичними способами (охорона, пломбування, контроль подачі живлення тощо) цілком доцільно використовувати криптографічний принцип хешування (або гешування), який широко застосовується в різноманітних програмних продуктах. У криптографії хешування (з англ. hashing) – це перетворення масиву даних довільного розміру в блок даних фіксованого розміру, який служить (у деяких випадках) замінювачем вихідного масиву даних. Криптографічно стійку хеш-функцію (геш-функцію) можливо використовувати для підтвердження автентичності будь-якої цифрової інформації (аудіо -, відео – файли, текстові і графічні файли, Інтернет трафік тощо), які записані за допомогою технічних засобів цифрової текінки. При копіюванні таких даних на зовнішній пристрій зберігання інформації необхідно за допомогою спеціального програмного забезпечення обчислити хеш-функцію, яка буде слугу-

[1] Н Зигура, 'Компьютерная информация как вид доказательств в уголовном процессе России' (дис канд юрид наук, Челябинск, 2010) 136

вати підтвердженням незмінності і цілісності вихідної цифрової інформації[1].

Для відновлення видаленої цифрової інформації або її розшифрування використовується спеціальне програмне забезпечення, яке пройшло сертифікацію та ліцензування.

Крім того, як спеціальну захисну структуру для цифрових даних можливо застосування електронного цифрового підпису, який визнається науковцями та практиками перспективним методом забезпечення автентичності змісту електронного документа, що має доказове значення в кримінальному провадженні. Такий підпис є криптографічним перетворенням інформації з використанням закритого ключа електронного підпису.

Також спеціальним методом перевірки цифрових доказів є комп'ютерно-технічна експертиза. Під час її проведення виконуються наступні дії, спрямовані на збереження цілісності вихідної інформації:

– накопичувач, який містить досліджувану інформацію, підключається до жорсткого диску експерта і обчислюється хеш-функція інформації, яка міститься на вихідному накопичувачі. Це підключення здійснюється способом, який виключає запис, у тому числі випадкову (тільки читання);

– створюється точна цифрова копія вихідного накопичувача шляхом копіювання інформації (при цьому використовується процедура клонування вмісту накопичувача за допомогою дублікаторів або спеціального програмного забезпечення типу Forencis, Norton Ghost, EnCase на жорсткий диск експерта);

– обчислюється хеш-функція дубліката, яка повинна збігатися з вихідною хеш-функцією;

– надалі вся робота з пошуку інформації ведеться на підключених до стендового комп'ютера дисках-клонах, що досліджуються[2].

Водночас, існує ще одне проблемне питання – допустимість цифрових доказів, отриманих з глобальної мережі Інтернет. Для цього перш за все необхідно визначитися з основними термінами, які характеризують роботу глобальної мережі Інтернет.

Законодавчі визначення понять «веб-сайт» та «веб-портал» надані в п. 1.3. «Порядку інформаційного наповнення та технічного забезпечення Єдиного веб-порталу органів виконавчої влад», затвердженого Наказом Державного комітету інформаційної політики, телебачення і радіомовлення України Державного комітету зв'язку та інформатизації України від 25.11.2002 № 327/225[3]. Зазначено, що «веб-сайт» – це сукупність програмних та апаратних засобів з унікальною адресою у мережі Інтернет разом з інформаційними ресурсами, що перебувають у розпорядженні певного суб'єкта і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інші інформаційні послуги через мережу Інтернет.

Також відповідно до ч. 1 ст. 1 Закону України «Про телекомунікації» «домен» – частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється[4]. Крім того, згідно з п. 2 «Порядку підключення до глобальних мереж передачі даних», затвердженого Постановою Кабінету Міністрів України від 12 квітня 2002 р. № 522, «доменне ім'я» – буквено-циф-

[1] А Александров, С Кувычков, 'О надежности «электронных доказательств» в уголовном процессе' (2013) 5 *Библиотека криминалиста. Научный журнал* 46

[2] П Костин, '*Исследование машинных носителей информации при расследовании преступлений в сфере экономики*' (Новгород 2009) 6

[3] Про затвердження порядку інформаційного наповнення та технічного забезпечення Єдиного веб-порталу органів виконавчої влади: Наказ Державного комітету інформаційної політики, телебачення і радіомовлення України, Державного комітету зв'язку та інформатизації України від 25.11.2002 № 327/225 <https://zakon.rada.gov.ua/laws/show/z1021–02> дата звернення: 18.09.2019.

[4] Про телекомунікації: Закон України від 18.11.2003 № 1280-IV <https://zakon.rada.gov.ua/laws/show/1280–15> дата звернення: 18.09.2019.

ровий вираз, що ідентифікує будь-який комп'ютер абонента у мережі Інтернет[1].

Таким чином, доменне ім'я, зареєстроване у відповідному домені, використовується для позначення відповідного сайту. Для того, щоб сайт був позначений конкретним доменним ім'ям, спочатку необхідно зареєструвати доменне ім'я у відповідному домені, внаслідок чого особа, яка зареєструвала відповідне доменне ім'я, і є власником веб-сайту. Наприклад, веб-сайт Верховної Ради України знаходиться в інтернеті за адресою: http://w1.c1.rada.gov.ua, де доменним ім'ям буде rada.gov.ua. Отже, вимога законності джерела цифрових доказів як ознаки допустимості при отриманні їх безпосередньо з мережі Інтернет виконується.

Проте основною проблемою цифрової інформації, яка розповсюджується через веб-сайт в глобальній мережі Інтернет, є можливість оперативної модифікації цієї інформації (вона може бути змінена, видалена або відредагована) власником або розповсюджувачем інформації, При тому, що доведення цієї модифікації цифрової інформації практично неможливе, оскільки найчастіше фізичне розташування веб-серверів виявляється за кордоном. Отже, найголовнішим завданням суб'єктів доказування при отриманні цифрових доказів з мережі Інтернет є оперативне закріплення фактичних даних з веб-сайту для подальшої їх оцінки.

Проведений аналіз науково-практичної літератури дозволив виявити основні варіанти закріплення фактичних даних у мережі Інтернет, які застосовуються в юридичній практиці:

1. Роздрукування сторінок веб-сайту в мережі Інтернет.

У ст. 1 Закону України «Про інформацію» міститься визначення документа, за яким документ – це матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі[2]. В свою чергу, в ст. 5 Закону України «Про електронні документи та електронний документообіг» зазначено, що електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа[3]. Крім того, в ч. 4 ст. 5 Закону вказується, що візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною. Отже, сторінка в мережі Інтернет може вважатися матеріальним носієм, що містить інформацію, і функціями якої є збереження та передання інформації, а, як наслідок, і документом.

Проте, як вже було зазначено вище, сучасні технології дають змогу внести зміни до інформаційного змісту веб-сайту, або взагалі створити сторінки, які ніколи не існували в реальності. Тому роздрукування веб-сторінки з мережі Інтернет – це досить сумнівний спосіб забезпечення допустимості цифрових доказів.

2. Нотаріальне засвідчення роздрукованих сторінок з веб-сайту в мережі Інтернет.

Згідно з ч. 6 ст. 7 Закону України «Про електронні документи та електронний документообіг» копією електронного документа є візуальне подання цього документа на папері, яке засвідчене у порядку, встановленому законодавством. Статтею 7 Закону України «Про нотаріат» визначено, що нотаріуси або посадові особи, які вчиняють нотаріальні дії, у своїй діяльності керуються законами України, постановами Верховної

[1] Про затвердження порядку підключення до глобальних мереж передачі даних: Постанова Кабінету Міністрів України від 12.04.2002 № 522 <https://zakon.rada.gov.ua/laws/show/522–2002-п> дата звернення: 18.09.2019.

[2] Про інформацію: Закон України від 02.10.1992 № 2657-XII <https://zakon.rada.gov.ua/laws/show/2657–12> дата звернення: 21.09.2019.

[3] Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV <https://zakon.rada.gov.ua/laws/show/ 851–15> дата звернення: 20.09.2019.

Ради України, указами і розпорядженнями Президента України, постановами і розпорядженнями Кабінету Міністрів України, а на території Республіки Крим, крім того, законодавством Республіки Крим, наказами Міністра юстиції України, нормативними актами обласних, Київської та Севастопольської міських державних адміністрацій[1]. Відповідно до Глави 7 «Порядку вчинення нотаріальних дій нотаріусами України» передбачено процедуру засвідчення вірності копій документів і витягів з них[2].

На думку С. Я. Фурси, засвідчена нотаріусом копія електронного документа відповідає вимогам чинного законодавства, а отже має цілком допустимий доказовий характер. Він наводить приклад зі своєї адвокатської практики, коли нотаріус вчинив таку нотаріальну дію, не дивлячись на те, що Порядком вона не передбачена та виходив із аналогії щодо допустимості у нотаріальному процесі електронних доказів шляхом відтворення інформації із електронних реєстрів (витяги із Єдиних та Державних реєстрів). При цьому він керувався принципом «Все що не заборонено законом, те дозволено» та тим самим сприяв особі в охороні права, тобто здійсненні охоронної функції[3]. На жаль, законами чи підзаконними нормативними актами України на сьогоднішній день не передбачене право нотаріусу проводити огляд веб-сайту, що, звичайно, з огляду на сучасний стан розвитку інформаційного кіберпростору потребує законодавчого регулювання.

3. Проведення судом безпосереднього огляду цифрових доказів на веб-сайті як процесуальної дії.

Кримінальний процесуальний кодекс України передбачає, що суд першої інстанції при розгляді кримінального провадження безпосередньо досліджує докази по справі, у тому числі оглядає речові докази (ст. 357 КПК) та документи (ст. 358 КПК). Зазначені докази повинні бути оглянуті судом і пред'явлені учасникам судового розгляду, а в разі потреби – свідкам, спеціалісту, експерту. Якщо речові докази не можна доставити в судове засідання, то за наявності клопотання сторін або з власної ініціативи суд може провести огляд речового доказу за місцем його розташування. Проведення огляду таких речових доказів і його результати відображаються в протоколі огляду речового доказу судом на місці. Таким чином, протокол огляду, складений судом, з додатками, а саме роздрукованою копією веб-сайту, фотознімком чи відеозаписом буде вважатися допустимим доказом. Проте виникає проблема з тим, що стороні судового кримінального процесу вже буде відомо про ваше звернення до суду і, в свою чергу, суд повинен повідомити сторони і підготуватися до огляду доказів, що також потребує часу. Оперативність отримання цифрових доказів у такому випадку зводиться до мінімуму, тому що в момент огляду наявні фактичні дані на сторінці в мережі Інтернет вже можуть бути знищені чи змінені. Такий спосіб забезпечення достовірності цифрових доказів можна застосовувати як додатковий.

3. Надання в суд висновку експерта.

Так, Т. Ю. Кудрицька вважає, що не слід недооцінювати такий спосіб фіксації доказів у мережі Інтернет, як дослідження сторінки експертом, атестованим за спеціальністю «Дослідження телекомунікаційних систем (обладнання) та засобів». Якщо таке дослідження проводилося в рамках так званої «досудової експертизи», за його результатами складається висновок фахівця в галузі до-

[1] Про нотаріат: Закон України від 02.09.1993 № 3425-XII <https://zakon.rada.gov.ua/laws/show/3425–12> дата звернення: 19.09.2019.

[2] Про затвердження Порядку вчинення нотаріальних дій нотаріусами України: Наказ Міністерства юстиції України від 22.02.2012 № 296/5 < https://zakon.rada.gov.ua/laws/show/z0282–12> дата звернення: 18.09.2019.

[3] С Фурса (ред), '*Теорія нотаріального процесу: Науково-практичний посібник*' (Київ, Алерта 2012) 86–87.

слідження телекомунікаційних систем[1]. Такий доказ буде вважатися допустимим з погляду процесуального закону. Проте на сьогодні в Україні в науково-дослідного інститутах судових експертиз лише два міста в країні – Київ і Харків мають експертів за спеціальністю «Дослідження телекомунікаційних систем (обладнання) та засобів», а на практиці загальна черга на вказані дослідження триває близько 2–3 місяців залежно від навантаження експертів. Тому існує загроза, що фактичні дані можуть бути знищені чи змінені на момент проведення такого дослідження.

4. Акт огляду веб-сайту з додатком друкованих фотографічних зображень сайту, який здійснено адвокатом.

Відповідно до п. 7 ч. 1 ст. 20 Закону України «Про адвокатуру та адвокатську діяльність»[2] під час здійснення адвокатської діяльності адвокат має право вчиняти будь-які дії, не заборонені законом, правилами адвокатської етики та договором про надання правової допомоги, необхідні для належного виконання договору про надання правової допомоги, зокрема збирати відомості про факти, що можуть бути використані як докази, в установленому законом порядку запитувати, отримувати і вилучати речі, документи, їх копії, ознайомлюватися з ними та опитувати осіб за їх згодою. Отже, адвокат як уповноважений суб'єкт доказування може збирати відомості про факти, які можуть бути використані як докази в кримінальному провадженні. Вказані відомості необхідно оформити як акт або протокол, де зафіксувати час складення, сайт, адресу, назву матеріалу з додаванням роздрукованої веб-сторінки та свідками, які можуть засвідчити час вироблення фотографій та адресу здійснення фотографування. Також можна додати фотографії сайту, зробити відеозапис та «скріншоти» сайту на диск, на якому будуть міститися первинні зразки веб-сторінки в електронному вигляді. Проте, на жаль, у законодавстві України не закріплено можливості збирання доказів шляхом складення аффідевіту (в англо-саксонській системі права США та Великій Британії під аффідевітом розуміється письмова заява, показання, свідоцтва, яке дається особою під присягою і яке посвідчується відповідною посадовою особою), що виключає допустимість таких доказів у судах України, однак не забороняє адвокату в Україні збирати таким чином фактичні дані, які можуть стати в подальшому доказами.

Загальновідомо, що належними вважаються докази, на підставі яких можна встановити обставини, котрі входять в предмет доказування. Суд не бере до розгляду докази, які не стосуються предмета доказування.

Тобто «…належність відповідає, з одного боку, на питання про наявність зв'язку між змістом доказу і фактом, який підлягає встановленню; з іншого боку – визначає, наскільки точно встановлено шуканий факт. Інакше кажучи, належний доказ має визначену доказову силу; не належний – не має її зовсім»[3].

Проведений системний аналіз вітчизняних та зарубіжних наукових досліджень дозволив виділити наступні принципи належності цифрових доказів, а саме:

1. Допустимість цифрових доказів. Перш за все докази мають бути зібрані та збережені таким процесуальним способом, щоб вони в подальшому могли використовуватись як докази в суді. Відповідно, наявність помилок та порушення процесуальної процедури тягне за собою визнання доказів недопустимими. Більш розгорнуто принцип допустимості був розглянутий вище.

[1] Т Кудрицкая, 'Сложности сбора доказательной базы в Интернете' <https://jurliga.ligazakon.net/analitycs/52188_slozhnosti-sbora-dokazatelnoy-bazy-v-internete> дата звернення 10.09.2019 року.

[2] Про адвокатуру та адвокатську діяльність: Закон України від 05.07.2012 № 5076-VI <https://zakon.rada.gov.ua/laws/show/5076–17> дата звернення: 19.09.2019.

[3] О Степанов, 'Належність та допустимість доказів у кримінальному процесі України' (автореф дис канд юрид наук, Київ 2007) 9

2. Справжність цифрових доказів. Цей принцип забезпечує те, що докази (отримані в результаті проведення НСРД відомості) мають бути релевантними відносно справи, і, відповідно, спеціаліст (експерт) повинен мати змогу оцінити справжність цифрових відомостей. Наприклад, перехоплення передачі електронної пошти ще не є достатньою підставою вважати, що ймовірний відправник – це об'єкт проведення НСРД. Електронний лист міг відправити хтось із родини об'єкта і встановити істину можливо тільки за сукупністю отриманих відомостей (наприклад, згодом об'єкт підтвердив телефонним зв'язком, що саме він відправив це поштове повідомлення). Крім того, має бути встановлений зв'язок між повідомленням та обліковим записом користувача або комп'ютером, з якого було відправлено повідомлення, та людиною, яка це повідомлення відправила. У випадку, коли повідомлення було дійсно відправлено, повинен залишитись слід у вигляді доказів на кількох комп'ютерах у різних інтернет-провайдерів, які це підтверджують.

3. Повнота отриманих цифрових доказів. Цей принцип полягає в тому, що наведені цифрові докази мають показати весь спектр подій, які відбулися. Чітка і повна картина подій має бути наведена з метою виявлення, яким саме чином були залишені цифрові сліди. Цілком очевидно, що неперевірена частина неповних доказів може залишитись непоміченою, що є набагато небезпечнішим, ніж відсутність доказів взагалі. Наприклад, із IP-адреси комп'ютера користувача була здійснена DdoS-атака на державний хост – gov.ua, в результаті якої була порушена робота державних установ. Проте після всебічного аналізу цифрових слідів жорсткого диску комп'ютера було встановлено, що відбулося зараження вірусною програмою операційної системи, в результаті якого комп'ютер в автоматичному режимі здійснив DdoS-атаку без участі користувача, причому, як згодом виявилось, заражений був увесь пул (окремий сегмент) IP-адрес провайдера в окремому районі міста.

Таким чином, ураховуючи всю різноманітність процесів, які можуть відбуватися на комп'ютері та в телекомунікаційній мережі, досить важливим є завдання щодо знаходження відповідності частини доказів із їх першоджерелом та мати уявлення про всю картину подій, що відбулися.

4. Надійність отриманих цифрових доказів. Сутність цього принципу полягає в тому, що будь-які зібрані докази мають бути надійними, і це в повну міру залежить від методології та обраних інструментів отримання цифрових доказів, при цьому перевагу необхідно надавати науковому підходу. Слід підкреслити, що методи, які беруться на озброєння, мають бути достовірними і загальноприйнятими в кіберпросторі. Також необхідно звернути увагу на важливість дотримання процесуальної процедури та регламентації отримання цифрових доказів.

5. Зрозумілість та правдоподібність. Останній принцип забезпечує те, що спеціаліст (експерт) повинен у судовому засіданні чітко, зрозуміло та обґрунтовано пояснити, які прийоми він використовував під час дослідження цифрових доказів і яким чином була збережена цілісність даних. Докази мають піддаватися легкому поясненню і бути правдоподібними.

Отже, вважаємо, що вказані характеристики цифрових доказів є гарантом прийняття законних і обґрунтованих процесуальних рішень у кримінальному провадженні, а також засобом запобігання порушення прав і свобод громадян, покарання невинуватого або виправдання особи, яка вчинила злочин. Також слід зауважити, що наведений перелік не є вичерпним, та вбачається за доцільне проведення подальших досліджень цієї тематики.

Висновки. На сьогодні в Україні ще не склалася єдина судова практика стосовно допустимості та належності

цифрових (електронних) доказів, отриманих як з матеріальних носіїв інформації, так і з мережі Інтернет. Існує нагальна необхідність урегулювання цього питання як на законодавчому рівні, так і шляхом відповідних судових роз'яснень. З огляду на специфіку природи цифрових (електронних) доказів забезпечення їх достовірності в кримінальному провадженні пов'язане, перш за все, з оперативністю проведення слідчих (розшукових) дій, обов'язковим залученням спеціаліста, фаховою підготовкою всіх суб'єктів доказування, неухильним дотриманням ними рекомендацій роботи з цифровими доказами.

REFERENCE LIST

LIST OF LEGAL DOCUMENTS

LEGISLATION

1. Kryminalnyi protsesualnyi kodeks Ukrainy: Zakon Ukrainy vid 13.04.2012 № 4651-VI [Criminal Procedural Code of Ukraine: The Law of Ukraine] <http://zakon5.rada.gov.ua/laws/show/4651–17 data zvernennia 19.09.2019 [in Ukranian].

2. Pro telekomunikatsii: Zakon Ukrainy vid 18.11.2003 № 1280-IV [On telecommunications: The Law of Ukraine] <https://zakon.rada.gov.ua/laws/show/1280–15> data zvernennia 18.09.2019 [in Ukranian].

3. Pro advokaturu ta advokatsku diialnist: Zakon Ukrainy vid 05.07.2012 № 5076-VI [On the Bar and Legal Practice: The Law of Ukraine] <https://zakon.rada.gov.ua/laws/show/5076–17> data zvernennia 19.09.2019 [in Ukranian].

4. Pro notariat: Zakon Ukrainy vid 02.09.1993 № 3425-XII [On Notariate: The Law of Ukraine] <https://zakon.rada.gov.ua/laws/show/3425–12> data zvernennia 19.09.2019 [in Ukranian].

5. Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 № 2657-XII [On Information: The Law of Ukraine] <https://zakon.rada.gov.ua/laws/show/2657–12> data zvernennia 21.09.2019 [in Ukranian].

6. Pro elektronni dokumenty ta elektronnyi dokumentoobih: Zakon Ukrainy vid 22.05.2003 № 851-IV [On Electronic Documents and Electronic Documents Circulation: The Law of Ukraine] <https://zakon.rada.gov.ua/laws/show/ 851–15> data zvernennia 20.09.2019 [in Ukranian].

7. Pro zatverdzhennia poriadku pidkliuchennia do hlobalnykh merezh peredachi danykh: Postanova Kabinetu Ministriv Ukrainy vid 12.04.2002 № 522 [On approval of the procedure for connection to global data transmission networks: Resolution of the Cabinet of Ministers of Ukraine] <https://zakon.rada.gov.ua/laws/show/522–2002-p> data zvernennia 18.09.2019 [in Ukranian].

8. Pro zatverdzhennia Poriadku vchynennia notarialnykh dii notariusamy Ukrainy: Nakaz Ministerstva yustytsii Ukrainy vid 22.02.2012 № 296/5 [On approval of the Procedure of committing notarial acts by notaries of Ukraine: Order of the Ministry of Justice of Ukraine] <https://zakon.rada.gov.ua/laws/show/z0282–12> data zvernennia 18.09.2019 [in Ukranian].

9. Pro zatverdzhennia poriadku informatsiinoho napovnennia ta tekhnichnoho zabezpechennia Yedynoho veb-portalu orhaniv vykonavchoi vlad: Nakaz Derzhavnoho komitetu informatsiinoi polityky, telebachennia i radiomovlennia Ukrainy Derzhavnoho komitetu zviazku ta informatyzatsii Ukrainy vid 25.11.2002 № 327/225 [On approval of the procedure for information content and technical support of the Unified web portal of executive bodies: Order of the State Committee for Information Policy, Television and Radio Broadcasting of Ukraine of the State Committee for Communication and Informatization of Ukraine] <https://zakon.rada.gov.ua/laws/show/z1021–02> data zvernennia: 18.09.2019 [in Ukranian].

BIBLIOGRAPHY

AUTHORED BOOKS

10. Bandurka O, Blazhivskyi Ye, Burdol Ye ta in., Kryminalnyi protsesualnyi kodeks Ukrainy. Naukovo-praktychnyi komentar u 2 t [Criminal Procedural Code of Ukraine: Scientific-practical commentary in 2 vol] (Pravo 2012) 768 <https://pidruchniki.com/1250071149245/pravo/dopustimist_dokazu#888/> data zvernennia 10.09.2019 [in Ukranian].

11. Kipnis N, Dopustimost' dokazatel'stv v ugolovnom sudoproizvodstve [Admissibility of evidence in criminal proceedings] (Moskva 1995) 128 (in Russian).

12. Kessler G, Judge Awareness, Understanding, and Application of Digital Evidence (Miami Nova Southeastern University 2010) 182 [in English].

13. Kostin P, Issledovanie mashinnyh nositelej informacii pri rassledovanii prestuplenij v sfere jekonomiki [The study of computer storage media in the investigation of economic crimes] (Novgorod 2009) 193 [in Russian].

14. Shejfer S, Sushhnost' i sposoby sobiranija dokazatel'stv v sovetskom ugolovnom processe [The essence and methods of gathering evidence in the Soviet criminal process] (Moskva 1972) 130 [in Russian].

15. Shpilev V, Soderzhanie i formy ugolovnogo sudoproizvodstva [Content and forms of criminal proceedings] (Minsk 1974) 144 [in Russian].

16. Strogovich M, *Kurs sovetskogo ugolovnogo protcessa* [The course of the Soviet criminal process] (Moskva 1968) t 1. 470 [in Russian].

17. Fursa S (red), *Teoriia notarialnoho protsesu: Naukovo-praktychnyi posibnyk* [Theory of the Notarial Process: Science-Practical tutorial] (Kyiv Alerta 2012) 920 [in Ukranian].

MONOGRAPS

18. Pohoretskyi M, *Funktsionalne pryznachennia operatyvno-rozshukovoi diialnosti u kryminalnomu protsesi: monohrafiya* [Functional purpose of operative and investigative activity in criminal processes] (Kharkiv, Arsis 2007) 576 [in Ukranian].

ARTICLES

19. Aleksandrov A, Kuvychkov C, 'O nadezhnosti «elektronnyh dokazatel'stv» v ugolovnom processe' [On the reliability of «electronic evidence» in criminal proceedings] (2013) 5 Biblioteka kriminalista. Nauchnyj zhurnal 46–48 [in Russian].

20. Belkin A, 'Novelly ugolovno-processual'nogo zakonodatel'stva – shagi vpered ili vozvrat na proverennye pozicii?' [Novels of the criminal procedure legislation – steps forward or return to proven positions?] (2013) 3 Ugolovnoe sudoproizvodstvo 413 [in Russian].

21. Kudrickaja T, 'Slozhnosti sbora dokazatel'noj bazy v Internete' [The difficulty of collecting evidence on the Internet] <https://jurliga.ligazakon.net/analitycs/52188_slozhnosti-sbora-dokazatelnoy-bazy-v-internete> data zvernennja 10.09.2019 [in Russian].

22. Tkachuk O, 'Vyznannia dokaziv dopustymymy za kryminalnym protsesualnym zakonodavstvom [Recognition of evidence admissible under criminal procedural law] (2013) 1 (10) Chasopys tsyvilnoho i kryminalnoho sudochynstva 86–91 [in Ukranian].

23. Shumylo M, 'Poniattia dokaziv u kryminalnomu protsesi: prolehomeny do rozuminnia «nevlovnoho» fenomenu dokazovoho prava [The concept of evidence in criminal proceedings: prolegomena to understand the «elusive» phenomenon of evidentiary law] (2015) 3 Visnyk kryminalnoho sudochynstva 95 [in Ukranian].

DISSERTATION

24. Zigura N, 'Komp'juternaja informacija kak vid dokazatel'stv v ugolovnom processe Rossii [Computer information as a type of evidence in the criminal process of Russia] (dic kand jurid nauk. Cheljabinsk 2010) 234 [in Russian].

THE DISSERTATION AUTHOR'S ABSTRACT

25. Stepanov O, 'Nalezhnist ta dopustymist dokaziv u kryminalnomu protsesi Ukrainy [Admissibility and appropriateness of evidence in criminal proceedings of Ukraine] (avtoref dys kand yuryd nauk Kyiv 2007) 20 [in Ukranian].

CONFERENCE PAPER

26. Shumylo M, 'Hnoseolohichna i protsesualna pryroda dokaziv u kryminalnomu protsesualnomu kodeksi Ukrainy [Gnoseological and procedural nature of evidence in Criminal Procedural Code of Ukraine] Aktualni pytannia kryminalnoho protsesualnoho zakonodavstva Ukrainy (Kyiv, 26 kvit. 2013 r.): zb materialiv mizhvuz nauk konf (Alerta Nats akad prokuratury Ukrainy 2013) 13–27 [in Ukranian].

WEBSITES

27. International Organization on Computer Evidence <http://www.ioce.org/> data zvernennia 10.09.2019 [in English].

28. Scientific Working Group on Digital Evidence <https://www.swgde.org/> дата data zvernennia 10.09.2019 [in English] data zvernennia: 18.09.2019

Metelev O.,
Postgraduate student,
Departtment of criminal
ang criminal procedural law
National academy of the Security service
of Ukraine
ORCID ID: *0000–0003–2969–8388*

DOI: *https://doi.org/10.17721/2413-5372.2019.3/224-238*

PROBLEMS OF DETERMINING THE ADMISSIBILITY AND APPROPRIATENESS OF DIGITAL (ELECTRONIC) EVIDENCE IN CRIMINAL PROCEEDINGS

Annotation. *The development of information technology, along with its indisputable advantages, has brought to our lives a number of negative phenomena related to the illegal use of computers and telecommunications. However, the issue of using digital information as evidence in the criminal procedural legislation of Ukraine remains almost unsettled, in particular, the place of digital evidence in the system of procedural sources of evidence (digital evidence is difficult to unambiguously attribute to material evidence or documents) remains unclear. Criminal proceedings raise problems regarding the correct assessment of digital (electronic) evidence for their identity and admissibility, which certainly does not contribute to the effective use of digital technologies and sources of information in national proceedings.*

The purpose of the article is to research the problematic issues of determining the appropriateness and admissibility of digital (electronic) evidence during criminal proceedings, as well as to identify and disclose individual principles for their proper procedural evaluation.

The research deals with the current state of theoretical studies of the issue of the appropriateness and admissibility of digital evidence both in Ukrainian criminal procedure science and abroad. The peculiarities of the requirements for the assessment of traditional evidence and digital evidence in criminal proceedings are analyzed.

The author identifies the features of obtaining (collecting) digital evidence, given their intangible nature, with a view to their further positive evaluation by admissibility and appropriateness criteria.

Taking into account the international experience, the author concludes that there is a need to distinguish separate principles of admissibility and availability for digital evidence, revealing their content.

The urgent need to settle this issue, both at the legislative level and through appropriate judicial clarification, is substantiated. It is emphasized that in view of the specific nature of digital (electronic) evidence to ensure their authenticity and reliability in criminal proceedings is associated with the promptness of investigative actions, mandatory involvement of an expert, professional training of all subjects of evidence and steady adherence to recommendations for working with digital evidence.

Keywords*: criminal process, digital information, digital (electronic) evidence.*

Стаття надійшла до редакції журналу 30.09.2019.