Пошук та фіксування цифрової інформації під час кримінального провадження

Михайло Щербаковський
доктор юридичних наук, професор, завідувач кафедри кримінального процесу, криміналістики та експертології, навчально-науковий інститут № 5, Харківський національний університет внутрішніх справ МВС України, м. Харків, Україна,
ORCID: https://orcid.org/0000-0003-1990-1231,
e-mail: shcherbakovskyi@gmail.com

Сформульовано поняття електронних документів у широкому та вузькому сенсі. Проаналізовано зв'язок між речовими та цифровими носіями інформації. Докладно описано формування джерел доказів залежно від носіїв цифрової інформації. Виокремлено процесуальні джерела доказів, у яких відображено цифрову інформацію або комп'ютерні дані.
Ключові слова: *цифрова інформація; носії цифрової інформації; цифрові докази; джерела доказів; протоколи слідчих дій; висновок експерта.*

The Search and Seizure of Digital Information in Criminal Proceedings

Mykhailo Shcherbakovskyi

This paper defines electronic documents in both broad and narrow senses. It analyzes the relationship between physical and digital information carriers. The formation of sources of evidence depending on the carriers of digital information is described in detail. The procedural sources of evidence that reflect digital information or computer data are highlighted.
Keywords: *digital information; digital information carriers; digital evidence; sources of evidence; investigative protocols; forensic report.*

У правоохоронній сфері усвідомлено факт необхідності новацій у кримінальній процесуальній сфері, у способах та інструментальних методах здійснення пошуку, огляду, фіксування та дослідження криміналістично значущої цифрової інформації. Водночас у кримінальному процесі залишається низка проблем, пов'язаних із трактуванням понять цифрової інформації, електронних документів, комп'ютерних даних, цифрових доказів та їх джерел, що негативно впливає на слідчо-судову практику.

З технічної позиції цифрова інформація є двійковим кодом, записаним за допомогою нулів та одиниць, призначеним для зчитування, оброблення та передавання за допомогою інформаційних технологій.

У первозданному вигляді вона не придатна для людського сприйняття, це відбувається за домогою застосування комп'ютерних засобів.

У нормативних актах надаються близькі визначення електронної (цифрової) інформації, електронних документів, комп'ютерних даних як відомостей, фактів в електронній, цифровій формі, придатних для оброблення в комп'ютерній системі [1—4]. Важливою характеристикою електронної інформації є спосіб її зберігання у форматі файлів, нефайлової структури, файлового контейнера тощо.

У кримінально-процесуальному аспекті поняття «електронна (цифрова) інформація», «комп'ютерні дані», «електронний документ» можна вживати як синоніми. Проте з практичної та процесуальної позицій доцільно виокремити поняття електронних документів у широкому та вузькому значенні. У широкому значенні електронним документом слід вважати будь-яку інформацію, представлену в електронній формі, формування та існування якої здійснюється за допомогою спеціальних програмно-технічних засобів. У вузькому значенні електронний документ — це документ, що має реквізити: обов'язкові дані, наприклад, електронний підпис або електронну печатку.

Поняття комп'ютерних даних невід'ємне від його носія, на якому можуть бути записані цифрові дані [5]. Зважаючи на природу комп'ютерних даних, для доказування доцільно об'єднати їх у дві групи: речові та цифрові. Під час розслідування речові носії важливі як об'єкти, у яких безпосередньо містяться криміналістично значущі для доказування комп'ютерні дані у формі файлів. Речовими носіями є будь-які пристрої, придатні для зберігання комп'ютерних даних. Цифрові носії — локальні або глобальні мережі (зокрема, інтернет), не пов'язані з певним речовим носієм. Запропонований розподіл носіїв цифрової інформації співвідносний із рішеннями Верховного Суду, згідно з якими головною особливістю електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія.

Отже, цифрова інформація має отримуватися з певного речового або цифрового носія у формі відповідного файлу.

Цифрова інформація перетворюється на цифрові (електронні) докази, якщо містить фактичні дані про обставини кримінального правопорушення. Однак цифрова інформація набуває статусу доказу лише тоді, коли буде знайдена, а її зміст, властивості й інші характеристики зафіксовані в процесуальних джерелах у формі, доступній для однозначного сприйняття всіма учасниками кримінального провадження. Законодавством передбачено спеціальні процесуальні дії формування джерел доказів, змістом яких є цифрова інформація, з урахуванням особливостей її носіїв та методів роботи з ними: тимчасовий доступ до електронних інформаційних систем, комп'ютерних систем

або їхніх частин, мобільних терміналів систем зв'язку (ст. 160 Кримінального процесуального кодексу України (далі — *КПК*), обшук (ст. 236 КПК), огляд (ст. 237 КПК), зняття інформації з електронних комунікаційних мереж (ст. 262 КПК) або електронних інформаційних систем (ст. 364 КПК) [6] та ін.

Формування джерел доказів залежить від носіїв цифрової інформації, складності її виявлення, необхідності залучення спеціалістів або експертів та інших обставин, що сукупно характеризують слідчі ситуації.

Якщо речовий носій інформації вимкнений, вилучений як речовий доказ, тимчасово вилучено майно або він є додатком до протоколу слідчих (розшукових) дій, проводять: а) включення носія та огляд його вмісту з описом інформації (комп'ютерних даних) у протоколі; відображення в додатках до протоколу у вигляді фото, відеозапису, роздруківки; б) за наявності системи логічного захисту, складності в пошуку необхідної інформації призначають експертизу, де у висновку експерта описується зміст і характеристики встановлених даних. У випадку, коли носій неможливо вилучити, здійснюють: а) огляд даних, їх опис у протоколі; б) копіювання інформації на зовнішній носій із наступним оглядом або призначенням експертизи; в) за неможливості вимкнення носія або копіювання даних експертизу проводять на місці його розташування. Під час кримінального провадження цифрова інформація (комп'ютерні дані) у такому разі набуває доказового значення разом із конкретним речовим носієм, вилученим у встановленому місці, у конкретної особи за певних обставин.

Для електронного носія інформації проводять: а) огляд комп'ютерних даних та їх опис у протоколі з додатками; б) копіювання даних із наступним оглядом або призначенням експертизи; в) призначення експертизи для пошуку, виявлення та дослідження комп'ютерних даних. У даній ситуації для процесу розслідування мають значення тільки дані, а не їх носій.

У простих ситуаціях, коли речовий носій перебуває у вимкненому стані і його слід вилучити, коли носій незаблокований, точно відомо найменування документа (файлу, вебсторінки тощо) і немає потреби в його пошуку, слідчий може здійснити всі операції самостійно. У складних слідчих ситуаціях, пов'язаних із копіюванням цифрової інформації, її пошуком і виявленням у комп'ютерних мережах, хмарних середовищах, на носіях, які неможливо вимкнути або зупинити функціювання, обов'язковим учасником є спеціаліст із інформаційних технологій. У такому разі маніпуляції спеціаліста із застосуванням технічних і програмних засобів здебільшого недоступні та незрозумілі учасникам слідчої дії. Для забезпечення допустимості цифрової інформації як доказу можна рекомендувати, по-перше, усі дії спеціаліста фіксувати за допомогою відеозапису, робити роздруківки документів, скриншоти вебсторінок тощо; по-друге, призначити комп'ютерно-технічну

експертизу щодо речових носіїв або експертизу електронних комунікацій для пошуку конкретної інформації в цифровому носії.

Отже, відповідно до ст. 84 КПК [6] процесуальними джерелами доказів, у яких відображається цифрова інформація або комп'ютерні дані, є документи, до яких належать протоколи слідчих (розшукових) дій із додатками та копії комп'ютерних даних, а також висновки експертів.

Перелік джерел посилання

1. Конвенція про кіберзлочинність : ратиф. із застереж. і заявами Законом України від 07.09.2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 02.09.2024).
2. 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/card/2811-20 (дата звернення: 02.09.2024).
3. 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: 02.09.2024).
4. 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: 02.09.2024).
5. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT) від 06.12.2017 р. [Чинний від 01.01.2019]. Київ, 2018. URL: https://online.bud-standart.com/ua/catalog/doc-page.html?id_doc=74978 (дата звернення: 02.09.2024).
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: 05.09.2024).