Дослідницька робота

Збирання та дослідження електронних документів із застосуванням спеціальних знань

Михайло Щербаковський * [a], **Віктор Сезонов** ** [b]

* Д-р юрид. наук, професор, Харківський національний університет внутрішніх справ, м. Харків, Україна, ORCID: https://orcid.org/0000-0003-1990-1231, e-mail: shcherbakovskyi@gmail.com

** Канд. юрид. наук, доц., Харківський науково-дослідний експертно-криміналістичний центр, м. Харків, Україна, ORCID: https://orcid.org/0000-0002-2580-2953, e-mail: sv26031985@gmail.com

[a] Написання оригінального рукопису, адміністрування проєкту, нагляд.
[b] Написання оригінального рукопису, методологія.

DOI: 10.32353/khrife.3.2024.02 УДК 343.98
Надійшло 13.06.2024 / Рецензовано 17.06.2024 / Прийнято до друку 25.09.2024 / Доступно онлайн 30.09.2024

Мета роботи — за допомогою сучасних загальних і спеціальних методів наукового пізнання дослідити сутність, форму електронних документів та їхніх носіїв, особливості залучення спеціалістів і експертів до їхнього пошуку, фіксування та дослідження. Доведено, що сутність понять «електронна (цифрова) інформація», «комп'ютерні дані», «електронний документ» у кримінальному процесуальному аспекті слід розглядати як тотожні. Показано, що у широкому значенні електронним документом є будь-яка інформація, представлена в електронній формі, у вузькому розумінні — це документ, що має обов'язкові електронні реквізити. Аргументовано, що електронні документи вміщено на речових або електронних носіях у формі файлів. Речовими носіями є цифрові пристрої, на яких зберігають електронні документи, а електронними носіями (електронним середовищем) — глобальні або локальні мережі, хмарні сховища, різноманітні електронні реєстри. Обґрунтовано, що у кримінальному провадженні речові носії є речовими доказами (ст. 98 Кримінального процесуального кодексу України) або додатками до протоколів слідчих дій у вигляді носіїв копій електронних документів (ст. 105 цього Кодексу), а вилучені з електронних носіїв документи — доку-

ментами-доказами (ст. 99 цього Кодексу). Для допустимості електронних документів як доказів у кримінальному провадженні під час проведення слідчих дій з пошуку, виявлення та фіксування електронних документів за участі спеціаліста з інформаційних технологій рекомендовано обов'язково фіксувати (письмово у протоколі або за допомогою відеозапису) усі операції спеціаліста з носієм електронних документів або призначати на місці огляду (обшуку) експертизу електронних комунікацій чи комп'ютерно-технічну експертизу.

Ключові слова: *електронні документи; електронна (цифрова) інформація; носії інформації; комп'ютерні дані; цифрові докази; спеціальні знання; спеціаліст; експерт; судова експертиза.*

Постановка наукової проблеми

Сьогодні новітніми інформаційними технологіями активно послуговуються в повсякденній діяльності: вони стали невід'ємною складовою сучасного суспільства. Водночас інформаційні технології застосовують також у протиправній діяльності (для створення шкідливих програм, підроблених документів, утручання в комп'ютери й комп'ютерні мережі, скоєння шахрайських дій, розкрадань та інших правопорушень) як складову способу скоєння злочинів. Особливо активно сучасні правопорушники використовують ресурси й можливості інтернету, соціальних мереж, сервіси електронної пошти й миттєвих повідомлень, засоби анонімізації та віддаленого доступу, технології створення й поширення непідтверджених фактів та ін. Отже, багато доказів у кримінальних провадженнях сьогодні мають цифровий (електронний) вигляд, що зумовлює їхнє збирання, зберігання, опрацювання й аналізування під час кримінального провадження. Інформація в електронній (цифровій) формі містить віртуальні активи, вебсайти, вебсторінки, текстові та графічні зображення, плани, фотографії, відео- і звукозаписи, мультимедійні й голосові повідомлення, бази даних та інші складові, які можна вважати електронними документами.

Не потребує доведення необхідність новацій у кримінально-процесуальній сфері, у способах та інструментальних методах здійснення пошуку, огляду, вилучення й дослідження електронних документів. Незважаючи на наявність окремих законодавчих актів, численних наукових публікацій і методичних рекомендацій, у кримінальному процесі залишається низка проблем, пов'язаних із трактуванням понять «цифрова інформація», «електронні документи», «комп'ютерні дані», «цифрові докази», що негативно позначається на слідчо-судовій практиці. З урахуванням особливостей електронних документів нагальними є питання перетворення їх на докази, розроблення правил щодо збирання, збереження, дослідження та використання цифрової інформації в доказуванні на підставі спеціальних знань.

Проблеми збирання та дослідження електронних документів, що утворюються безпосередньо в комп'ютерних засобах і їхніх системах, на носіях інформації, у віртуальному середовищі обумовлені передусім необхідністю застосування

спеціальних знань. Під час розслідування кримінальних правопорушень труднощі в роботі з електронними документами обумовлені прогалинами законодавства, недостатніми знаннями правозастосовників у галузі комп'ютерних технологій, необхідністю використання складного ліцензійного обладнання, обов'язкового залучення до проведення слідчих (розшукових) дій фахівців різного профілю. Останніми роками електронні документи стали об'єктами дослідження в багатьох видах судових експертиз, що спричинило цілу низку теоретичних, правових та організаційних проблем, істотно вплинуло на методологію й методику експертного дослідження, компетенцію судових експертів.

Мета статті

Визначити сутність, форму електронних документів і їхніх носіїв, особливості залучення спеціалістів та експертів до їх пошуку, фіксування й дослідження.

Методи дослідження

Під час дослідження застосовано загальні та спеціальні методи наукового пізнання. Для узагальнення матеріалів із літературних джерел, позицій авторів з окремих питань, що належать до предмета дослідження, стали в пригоді теоретичний аналіз і синтез (індукція, дедукція, порівняння, аналогія, абстрагування, класифікація); розгляд та обґрунтування поняття електронних документів, їх значення у процесі доказування здійснено системно-структурним методом; формально-юридичний метод допоміг розкрити особливості та критерії залучення спеціаліста до слідчих дій. Названі методи використано як взаємопов'язані та взаємодоповнювальні, що сприяло повноті дослідження й обґрунтованості сформульованих наукових висновків і пропозицій.

Аналіз основних досліджень і публікацій

Поняття, види, способи збирання та дослідження електронних документів й цифрових доказів у кримінальному процесі аналізували вітчизняні вчені Г. Авдєєва, Д. Алєксєєва-Процюк, Н. Ахтирська, О. Брисковська, О. Гарасимів, С. Гонгало, М. Гуцалюк, І. Г. Каланча, А. Коваленко, І. Крицька, С. Марко, Ю. Орлов, Л. Остапчук, А. Ратнова, О. Ряшко, О. Самойленко, А. Скрипник, І. Смаль, А. Столітній, І. Хараберюш, В. Хахановський, А. Хитра, Д. Цехан, С. Чернявський, Г. Чигрина та ін. Низку праць згадані й інші автори присвятили, зокрема, проблемам залучення обізнаних осіб до збирання та дослідження електронних документів. Проте окремі аспекти суті електронних документів, використання спеціальних знань щодо їх виявлення, фіксування, вилучення та дослідження проаналізовано не повною мірою, що зумовлює необхідність більш ґрунтовно проаналізувати окреслену проблематику.

Викладення основного матеріалу дослідження

З урахуванням відсутності в доктрині кримінального процесуального права України визначення поняття «електронні документи», у контексті розкриття мети нашого дослідження важливо з'ясувати сутність, особливості цих об'єктів, зв'язок з іншими дотичними категоріями інформаційних технологій.

У сучасному вітчизняному законодавстві загальне поняття «документ» трактовано як «*матеріальний носій, що*

містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі» [1] або як *«матеріальна форма одержання, зберігання, використання і поширення інформації, зафіксованої на папері, магнітній, кіно-, фотоплівці, оптичному диску або іншому носієві»* [2]. Дещо інші визначення поняття «документ» містив не чинний нині ДСТУ 2732:2004 (який поступився місцем ДСТУ 2732:2023) — *«інформація, зафіксована на матеріальному носії, основною функцією якого є зберігати та передавати її в часі та просторі»* [3]. Отже, у різний час законодавці давали різні визначення: з одного боку, документ сприймали як матеріальний носій інформації, з іншого — як саму інформацію. Проте ці поняття не є тотожними.

Інформацію визначено як *«будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді»* [4]. Електронну (цифрову) інформацію (цифровий контент) становлять *«будь-які відомості чи дані в електронній (цифровій) формі, що містять об'єкти авторського права та/або суміжних прав і можуть зберігатися та/або поширюватися у вигляді одного або декількох файлів (частин файлів), записів у базі даних на зберігаючих пристроях комп'ютерів, серверів тощо у мережі "Інтернет"»* [5].

У Кримінальному процесуальному кодексі України (далі — *КПК України*) відсутнє поняття «електронна цифрова інформація», але згадано «комп'ютерні дані», огляд яких слідчий, прокурор проводять відповідно до ст. 237 [6]. Поняття «комп'ютерні дані» у нормативно-правових документах визначено як *«будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою»* [7], «дані» сформульовано як інформацію, подану *«у формі, придатній для її оброблення електронними засобами»* [8], а «електронні дані» — як будь-яку інформацію *«в електронній формі»* [9]. Варто

1 Про інформацію : Закон України від 02.10.1992 р. № 2657-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 02.06.2024).

2 Про обов'язковий примірник документів : Закон України від 09.04.1999 р. № 595-XIV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/595-14#Text (дата звернення: 02.06.2024).

3 ДСТУ 2732:2004 Діловодство й архівна справа. Терміни та визначення понять [Не чинний від 29.02.2024]. Київ, 2005. С. 2. URL: http://old.loga.gov.ua/netcat_files/4895/4106/h_7d602cb292dd3a86478915757d0425f9 (дата звернення: 20.08.2024).

4 Про інформацію … . URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 20.08.2024).

5 Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text (дата звернення: 02.06.2024).

6 Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.05.2024).

7 Конвенція про кіберзлочинність : прийнята Ком. міністр. Ради Європи 08.11.2001 р. ; ратифік. Законом України від 07.09.2005 р. № 2824-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 02.06.2024).

8 Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 02.06.2024).

9 Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 02.06.2024).

зауважити, що за своєю суттю електронна (цифрова) інформація є двійковим кодом, записаним за допомогою нулів та одиниць і призначеним для зчитування, опрацювання та передавання за допомогою інформаційних технологій. У первинному вигляді вона не придатна для людського сприйняття: лише комп'ютерні засоби перетворюють її на зрозумілу для людей.

Важливою характеристикою електронних документів є спосіб їх зберігання у форматі файлу, який науковці пропонують розглядати як кримінально-процесуальну форму цифрової інформації [10]. Існують різноманітні формати файлів, використовувані для підготовки, опрацювання, зберігання електронних документів. Формати файлів зазвичай поділяють на текстові (*txt, rtf, pdf, doc* (*docx*) та ін.), графічні (векторні *dxf, tps, cgm* та ін.; растрові *bmp, tiff, gif, jpeg* та ін.), електронних таблиць, баз даних, відео- та аудіо, архівного зберігання (*pdf-a* та ін.) і так звані мови розмітки, що дають змогу відобразити інформацію про документ (*sgml, html, xml*).

Законодавці визначають електронний документ як «*документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа*» [11]. Науковці називають електронним документом інформацію в електронній (цифровій) формі, яку можна використати «*як доказ факту чи обставин, що встановлюються під час кримінального провадження*» [12]. Аналізування наведених формулювань дає підстави вважати, що у кримінально-процесуальному аспекті поняттями «електронна (цифрова) інформація», «комп'ютерні дані», «електронний документ» можна послуговуватися як синонімами. Однак з практичної та процесуальної позицій доцільно виокремити поняття електронних документів у широкому та вузькому сенсах. У першому значенні електронним документом слід уважати будь-яку інформацію, представлену в електронній формі, формування й існування якої відбуваються завдяки спеціальним програмно-технічним засобам [13]. Варто зауважити, що поняття електронного документа в широкому розумінні охоплює багато різних категорій, а саме: документи бухгалтерської та податкової звітності, інтернет-сторінки, вебсайти, аудіо- й відеозаписи, які створені, передані, отримані в електронній формі, сторінки месенджерів, листування через e-mail тощо. У вузькому значенні електронний документ — це документ, що має електронні реквізити — обов'язкові дані (наприклад, електронний підпис або електронну печатку), без яких він не може бути підставою для його обліку й не матиме юридичної сили. Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі,

10 Метелев О. П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства*. 2023. № 1—2. С. 50. DOI: 10.17721/2413-5372.2023.1-2/42-53 (дата звернення: 02.06.2024).

11 Про електронні документи … . URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 02.06.2024).

12 Остапчук Л. Г., Смаль І. А. До питання правової природи електронного документу та його місця у системі доказів кримінального процесу. *Прикарпатський юридичний вісник*. 2022. Вип. 2 (43). С. 124. DOI: 10.32837/pyuv.v0i2.1028 (дата звернення: 02.06.2024).

13 Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Серія: Право*. 2017. № 4 (58). С. 81. URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf (дата звернення: 02.06.2024).

придатній для сприйняття його змісту людиною [14].

Поняття електронного документа невіддільне від його носія — матеріального об'єкта або середовища, які здатні зберігати у своїй структурі внесену інформацію. Носій для збереження електронних (цифрових) даних визначено як «*матеріальний носій, який використовують для записування, зберігання та відтворення інформації, обробленої засобами комп'ютерної техніки*» [15]. Із метою більш ефективного застосування спеціальних знань для збирання та дослідження носіїв електронних документів і зважаючи на їхню природу, такі носії з позицій доказування доцільно об'єднати у дві групи: речові й електронні. Речові носії під час розслідування важливі як об'єкти, що безпосередньо містять криміналістично значущу для доказування інформацію у формі файлів електронних документів. Електронні документи в цьому випадку мають доказове значення, коли вони поєднані з конкретним матеріальним носієм, вилученим у встановленому місці, у конкретної особи за певних обставин як доказ факту або обставин, що їх з'ясовують під час кримінального провадження. Речовими носіями можуть бути: об'єкт для зберігання цифрових даних, використовуваний у стандартних комп'ютерах (жорсткі, гнучкі, оптичні, магнітооптичні диски; цифрові пристрої з подібними функціями); мобільні телефони, персональні цифрові помічники (*PDAs*), персональні електронні прилади (*PEDs*), карти пам'яті; мобільні навігаційні системи; цифрові фото- та відеокамери (зокрема, *CCTV*); стандартний комп'ютер з мережевими з'єднаннями; мережі, базовані на *TCP/IP* та інших цифрових протоколах, а також прилади з функціями, подібними наведеним вище [16].

Електронними носіями документів є електронне середовище — глобальні й локальні мережі, хмарні сховища, різноманітні електронні реєстри (зброї, речових прав на нерухоме майно, прав власності на нерухоме майно, іпотек, заборон відчуження об'єктів нерухомого майна, відшкодування податку на додану вартість та ін.). Завдяки лише тій інформації, яку вони містять, електронні документи мають самостійне доказове значення безвідносно до речового носія. Запропонований поділ носіїв електронних документів співвідноситься з рішеннями Верховного Суду України, згідно з якими головною особливістю електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія, який є лише способом збереження інформації та має значення тільки тоді, коли електронний документ є речовим доказом. Той самий електронний документ може існувати на різних носіях. Усі «*ідентичні за своїм змістом примірники електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом та датою створення*» [17].

14 Про електронні документи … . URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 02.06.2024).

15 ДСТУ 7448:2013 Інформація та документація. Бібліотечно-інформаційна діяльність. Терміни та визначення понять [Чинний від 01.07.2014]. Київ, 2014. 42 с. URL: https://lib.nure.ua/storage/app/media/nmbk/doc/dstu.pdf (дата звернення: 02.06.2024).

16 ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT) [Чинний від 01.01.2019]. Київ, 2018. 31 с. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (дата звернення: 02.06.2024).

17 Постанова Верховн. Суду України від 10.09.2020 р., справа № 751/6069/19, провадж. № 51-1704км20 / ЄДРСР : офіц. сайт. URL: https://reyestr.court.gov.ua/Review/91722819 (дата звернення: 02.06.2024) ; Постанова Верховн. Суду України від 26.01.2021 р., справа

Підсумовуючи викладене, доходимо висновку, що певний речовий або електронний носій може містити електронний документ (цифрову інформацію) у формі відповідного файлу.

Електронний документ набуває статусу доказової інформації лише тоді, коли його знайдено, а його зміст, особливі ознаки й характеристики тощо задокументовано й перетворено на письмово-образотворчий документ, доступний для однозначного сприйняття всіма учасниками кримінального провадження. Для того щоб використати електронні документи під час кримінального провадження як докази, їх потрібно отримати в передбаченому процесуальним законом порядку [18]. Необхідність використовувати електронні документи (комп'ютерні дані, електронну (цифрову) інформацію) у доказуванні спричинило жваву дискусію серед науковців щодо виокремлення нового виду джерел — «цифрового доказу» [19]. Слід підтримати пропозицію про законодавче закріплення у КПК України визначення поняття «електронні (цифрові) докази», як це сформульовано у ст. 100 Цивільного процесуального кодексу України [20] або Міжнародному стандарті ISO/IEC 27037:2017 [21]. Проте в межах чинного кримінального процесуального законодавства вчені та практики пропонують розглядати електронні документи як документи-докази [22], як речові докази [23] або як обидві ці категорії [24]. Наш підхід ґрунтується на запропонованому поділі носіїв електронних документів,

№ 236/4268/18, провадж. № 51-3124км20 / Там само. URL: https://reyestr.court.gov.ua/Review/94905297 (дата звернення: 02.06.2024).

18 Авдєєва Г. К. Проблеми визначення достовірності цифрових доказів у кримінальному провадженні. *Вісник Луганського навчально-наукового інституту імені Е. О. Дідоренка*. 2024. Вип. 1 (105). С. 33—48. DOI: 10.33766/2786-9156.105.33-48 (дата звернення: 02.06.2024).

19 Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : кол. моногр. Львів, 2022. С. 34. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%d0%93%d1%83%d1%82%d0%bd%d0%b8%d0%ba%2c%20%d0%a5%d0%b8%d1%82%d1%80%d0%b0_%d0%bc%d0%be%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d1%96%d1%8f_21_06_2022.pdf (дата звернення: 02.06.2024) ; Ковальчук С. О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи : дис. … д-ра юрид. наук. Одеса, 2018. С. 154. URL: https://dspace.onua.edu.ua/bitstreams/94e3af63-a41b-4f31-8a68-07c2b8bc430b/download (дата звернення: 02.06.2024) ; Скрипник А. В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні : дис. … д-ра філос. у галузі права. Харків, 2021. С. 102.

20 Цивільний процесуальний кодекс України від 18.03.2004 р. № 1618-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення: 02.06.2024).

21 ДСТУ ISO/IEC 27037:2017. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (дата звернення: 02.06.2024).

22 Бідняк Г. С. Використання спеціальних знань при розслідуванні шахрайств : дис. … канд. юрид. наук. Дніпро, 2018. С. 142 ; Гонгало С. Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку : дис. … канд. юрид. наук. Київ, 2013. С. 121.

23 Крицька І. О. Речові докази у кримінальному провадженні : монографія. Харків, 2018. С. 67 ; Гутник А. В., Хитра А. Я. Зазнач. твір. С. 25. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%d0%93%d1%83%d1%82%d0%bd%d0%b8%d0%ba%2c%20%d0%a5%d0%b8%d1%82%d1%80%d0%b0_%d0%bc%d0%be%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d1%96%d1%8f_21_06_2022.pdf (дата звернення: 02.06.2024).

24 Остапчук Л. Г., Смаль І. А. Зазнач. твір. DOI: 10.32837/pyuv.v0i2.1028 (дата звернення: 02.06.2024).

згідно з яким вилучені з електронних носіїв документи слід уважати документами-доказами (ст. 99 КПК України), а речові носії — речовими доказами (ст. 98 КПК України) або додатками до протоколів слідчих і негласних слідчих (розшукових) дій у вигляді дисків, флеш-накопичувачів з копіями документів (ст. 105 КПК України) [25]. Підкреслимо, що відповідно до нашої концепції речовим доказом є саме речовий носій, а не електронний документ, який є своєрідною ознакою, характеристикою носія й не має самостійного доказового значення.

Незважаючи на наявну правову колізію, законодавці передбачили певний перелік слідчих дій, спрямованих на формування джерел доказів, змістом яких є електронні документи, з урахуванням особливостей носіїв і методів роботи з ними. Так, електронні документи у вигляді комп'ютерних даних можна виявити в разі тимчасового доступу до електронних інформаційних систем, комп'ютерних систем або їхніх частин, мобільних терміналів систем зв'язку (ст. 160 КПК України), обшуку (ст. 236 КПК України), огляду (ст. 237 КПК України), зняття інформації з електронних комунікаційних мереж (ст. 263 КПК України) або електронних інформаційних систем (ст. 264 КПК України) [26]. Під час проведення процесуальних дій допускається повне копіювання інформації з об'єктів огляду, обшуку, доступу; за потреби для виявлення кримінально релевантної інформації призначають експертизу за ст. 242 КПК України [27] (у нашому випадку — комп'ютерно-технічну експертизу вилучених речових доказів або носіїв скопійованої інформації).

Неможливість безпосереднього сприйняття електронного документа та необхідність застосування для цього програмно-технічних засобів — одна з найважливіших особливостей цього об'єкта, що відрізняє його від аналогових документів (документів на паперовому носії) і потребує послуговування спеціальними знаннями для надання такому електронному документу доступного для сприйняття учасниками кримінального провадження вигляду. Особливості пошуку, фіксування та копіювання комп'ютерних даних під час слідчих дій широко висвітлено у криміналістичній літературі [28]. Водночас низка проблем щодо застосування спеціальних знань для збирання та дослідження електронних документів під час кримінального провадження залишається не розв'язаною.

Одним із провідних учасників слідчих дій, пов'язаних із виявленням і вилученням електронних документів,

25 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.05.2024).

26 Там само.

27 Там само.

28 Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Науковий вісник Херсонського державного університету. Серія: юридичні науки.* 2023. Вип. 4. С. 53—58. DOI: 10.32999/ksu2307-8049/2023-4-9 (дата звернення: 02.06.2024) ; Лісніченко Д. В. Особливості вилучення за допомогою технічних засобів інформації з мобільних терміналів зв'язку (смартфонів) під час кримінального провадження. *Південноукраїнський правничий часопис.* 2022. Вип. 1—2. С. 120—125. DOI: 10.32850/sulj.2022.1-2.22 (дата звернення: 02.06.2024) ; Чигрина Г. Електронні документи: залучення спеціаліста до збирання та використання під час кримінального провадження. *Jurnalul juridic naţional: teorie şi practică.* 2017. № 3. С. 134—137. URL: http://www.jurnaluljuridic.in.ua/archive/2017/3/30.pdf (дата звернення: 02.06.2024).

є спеціаліст (ст. 71 КПК України) [29], що зумовлено необхідністю надати електронним документам візуально доступну для сприйняття учасниками процесу форму, застосувати конкретні методи й технічні засоби з виявлення та збереження необхідної інформації з метою її подальшого експертного дослідження. Як і будь-якого учасника слідчої дії, спеціаліста наділено особливими правами й обов'язками щодо застосування ним спеціальних знань. Спеціаліста з інформаційних технологій залучають до пошуку, фіксування та вилучення електронних документів.

Перше, на що необхідно звернути увагу,— це ситуаційність залучення спеціаліста, яка впливає на необхідність застосування спеціальних знань, вибір спеціаліста, засобів, прийомів пошуку, фіксування та збереження електронних документів. Загальний алгоритм огляду окремого речового носія містить такі етапи: 1) зовнішній огляд та ідентифікація; 2) перевірка наявності кабельних або бездротових підключень (адаптерів сотового, безконтактного зв'язку та ін.), від'єднання кабелів і зовнішніх пристроїв; 3) огляд комп'ютерної інформації (установлених і використовуваних додатків, файлової системи, запущених процесів) на носії; 4) збереження (копіювання) інформації з оперативної пам'яті; 5) штатне вимкнення пристрою та копіювання постійної пам'яті (твердого носія або жорсткого магнітного диска); 6) складання протоколу й пакування вилученого з урахуванням типу носія та можливості бездротового управління ним. Не в усіх слідчих ситуаціях потрібна участь спеціаліста з інформаційних технологій. У простих ситуаціях, коли речовий носій перебуває у вимкненому стані і його слід вилучити як речовий доказ; коли носій незаблокований, слідчому точно відомо найменування документа (файлу, вебсторінки тощо) і немає потреби у його пошуку, можна обійтися без залучення спеціаліста. Огляд і фіксування зображення документа цілком доступні слідчому, який має початкові навички роботи з комп'ютером. Для етапів 1, 2 та 6 достатньо фотокамери, переносного робочого комп'ютера (ноутбука) слідчого з типовим набором програм і друкарського пристрою (принтера), щипців і екрануючої обгортки з пакуванням. Складна, проблемна ситуація виникає через відсутність пароля доступу до роботи на комп'ютерному засобі; невідому наявність і найменування документа, що має значення для розслідування; необхідність повного копіювання інформаційного вмісту речового носія в разі неможливості вилучити сам носій інформації або зупинити (вимкнути) автоматизовані системи. Здійснення етапів 3, 4 і 5 потребує застосування додаткових спеціальних знань та інструментальних засобів. У цій ситуації залучення спеціаліста з інформаційних технологій є обов'язковим.

Необхідність обов'язкового залучення спеціаліста обумовлено труднощами, що пов'язані з пошуком і виявленням на носіях електронних документів, важливих для розслідування, особливо актуальні під час огляду (обшуку) великих комп'ютерних мереж, функціювання яких призупинити неможливо через їхню критичну важливість для виробничих процесів, які не можна переривати. До того ж вилучити їх цілком з місця злочину найчастіше технічно неможливо, а навіть якби й можливо, то значні обсяги інформації, яка підлягає вивченню, робили б це недоцільним. У такій ситуації слід виявити в мережі конкрет-

29 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.05.2024).

ні пристрої з необхідною інформацією, локалізувати їх і досліджувати окремо. Комп'ютерна система навіть найпростішої корпоративної мережі містить робочі станції співробітників, сервери, зокрема поштові та проксі, контролери доменів, маршрутизатори, комутатори, кабельну систему. Елементи мережі (кабельної та бездротової, корпоративної або локальної мережі та цілі її сегменти) можуть розташувати не тільки в різних приміщеннях будівлі, а й у різних географічних регіонах (наприклад, якщо для організації мережі застосовано технології віртуальних (логічних) каналів, трансграничної, хмарної системи, то опрацювання інформації, що є найбільш складним під час організації та проведення огляду, потребує обов'язкового застосування інструментальних засобів і методів). Аналогічна ситуація може виникнути на місці огляду (обшуку) у разі виявлення цифрових пристроїв, підключених до віддаленого сховища інформації, зокрема хмарного, або під час огляду приміщення провайдера хостингових послуг, що надає в оренду обчислювальні потужності, сервери, які фізично розміщено в різних регіонах країни або зашифровано. У відповідних методичних рекомендаціях спеціалістові запропоновано, наприклад, здійснити пошук документів у віддаленому ресурсі комп'ютерної мережі, подолати блокування комп'ютера й виконати інші маніпуляції [30]. За таких обставин багаторазово зростає роль спеціаліста, який уже не має виконувати рутинних дій: тепер на нього чекає тривала творча дослідна робота. У такій ситуації участь спеціаліста в галузі інформаційних технологій під час проведення слідчих дій полягає у здійсненні маніпуляцій з комп'ютерними засобами, недоступних і здебільшого незрозумілих учасникам слідчої дії: слідчому, понятим, власникам засобів.

У протоколі слідчої дії (відповідно до ст. 103 КПК України) необхідно обов'язково описати всі операції та переходи, здійснені під час проведення огляду (обшуку) комп'ютерного засобу [31]. Водночас, як зазначено вище, ці дії неочевидні для решти учасників, ще й можуть тривати довше за розумний строк проведення слідчої дії, до того ж спеціаліст своїми діями робить у цифровому середовищі зміни, не пов'язані з кримінальним правопорушенням.

Для забезпечення допустимості електронних документів як доказів, отриманих під час проведення слідчих дій за участі спеціаліста з інформаційних технологій, можна рекомендувати два способи. Перший — фіксування кожної дії спеціаліста (відеофіксування, роздруківка, скриншоти вебсторінок тощо) з тим, щоб у разі виникнення сумнівів у правильності отримання електронних документів переглянути й перевірити кожну операцію спеціаліста з речовим або електронним носієм. Другим способом (коли пошук електронних документів як у речових носіях, так і в кіберпросторі потребує складних маніпуляцій із застосуванням програмних і технічних засобів) є призначення судової експертизи на місці

30 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / за заг. ред. О. В. Корнейка. Київ, 2020. Вид. 2-ге., допов. С. 23, 29. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content (дата звернення: 02.06.2024).

31 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.05.2024).

проведення огляду (обшуку) [32]. У такому разі увесь процес пошуку та фіксування електронних документів описують у дослідницької частині висновку експерта.

Іще одною проблемою, якій не приділено достатньої уваги, є визначення компетенції спеціаліста, залученого до слідчих дій. У галузі знань «Інформаційні технології» (відповідно до постанови Кабінету Міністрів України) набувають різних спеціальностей: «Інженерія програмного забезпечення», «Комп'ютерні науки», «Комп'ютерна інженерія», «Системний аналіз», «Кібербезпека та захист інформації», «Інформаційні системи та технології» [33], кожна з яких має специфічний предмет, пов'язаний із програмним забезпеченням; програмно-технічними засобами; інформаційними технологіями; телекомунікаційними системами, збиранням, представленням, опрацюванням, зберіганням, передаванням і доступом до інформації в комп'ютерних системах тощо. Саме тому на підготовчому етапі проведення слідчих дій слідчий має окреслити мету огляду (обшуку), особливості носія електронних документів, їхній вид і вигляд та визначитися із компетенцією спеціаліста.

Експертне дослідження електронних документів — основна процесуальна форма застосування спеціальних знань. Речові докази, складовою яких є електронні документи, а також копії цих документів, що є додатками до протоколів слідчих дій, є процесуальними об'єктами досліджень у таких експертизах: відео- та звукозапису, лінгвістичній, фототехнічній, портретній, економічній, технічній документів. Відповідно до положень судової експертології безпосередніми об'єктами досліджень цих експертиз є, відповідно, зображення, фізичні параметри звуку, усне мовлення, зовнішність людини, бухгалтерські й інші документи та ін. Електронні документи, що підлягають експертному дослідженню в названих експертизах, заздалегідь відомі слідчому, їх зазначають у питаннях експертові. Інша ситуація стосується судової комп'ютерно-технічної експертизи, типовим завданням якої є пошук і виявлення невідомих слідчому електронних документів (інформації, програмного забезпечення), що містяться на речових доказах — комп'ютерних засобах або носіях-додатках до слідчих дій [34]. Уважаємо, що такі завдання можна поставити в межах експертизи електронних комунікацій для пошуку конкретних документів в електронному носії — кіберпросторі [35]. Безпосередніми експертними об'єктами цих експертиз є зміст і параметри (метадані) документів. Виявлені у такий спосіб електронні документи можуть стати об'єктами подальших

32 Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів : навч. посіб. Харків, 2010. 116 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/2b0c8656-bc78-4c21-8ff0-3808403f00ca/content (дата звернення: 02.06.2024).

33 Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : затв. постанов. КМУ від 29.04.2015 р. № 266 (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF#n11 (дата звернення: 02.06.2024).

34 Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень : затв. наказ. Мін'юсту України від 08.10.1998 р. № 53/5 (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення 15.08.2024).

35 Щербаковський М. Відкриті джерела кіберпростору як об'єкти судово-експертного дослідження. *Теорія та практика судової експертизи і криміналістики.* 2024. Вип. 2 (35). С. 10—27. DOI: 10.32353/khrife.2.2024.02 (дата звернення: 02.07.2024).

експертних досліджень однорідних або комплексних експертиз.

Висновки

Поняття «електронна (цифрова) інформація», «комп'ютерні дані», «електронний документ» за своєї суттю в кримінальному процесуальному аспекті тотожні. У широкому значенні електронним документом є будь-яка інформація, представлена в електронній формі, у вузькому розумінні — це документ, що має обов'язкові електронні реквізити.

Речові або електронні носії уміщують електронні документи у формі файлів. Речовими носіями є цифрові пристрої, на яких зберігаються електронні документи. Електронні носії — це електронне середовище: глобальні або локальні мережі, хмарні сховища, різноманітні електронні реєстри. У кримінальному провадженні речові носії є речовими доказами (ст. 98 КПК України) або додатками до протоколів слідчих дій у вигляді носіїв копій електронних документів (ст. 105 КПК України), а вилучені з електронних носіїв документи є документами-доказами (ст. 99 КПК України).

На етапі підготовки до проведення процесуальної дії, залежно від особливостей носія електронних документів, слідчий має визначитися із компетенцією спеціаліста відповідно до спеціальностей, що належать до галузі знань «Інформаційні технології».

Для допустимості електронних документів як доказів у кримінальному провадженні під час проведення слідчих дій з пошуку, виявлення та фіксування електронних документів за участі спеціаліста з інформаційних технологій рекомендовано обов'язково фіксувати (письмово у протоколі або за допомогою відеозапису) усі операції спеціаліста з носієм електронних документів або призначати на місці огляду (обшуку) експертизу електронних комунікацій чи комп'ютерно-технічну експертизу.

Collection and research on electronic documents using specific expertise

Mykhailo Shcherbakovskyi, Viktor Sezonov

This research paper purpose is to use modern general and special methods of scientific knowledge to investigate the essence, form of electronic documents and their carriers, the specifics of the involvement of specialists and experts in their search, recording and research. It has been proven that the essence of the concepts «electronic (digital) information», «electronic data», «electronic document» in the criminal procedural aspect should be considered identical. It is shown that in the broadest sense an electronic document is any information presented in electronic form, in a narrow sense it is a document with mandatory electronic details. It is argued that electronic documents are placed on physical or electronic media in the form of files. Physical media are digital devices on which electronic documents are stored, and electronic media (electronic environment) are global or local networks, cloud storage, various electronic registers. It is substantiated that in criminal proceedings physical media are physical evidence (Article 98 of Criminal Procedural Code of Ukraine) or appendices to the protocols of investigative actions in the form of carriers of copies of electronic documents (Article 105 of this Code), and documents removed from electronic media are evidence documents (Article 99 of this Code). For admissibility of electronic documents as evidence in criminal proceedings during investigative actions for the search, detection and recording of electronic documents with the participation of an information technology specialist, it is recommended to necessarily record (in writing in the protocol or with the help of a video recording) all operations

of the specialist with the carrier of electronic documents or appoint an electronic communications examination or a computer examination at the place of inspection (search).

Keywords: *electronic documents; electronic (digital) information; information carriers; electronic data; digital evidence; specific expertise; specialist; forensic expert; forensic science.*

Фінансування
Це дослідження не отримало жодного спеціального гранту від фінансових установ у державному, комерційному або некомерційному секторах.

Відмова від відповідальності
Засновники не грали жодної ролі у розробленні дослідження, добиранні й аналізуванні даних, рішенні про публікацію або підготовку рукопису.

Учасники
Автори зробили свій внесок винятково в інтелектуальну дискусію, що є основою цього документа, дослідження судової практики, написання та редагування, і бере на себе відповідальність за її зміст і тлумачення.

Декларація щодо конфлікту інтересів
Автори заявляють, що у них відсутній конфлікт інтересів, що стосується цієї теми; хоча Михайло Щербаковський є членом консультативної ради збірника, він не брав участі в ухваленні рішення щодо оприлюднення, і цю статтю піддано повному процесу експертної перевірки та редагування.

References

Avdieieva, H. K. (2024). Problemy vyznachennia dostovirnosti tsyfrovykh dokaziv u kryminalnomu provadzhennia [Problems of determining the reliability of digital evidence in criminal proceedings]. *Visnyk Luhanskoho navchalno-naukovoho instytutu imeni E. O. Didorenka*. Vyp. 1 (105). DOI: 10.33766/2786-9156.105.33-48 [in Ukrainian].

Bidniak, H. S. (2018). *Vykorystannia spetsialnykh znan pry rozsliduvanni shakhraistv* [Specific expertise use in the investigation of fraud] : dys. ... kand. yuryd. nauk. Dnipro [in Ukrainian].

Chyhryna, H. (2017). Elektronni dokumenty: zaluchennia spetsialista do zbyrannia ta vykorystannia pid chas kryminalnoho provadzhennia [Electronic documents: the involvement of a specialist in the collection and use during criminal proceedings]. *Jurnalul juridic național: teorie* și *practică*. № 3. URL: http://www.jurnaluljuridic.in.ua/archive/2017/3/30.pdf [in Ukrainian].

Honhalo, S. Y. (2013). *Sudova tekhniko-kryminalistychna ekspertyza dokumentiv: suchasni mozhlyvosti doslidzhennia ta perspektyvy rozvytku* [Forensic examination of documents: modern research opportunities and development prospects] : dys. ... kand. yuryd. nauk. Kyiv. [in Ukrainian].

Hutnyk, A. V., Khytra, A. Ya. (2022). *Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv* u *dokazuvanni* [Criminal procedural and forensic bases for the use of electronic documents in evidence] : kol. monohr. Lviv. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%d0%93%d1%83%d1%82%d0%bd%d0%b8%d0%ba%2c%20%d0%a5%d0%b8%d1%82%d1%80%d0%b0_%d0%bc%d0%be%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d1%96%d1%8f_21_06_2022.pdf [in Ukrainian].

Hutsaliuk, M. V., Havlovskyi, V. D., Khakhanovskyi, V. H. ta in. (2020). *Vykorystannia elektronnykh (tsyfrovykh) dokaziv* u *kryminalnykh provadzhenniakh* [Use of electronic (digital) evidence in criminal proceedings] : metod. rek. / za zah. red. O. V. Korneika. Kyiv. Vyd. 2-he., dopov. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content [in Ukrainian].

Khyzhniak, Ye. C. (2017). Osoblyvosti ohliadu elektronnykh dokumentiv pid chas rozsliduvannia kryminalnykh pravoporushen [Peculiaritiea of the digital document review during the investigation of criminal offenses]. *Derzhava ta rehiony. Seriia: Ppavo*. № 4 (58). URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf [in Ukrainian].

Kovalchuk, S. O. (2018). *Vchennia pro rechovi dokazy* u *kryminalnomu protsesi: teoretyko-pravovi*

ta praktychni osnovy [The doctrine of material evidences in the criminal process: theoretical, legal and practical basis.] : dys. … d-ra yuryd. nauk. Odesa. URL: https://dspace.onua.edu.ua/bitstreams/94e3af63-a41b-4f31-8a68-07c2b8bc430b/download [in Ukrainian].

Kovalenko, A. V. (2023). Orhanizatsiia i taktyka provedennia ohliadu komp'iuternykh danykh [Organization and tactics of computer data inspection]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia: yurydychni nauky*. Vyp. 4. DOI: 10.32999/ksu2307-8049/2023-4-9 [in Ukrainian].

Krytska, I. O. (2018). Rechovi dokazy u kryminalnomu provadzhenni [Physical evidence in criminal proceedings] : monohrafiia. Kharkiv [in Ukrainian].

Lisnichenko, D. V. (2022). Osoblyvosti vyluchennia za dopomohoiu tekhnichnykh zasobiv informatsii z mobilnykh terminaliv zv'iazku (smartfoniv) pid chas kryminalnoho provadzhennia [Features of extraction by technical means of information from mobile communication terminals (smartphones) during criminal proceedings]. *Pivdennoukrainskyi pravnychyi chasopys*. Vyp. 1—2. DOI: 10.32850/sulj.2022.1-2.22 [in Ukrainian].

Metelev, O. P. (2023). Tsyfrovi dokazy u kryminalnomu protsesi: vydova kharakterystyka [Digital evidence in criminal procedure: typological characteristic]. *Visnyk kryminalnoho sudochynstva*. № 1—2. DOI: 10.17721/2413-5372.2023.1-2/42-53 [in Ukrainian].

Ostapchuk, L. H., Smal, I. A. (2022). Do pytannia pravovoi pryrody elektronnoho dokumentu ta yoho mistsia u systemi dokaziv kryminalnoho protsesu [On the issue of legal nature of an electronic document and its place in the system of the criminal processevidence]. *Prykarpatskyi yurydychnyi visnyk*. Vyp. 2 (43). DOI: 10.32837/pyuv.v0i2.1028 [in Ukrainian].

Shcherbakovskyi, M. (2024). Open Sources of Cyberspace as Objects of Forensic Research. *Theory and Practice of Forensic Science and Criminalistics.* Is. 2 (35). DOI: 10.32353/khrife.2.2024.02.

Shcherbakovskyi, M. H., Pashniev, D. V. (2010). *Rozsliduvannia komp'iuternykh zlochyniv* [Investigation of computer crimes] : navch. posib. Kharkiv. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/2b0c8656-bc78-4c21-8ff0-3808403f00ca/content [in Ukrainian].

Skrypnyk, A. V. (2021). *Vykorystannia informatsii* z *elektronnykh nosiiv* u *kryminalnomu protsesualnomu dokazuvanni* [Use of information from electronic media in criminal procedural evidence] : dys. … d-ra filos. u haluzi prava. Kharkiv [in Ukrainian].

Щербаковський, М., Сезонов, В. (2024). Збирання та дослідження електронних документів із застосуванням спеціальних знань. *Теорія та практика судової експертизи і криміналістики*. Вип. 3 (36). С. 10—23. DOI: 10.32353/khrife.3.2024.02.