УДК 343.14(477):004 DOI: https://doi.org/10.32631/pb.2024.2.13

ВІТАЛІЙ ВОЛОДИМИРОВИЧ РОМАНЮК,
кандидат юридичних наук, доцент,
Харківський національний університет внутрішніх справ,
факультет № 1;
https://orcid.org/0000-0001-6077-4591,
e-mail: romaniukukraine@gmail.com;

СЕРГІЙ ЄВГЕНОВИЧ АБЛАМСЬКИЙ,
кандидат юридичних наук, доцент,
Харківський національний університет внутрішніх справ,
кафедра кримінального процесу та організації досудового слідства;
https://orcid.org/0000-0003-4716-3985,
e-mail: ablamu4@gmail.com

КРИТЕРІЇ ДОПУСТИМОСТІ ЦИФРОВИХ (ЕЛЕКТРОННИХ) ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ

Статтю присвячено розгляду сучасних проблем визначення допустимості цифрових (електронних) доказів у кримінальному процесі. Зважаючи на важливість окресленої проблематики, основною метою дослідження визначено надання характеристики кожній складовій допустимості таких доказів, а саме: належне джерело отримання, належний суб'єкт і належний спосіб збирання. Наголошено, що найбільшою доктринальною проблемою, яка створює перепону у визначенні таких критеріїв, є відсутність єдиного наукового бачення щодо поняття цифрових (електронних) доказів та визначення їх джерела. Констатовано наявність трьох наукових підходів до вирішення цієї проблеми, з урахуванням чого висловлено авторську позицію щодо можливих шляхів її вирішення. Розкрито окремі практичні аспекти, пов'язані з проблемами дотримання критеріїв допустимості цифрових (електронних) доказів під час розслідування кримінальних правопорушень.

На основі системного аналізу наукового доробку та судової практики визначено, що складність вирішення проблемних аспектів допустимості цифрових (електронних) доказів пов'язана з їхньою складною технічною природою. Це зумовлено тим, що цифрові (електронні) докази містять абстрактні технічні та математичні моделі, характеризуються специфічними умовами виникнення, існування, копіювання та зберігання, що суттєво відрізняє їх від інших видів доказової інформації.

Доведено, що під час визначення цифрових (електронних) доказів слід відобразити таку обов'язкову їхню ознаку, як релевантність щодо певного кримінального провадження. Означене пояснено тим, що у кримінальному процесі цифровим (електронним) доказом може бути лише та інформація, яка має безпосереднє значення для певного кримінального провадження. Іншою обов'язковою складовою дефініції «цифровий (електронний) доказ» має бути вказівка на його специфічну природу. При цьому недоцільним визнано підхід, коли у визначеннях паралельно вказують на електронний характер такої інформації та її концентрацію на певному електронному носієві. Інформація, яка міститься на певному електронному носієві, є електронною, а не якоюсь іншою. Інакше це призводить до дублювання та є логічною помилкою. Запропоновано джерелом цифрових (електронних) доказів вважати цифровий (електронний) об'єкт, за допомогою якого ця доказова інформація була створена, зафіксована або передана.

До недоліків чинного кримінального процесуального законодавства України віднесено відсутність офіційного визначення цифрових (електронних) доказів та їхніх джерел, на відміну від цивільного процесуального та адміністративного процесуального законодавства. Проте запропоновані законодавцем визначення містять недоліки. Зокрема, у закріплених дефініціях цифрових (електронних) доказів міститься невиправдане протиставлення суміжних понять «інформація», «дані» та «відомості».

Ключові слова: *кримінальне провадження, цифрові (електронні) докази, допустимість доказів, критерії допустимості доказів, електронний документ, слідчий, дізнавач, прокурор.*

© Романюк В. В., Абламський С. Є., 2024

Оригінальна стаття

ВСТУП. На доктринальному рівні сформована цілком виправдана теза, що доказування посідає центральне місце у кримінальній процесуальній діяльності, є його ядром. Недарма з гносеологічної точки зору розслідування кримінальних правопорушень розглядається як процес пізнання кримінальної події, який має ретроспективний характер (тобто спрямований на пізнання події, що мала місце в минулому) та здійснюється у формі доказування. Це означає, що будь-яка обставина кримінального правопорушення вважається встановленою тоді, коли її існування підтверджується належними, допустимими, достовірними та достатніми доказами. Тим часом стрімкий розвиток науки й техніки, впровадження їх досягнень у повсякденне життя є фактором виникнення кримінальних правопорушень нового типу, які вчиняються із застосуванням передових засобів і способів.

На сучасному етапі розвитку суспільства вчинення кримінальних правопорушень супроводжується застосуванням цифрових (електронних) засобів, внаслідок чого, з одного боку, їх використовують злочинці, а з іншого – слідчі для збирання доказів, які також мають цифрову (електронну) форму. Однією з обов'язкових характеристик доказової інформації у кримінальному провадження є її допустимість, через що (у разі відповідності іншим вимогам) вона набуває власне значення доказу. У зв'язку із цим на практиці правильне розуміння допустимості цифрових (електронних) доказів, складових цього поняття та їхнього впливу на процедуру збирання доказів є дуже важливим.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. Зважаючи на тематику статті, *метою* наукового пошуку є: по-перше, сформулювати особливості визначення допустимості цифрових (електронних) доказів у кримінальному провадженні; по-друге, окреслити наявні практичні проблеми в цьому напрямі.

Мета дослідження досягалась через поступове виконання таких *завдань*:

1) дослідження наукових джерел щодо поняття цифрових (електронних) доказів у кримінальному процесі;

2) визначення джерел цифрових (електронних) доказів;

3) з'ясування місця цифрових (електронних) доказів серед інших видів доказів та їх допустимості у кримінальному провадженні;

4) аналіз судової практики на предмет виявлення проблем, пов'язаних із допустимістю цифрових (електронних) доказів;

5) формулювання авторської позиції та висновків щодо порушених у дослідженні питань.

ОГЛЯД ЛІТЕРАТУРИ. Проблемам доказування у кримінальному процесі присвячено чимало наукових праць, оскільки індикатором прийняття законних і неупереджених процесуальних рішень є допустимість доказів, які беруться за основу їх обґрунтування.

Серед наукового доробку, присвяченого проблематиці допустимості доказів у кримінальному процесі, слід згадати останні дослідження таких учених: В. М. Зінченко (2020) «Достатність доказів у кримінальному провадженні», Г. Р. Крет (2020) «Міжнародні стандарти доказування у кримінальному процесі України: теоретико-правові та практичні основи», Б. В. Шабаровський (2019) «Перевірка доказів у кримінальному процесі України», Х. Р. Слюсарчук (2017) «Стандарти доказування у кримінальному провадженні», А. С. Степаненко (2017) «Стандарт доказування "поза розумним сумнівом" у кримінальному провадженні», О. В. Литвин (2016) «Кримінально-процесуальне доказування у стадії судового розгляду», І. Л. Чупрікова (2016) «Допустимість доказів у світлі нового Кримінального процесуального кодексу».

Ознайомлення зі згаданими дослідженнями, а також іншими працями дозволяє констатувати доволі високий рівень розробленості теорії доказування у кримінальному процесі. Попри це залишаються невирішеними проблеми, що стосуються збирання та дослідження цифрових (електронних) доказів у кримінальному провадженні. Насамперед це пов'язано з наявною в науці кримінального процесу дискусією щодо поняття цього різновиду доказів та його місця в чинній класифікаційній моделі доказів. І як слушно зазначають окремі науковці, складність вирішення цієї проблеми пов'язана з тим, що цифрові (електронні) докази мають складну технічну природу. Зокрема, цифрові (електронні) докази містять абстрактні технічні й математичні моделі, характеризуються специфічними умовами виникнення, існування, копіювання та зберігання (Метелев, 2019, с. 225). Із такою тезою слід погодитися і додати, що з розвитком інформаційно-телекомунікаційних технологій значно ускладнюється процес збирання та фіксації таких доказів, а це вимагає від слідчого, прокурора постійно підвищувати власні знання, вміння та навички не лише щодо збирання таких доказів, а й розуміння того, що вони в подальшому не будуть визнанні судом недопустимими.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. Для виконання завдань дослідження використовувались як загальнонаукові, так і спеціальнонаукові методи. Історико-правовий метод дозволив проаналізувати становлення та розвиток кримінального процесуального законодавства України в царині регулювання допустимості доказів. За допомогою порівняльноправового методу охарактеризовано норми щодо допустимості доказів та їхніх критеріїв за чинним Кримінальним процесуальним кодексом України. Для вивчення судової практики застосовано статистичний метод, за допомогою якого визначено особливості та закономірності в частині допустимості доказів у кримінальному провадженні.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ ТА ДИСКУСІЯ. Злочинність є одним із соціальнонегативних явищ, через що питання протидії їй постійно перебувають на порядку денному не лише серед науковців і практичних працівників правоохоронних органів, а й населення (Абламський, Конюшенко, 2023, с. 123). Оновлені норми Кримінального процесуального кодексу України (далі – КПК України) стали передумовою для вдосконалення концепції захисту прав і основоположних свобод людини під час досудового розслідування та судового розгляду. Ці зміни стосуються особливостей оцінки судом доказів на предмет їх допустимості, встановлення підстав та порядку визнання доказів недопустимими, визначення переліку діянь, які визнаються істотними порушеннями прав людини і основоположних свобод під час здійснення процесуальних дій щодо отримання доказів (Ablamskyi et al., 2021, p. 48). Нині до недоліків чинного кримінального процесуального законодавства слід віднести відсутність офіційного визначення цифрових (електронних) доказів. При цьому склалась така ситуація, коли законодавчі акти, що регулюють діяльність в інших сферах судочинства, таке визначення містять. Так, у ч. 1 ст. 99 Кодексу адміністративного судочинства України[1], ч. 1 ст. 96 Господарського процесуального кодексу України[2] та ч. 1 ст. 100 Цивільного процесуального кодексу України[3] надається визначення терміна «електронні докази». Це інформація в електронній (цифровій) формі, що містить дані про обставини, які мають значення для справи, зокрема: електронні документи (текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Незрозумілим є відсутність аналогічного визначення в нормах чинного КПК України. Хоча спроби законодавця в цьому напрямі відомі. Зокрема, у 2020 році було розроблено Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів, у ч. 1 ст. 100 якого у кримінальний процес передбачалось запровадження визначення поняття «електронний доказ», під яким розумілась «інформація в електронній (цифровій) формі з відомостями, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження»[4].

Проте ці визначення містять недоліки. Слід погодитись з абсолютно слушним зауваженням, яке існує в науці, про те, що в наведених дефініціях електронних доказів міститься невиправдане протиставлення суміжних понять «інформація», «дані» та «відомості» (Фігурський, 2023, с. 99), які у загальнонауковому розумінні розглядають як синоніми. Доказ будь-якого виду традиційно й абсолютно правильно за своєю природою визначається як інформація, що має значення для розслідування кримінального правопорушення. Тому доповнення визначення цього поняття словами «дані» чи «відомості» призводить до логічних помилок. Інформація не може містити дані, адже вона сама по собі і є даними (Фігурський, 2023, с. 99).

---

[1] Кодекс адміністративного судочинства України : Закон України від 06.07.2005 № 2747-IV // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2747-15 (дата звернення: 26.03.2024).

[2] Господарський процесуальний кодекс України : Закон України від 06.11.1991 № 1798-XII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1798-12 (дата звернення: 26.03.2024).

[3] Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1618-15 (дата звернення: 26.03.2024).

[4] Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : від 01.09.2020 № 4004 / ініціатори С. А. Мінько, О. С. Бакумов, Г. О. Михайлюк та ін. // БД «Законодавство України» / ВР України. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771 (дата звернення: 26.03.2024).

Існують і дещо інші погляди на поняття цифрових (електронних) доказів у кримінальному провадженні. Зокрема, Д. М. Цехан (2013, с. 257) під цифровим доказом розуміє фактичні дані в дискретній (цифровій) формі, що містяться на певному матеріальному носії та після оброблення стають доступними для сприйняття. І. Г. Каланча та А. В. Столітній (2019, с. 182) стверджують, що електронні доказі – це збережена в електронній формі інформація, яка міститься на будь-якому матеріально-електронному носії, електронних пристроях чи інформаційних системах. В. В. Мурадов (2013, с. 314) електронні докази визначає як сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах.

Отже, можна побачити, що науковці виокремлюють такі ознаки цифрових (електронних) доказів: 1) це інформація в цифровій (електронній) формі; 2) вона міститься на специфічному електронному носієві. Вбачається, що у визначенні цифрового (електронного) доказу слід відобразити таку обов'язкову його ознаку, як релевантність щодо певного кримінального провадження. Інакше кажучи, у кримінальному процесі цифровим (електронним) доказом може бути лише та інформація, яка має значення для певного кримінального провадження. Тому саме вказівкою на цю ознаку слід доповнити згадані визначення. Крім того, обов'язковою складовою визначення поняття «цифровий (електронний) доказ» має бути вказівка на його специфічну природу. Аналіз наявних визначень показує, що дослідники також поділяють зазначену думку. Можна побачити, що ця ознака описується науковцями через словосполучення «фактичні дані у дискретній (цифровій) формі», «збережена в електронній формі інформація». На нашу думку, такої вказівки цілком достатньо, щоб задовольнити потреби у правовому розумінні цифрових доказів. Хоча зустрічаються й більш складні визначення, що більше розкривають технічну сторону цього поняття. Наприклад, В. М. Фігурський (2023, с. 99) визначає їх як інформацію, створену, оброблену, збережену або передану за допомогою аналогових чи цифрових сигналів, що має значення для кримінального провадження. І таке визначення цілком має право на існування.

Водночас недоцільним слід визнати паралельну вказівку на електронний характер такої інформації та її концентрацію на певному електронному носієві. Адже зрозуміло, що інформація, яка міститься на певному електронному носієві, є електронною, а не якоюсь іншою. В іншому разі це призводить до дублювання та є логічною помилкою.

Безумовно, ця дискусія має важливе фундаментальне значення для визначення сутності та місця цифрових (електронних) доказів у кримінальному процесі, а їх віднесення до категорії документів з огляду на їхню природу має суперечливий характер.

Проте згадане обговорення має більше доктринальне, аніж практичне значення. Для практики більш важливим є чітке розуміння критеріїв, за якими цифрова (електронна) інформація може набувати значення доказу у кримінальному провадженні. З огляду на це розглянемо вимоги, які висуваються та відображені в чинному КПК України щодо допустимості цифрових (електронних) доказів у кримінальному провадженні. У вітчизняній кримінальній процесуальній доктрині виокремлюють такі критерії допустимості доказів: 1) належне джерело отримання доказів; 2) належний суб'єкт; 3) належний спосіб збирання доказів (Гутник, Хитра, 2022, с. 75–89).

Належне джерело отримання доказів

Кримінальний процесуальний кодекс України визначає, що процесуальними джерелами доказів є показання, речові докази, документи та висновки експертів (ч. 2 ст. 84). У літературі сьогодні сформувалось три основні підходи до вирішення цієї проблеми.

Перший підхід заснований на законодавчому визначенні класифікації джерел доказів у кримінальному процесі, в якій цифрові (електронні) докази посідають місце різновиду документа. Зокрема, згідно з п. 1 ч. 2 ст. 99 КПК України до документів належать: «матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані)». Водночас у ч. 4 згаданої статті вказується, що «дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа», що також підтверджує належність цього виду інформації до електронних доказів.

Представники другого підходу не відносять цифрові (електронні) докази до жодного з процесуальних джерел доказів на підставі того, що вони є лише способом відображення доказів, а джерело доказів може бути продемонстроване у цифровому форматі (Каланча,

Столітній, 2019, с. 186–188). Інші вчені цифрові матеріали розглядаються як різновид речових доказів (Білоусов, 2008, с. 14) або ж одночасно як різновид речових доказів і документів в електронній формі (Козицька, 2020, с. 420).

Третя група науковців є прибічниками позиції, що існують окремі цифрові (електронні) джерела доказів. На думку дослідників, такі джерела суттєво відрізняються від документів. Лист, графік або малюнок можна безпосередньо продемонструвати на видимому носії, тоді як докази в електронній формі створюються, зберігаються та передаються шляхом перетворення інформації в цифровий код, а також демонструються та зчитуються за допомогою спеціальних пристроїв і програмного забезпечення. Отже, спосіб зберігання та відображення інформації між ними є докорінно різним. Відмінність, на думку вчених, можна побачити також між цифровими (електронними) доказами та аудіовізуальними матеріалами. Ця відмінність полягає в тому, що аудіовізуальні матеріали відтворюються за допомогою відео- чи аудіопристрою, а інформація сприймається зором, або слухом, або ж обома способами одночасно. Докази ж в електронній формі можуть демонструватись за допомогою кількох носіїв, які не зберігаються так само як аудіовізуальні матеріали. При цьому аудіовізуальні матеріали не можуть включати докази в електронній формі, натомість електронні докази можуть охоплювати аудіовізуальні дані. Тож дослідниками пропонується виокремити процесуальне джерело цифрових (електронних) доказів на рівні з показаннями, речовими доказами, документами та висновками експертів (Цехан, 2013, с. 259; Метелев, 2018, с. 83; Коваленко, 2018, с. 242). У цьому контексті постає питання: що в такому разі може бути джерелом цифрових (електронних) доказів? На наше переконання, ним слід вважати цифровий (електронний) об'єкт, за допомогою якого ця доказова інформація була створена, зафіксована або передана.

Однак сьогодні практика боротьби зі злочинністю повинна керуватись положеннями чинного кримінального процесуального законодавства України, а отже, виходити з формального їх розуміння як різновиду документів, зокрема як електронного документа.

Стаття 99 КПК України закріплює офіційне поняття «документ» як джерело доказу, а саме визначає його як спеціально створений для збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо певні відомості, що можуть бути використані як доказ фактів чи обставин, які встановлюються під час кримінального провадження.

Крім цього, згадана стаття містить конкретизований перелік документів, які можуть бути доказами у кримінальному процесі: матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (зокрема, електронні), на яких за допомогою технічних засобів зафіксовано процесуальні дії.

Деякі науковці стверджують, що, враховуючи законодавче закріплення лише чотирьох джерел доказів, джерелом цифрових (електронних) доказів є документ або речовий доказ (річ). Згадані дослідники вважають, що для того, щоб відрізнити електронний документ від речового доказу в електронній формі, слід звернути увагу на те, що саме може бути використане як доказ факту чи обставин, що встановлюються під час кримінального провадження: інформація чи матеріальний об'єкт (Гутник, Хитра, 2022, с. 83). Вказана теза є спірною, адже доказом не може бути матеріальний об'єкт, доказом завжди виступає інформація, яку містить певний матеріальний об'єкт як її носій.

Точне визначення джерела цифрового (електронного) доказу є запорукою застосування правильного засобу та процедури фіксації й вилучення доказової інформації, її збереження відповідно до визначених КПК України правил. Крім того, при роботі із джерелами цифрових (електронних) доказів, при пошуку таких доказів, їх фіксації та вилученні обов'язково слід залучати відповідних спеціалістів, що гарантуватиме належність виконання зазначених завдань.

Належний суб'єкт збирання цифрових (електронних) доказів

Вимога про те, що цифровий (електронний) доказ має бути отриманий належним суб'єктом, означає одержання його таким учасником кримінального провадження, який є правомочним здійснювати це провадження або ж окрему процесуальну дію. Так, належним суб'єктом, уповноваженим на проведення досудового розслідування, є слідчий або дізнавач, визначений керівником органу досудового розслідування для здійснення конкретного кримінального провадження (ч. 1 ст. 214 КПК України). Не слід також забувати, що в разі, якщо слідчому із заяви, повідомлення чи інших джерел стало відомо про обставини, які можуть свідчити про вчинення кримінального правопорушення, розслідування якого не віднесено до його компетенції (підслідності), він проводить розслідування доти, доки прокурор не визначить іншу підслідність (ч. 2 ст. 218 КПК України). У такому разі слідчий або дізнавач є

належними в цьому кримінальному провадженні до моменту визначення підслідності прокурором.

Ця особливість є актуальною при розслідуванні кримінальних правопорушень, що вчиняються за допомогою мережі Інтернет. Як свідчить практика, у більшості випадків місця вчинення таких кримінальних правопорушень визначаються за місцем реєстрації або проживання потерпілих, через що й визначається територіальна підслідність. Однак у подальшому, після встановлення місця перебування (проживання) підозрюваної особи, виникає необхідність зміни територіальної підслідності та передачі матеріалів кримінального провадження в порядку ст. 218 КПК України. Наприклад, після проведення низки процесуальних дій за IP-адресою було встановлено пристрій, з якого злочинець вчинив шахрайські дії. Відповідно місцезнаходження цього пристрою і буде місцем вчинення кримінального правопорушення.

При цьому слід пам'ятати, що при вирішенні питання щодо підслідності в кожному випадку надходження зазначеної інформації слідчий в порядку ст. 218 КПК України протягом п'яти днів з дня її отримання письмово повідомляє прокурора та продовжує здійснювати досудове розслідування доти, доки прокурор не визначить іншу підслідність.

Уповноваженим на здійснення окремих процесуальних дій слід також вважати слідчого (дізнавача):

– якому постановою слідчого іншого органу досудового розслідування іншої територіальної юрисдикції чи прокурора доручено проведення слідчих (розшукових) і негласних слідчих (розшукових) дій (ч. 6 ст. 218 КПК України);

– який входить до складу слідчої групи (п. 1 ч. 2, ч. 4 ст. 39 КПК України) або спільної слідчої групи (ст. 571 КПК України);

– який на час провадження конкретних слідчих (розшукових) чи інших процесуальних дій, у результаті яких були отримані докази, перебував на посаді слідчого й виконував свої трудові обов'язки (зокрема, не перебував на лікуванні, у відпустці тощо) (Вапнярчук, 2017, с. 246–247).

Крім того, до цього переліку можна додати ситуації, коли процесуальні дії здійснює прокурор (процесуальний керівник у кримінальному провадженні) відповідно до п. 4 ч. 2 ст. 36 КПК України та коли такі дії здійснює оперативний працівник за дорученням слідчого (дізнавача) або прокурора відповідно до частин 2 і 3 ст. 41 КПК України.

Проте на практиці виникають проблеми. Наприклад, згідно зі ст. 160 КПК України сторони кримінального провадження мають право звернутися до слідчого судді під час досудового розслідування чи суду під час судового провадження із клопотанням про тимчасовий доступ до речей і документів.

Отже, законодавець визначив вичерпний перелік осіб, які мають право звертатися з відповідним клопотанням, і недотримання вказаної вимоги закону є підставою для відмови в задоволенні клопотання. При цьому подавати відповідне клопотання повинен саме той слідчий, який здійснює досудове розслідування у кримінальному провадженні, в межах якого таке клопотання подається. У разі ж заміни слідчого у кримінальному провадженні разом із клопотанням слід подавати докази про це, чим може слугувати постанова про призначення нового слідчого. У разі ж якщо досудове розслідування здійснюється групою слідчих (слідчою групою), а клопотання, відповідно, підписується одним із них, то слід додавати постанову про призначення групи слідчих у цьому кримінальному провадженні. Це ж правило стосується і прокурора, який погоджує відповідне клопотання або подає його самостійно. Іншим прикладом є факт звернення з відповідним клопотанням не слідчим, а оперуповноваженим, який не є учасником кримінального провадження, а тому йому не може бути наданий тимчасовий доступ до речей і документів. Порушення цієї вимоги може призвести до відмови слідчого судді в задоволенні клопотання[1].

Належний спосіб збирання цифрових (електронних) доказів

Зазвичай вважають, що процес доказування є триступеневим та полягає в збиранні, перевірці й оцінці доказів. Збирання доказів, тобто їх отримання, має проводитися відповідно до спеціально встановленої процедури. Її дотримання гарантує їх допустимість, що означає можливість їх використання в межах кримінального провадження. Аналіз положень ст. 93 КПК України дозволяє виокремити такі законні способи збирання доказів стороною обвинувачення:

– надання доказів добровільно учасником кримінального провадження (отримання);

– витребування доказів;

[1] Тютюн Т. М. Узагальнення проблемних питань, які виникають при розгляді клопотань про тимчасовий доступ до речей і документів // Київський апеляційний суд : офіц. сайт. URL: https://www.kas.gov.ua/wp-content/uploads/2015/07/12014-kr.pdf (дата звернення: 26.03.2024).

– проведення тимчасового доступу до електронного документа (як заходу забезпечення);

– проведення слідчих (розшукових) дій (огляд, обшук);

– проведення негласних слідчих (розшукових) дій.

Після отримання електронного документа на носії інформації слідчий, дізнавач зобов'язані оглянути його.

Зі свого боку сторона захисту, потерпілий та його представник можуть збирати електронні документи шляхом: 1) отримання чи витребування їх від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб; 2) ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій стороною обвинувачення. Якщо говорити про право сторони захисту, потерпілого на ініціювання проведення процесуальних дій, то тут учасники виступають лише ініціаторами, а суб'єктами збирання в разі задоволення клопотання буде слідчий, дізнавач або прокурор (Чупрікова, 2016, с. 63).

Розглянемо окремі особливості збирання цифрових (електронних) доказів у кримінальному провадженні з огляду на судову практику. При розслідуванні кримінальних правопорушень, сліди вчинення яких мають цифровий (електронний) характер, типовим є застосування таких процесуальних засобів, як витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб речей, документів і тимчасового доступу до речей і документів. Кримінальний процесуальний кодекс України містить певний порядок послідовності реалізації цих процесуальних дій, порушення якого призводить до недопустимості зібраних доказів.

Так, при зверненні до суду з клопотанням про тимчасовий доступ до речей та документів слідчими іноді не виконуються вимоги ч. 2 ст. 93 КПК України. Зокрема, в деяких випадках слідчі, попри надані їм повноваження, безпосередньо не звертаються до фізичних та юридичних осіб з метою отримання вказаних у їхніх клопотаннях документів, а у судовому засіданні не доводять, що речі або документи, до яких просять надати доступ, перебувають або можуть перебувати у володінні відповідно фізичної чи юридичної особи[1].

Аналіз судової практики з розгляду клопотань зазначеної категорії також свідчить про те, що слідчі судді виносять ухвали про відмову в задоволенні клопотань про надання тимчасового доступу до речей і документів через недоведеність обґрунтування значення конкретних речей і документів для встановлення обставин у кримінальному провадженні, а також з підстав недоведеності органом досудового розслідування того, що лише шляхом вилучення оригіналів документів можливе з'ясування тих чи інших обставин, на які орган досудового розслідування посилається в клопотанні[2].

Відповідно до ст. 162 КПК України до охоронюваної законом таємниці, яка міститься в речах і документах, серед іншого належать відомості, що можуть становити банківську таємницю, особисте листування особи та інші записи особистого характеру, а також інформація, яку мають оператори та провайдери телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, зокрема отримання послуг, їх тривалості, змісту, маршрутів передавання тощо. Вказані дані зазвичай становлять інтерес для слідства при розслідуванні справ про шахрайство, вчинене з використанням інформаційно-комунікаційних технологій, адже за допомогою розкриття цих даних здійснюється ідентифікація особи злочинця.

Як свідчить судова практика, при поданні клопотань про тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю (банківська, інформація про зв'язок абонента тощо), слідчими не завжди належним чином обґрунтовується неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів (ч. 6 ст.163 КПК України)[3].

---

[1] Єфімова О. І., Коваль С. М. Узагальнення судової практики розгляду слідчими суддями клопотань сторін кримінального провадження про тимчасовий доступ до речей та документів відповідно до статей 159–166 КПК України // Київський апеляційний суд : офіц. сайт. URL: https://www.kas.gov.ua/wp-content/uploads/2015/07/Uzag4.doc (дата звернення: 26.03.2024).

[2] Єфімова О. І., Коваль С. М. Узагальнення судової практики розгляду слідчими суддями клопотань сторін кримінального провадження про тимчасовий доступ до речей та документів відповідно до статей 159–166 КПК України // Київський апеляційний суд : офіц. сайт. URL: https://www.kas.gov.ua/wp-content/uploads/2015/07/Uzag4.doc (дата звернення: 26.03.2024).

[3] Тютюн Т. М. Узагальнення проблемних питань, які виникають при розгляді клопотань про тимчасовий доступ до речей і документів // Київський апеляційний суд : офіц. сайт. URL: https://www.kas.gov.ua/wp-content/uploads/2015/07/12014-kr.pdf (дата звернення: 26.03.2024).

ВИСНОВКИ. Складність вирішення проблеми допустимості цифрових (електронних) доказів пов'язана з тим, що вони мають складну технічну природу. Насамперед це зумовлено тим, що цей різновид доказів містить абстрактні технічні і математичні моделі, характеризується специфічними умовами виникнення, існування, копіювання та зберігання, що явно відрізняє їх від інших видів доказової інформації.

До недоліків чинного кримінального процесуального законодавства слід віднести відсутність легального визначення поняття «цифрові (електронні) докази» та їх джерел, на відміну від цивільного процесуального та адміністративного процесуального законодавства. Проте й запропоновані законодавцем визначення містять недоліки, зокрема в наведених дефініціях цифрових (електронних) доказів міститься невиправдане протиставлення суміжних понять «інформація», «дані» та «відомості».

На наше переконання, у визначенні цифрових (електронних) доказів слід відобразити таку обов'язкову їхню ознаку, як релевантність щодо певного кримінального провадження. Інакше кажучи, у кримінальному процесі цифровим (електронним) доказом може бути лише та інформація, яка має значення для певного кримінального провадження. Іншою обов'язковою складовою визначення поняття «цифровий (електронний) доказ» має бути вказівка на його специфічну природу. Водночас недоцільним слід визнати підхід, коли у визначеннях паралельно вказують на електронний характер такої інформації та її концентрацію на певному електронному носієві. Інформація, яка міститься на певному електронному носієві, є електронною, а не якоюсь іншою. Інакше це призводить до дублювання та є логічною помилкою. У такому разі джерелом цифрових (електронних) доказів слід вважати цифровий (електронний) об'єкт, за допомогою якого ця доказова інформація була створена, зафіксована або передана. Однак слід констатувати, що практика боротьби зі злочинністю повинна керуватись положеннями чинного кримінального процесуального законодавства України, а отже, виходити з формального розуміння цифрових (електронних) доказів як різновиду документів, зокрема як електронних документів.

Важливим для практики є чітке розуміння критеріїв, за якими цифрова (електронна) інформація може набувати значення доказу у кримінальному провадженні. З огляду на це визначено та розкрито такі критерії допустимості доказів: 1) належне джерело отримання доказів; 2) належний суб'єкт; 3) належний спосіб збирання доказів.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Абламський С. Є., Конюшенко Я. Ю. Стратегічне управління у сфері протидії злочинності в Україні. *Форум права*. 2023. № 1 (74). С. 122–131. DOI: https://doi.org/10.5281/zenodo.7699516.

2. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2008. 18 с.

3. Вапнярчук В. В. Теорія і практика кримінального процесуального доказування : монографія. Харків : Юрайт, 2017. 408 с.

4. Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : монографія. Львів : ЛьвДУВС, 2022. 204 с.

5. Зінченко В. М. Достатність доказів у кримінальному провадженні : дис. … канд. юрид. наук : 12.00.09. Одеса, 2020. 231 с.

6. Каланча І. Г., Столітній А. В. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. 2019. Вип. 146. С. 179–191. DOI: https://doi.org/10.21564/2414-990x.146.171218.

7. Коваленко А. В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2018. Вип. 4. С. 237–245.

8. Козицька О. Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 8. С. 418–421. DOI: https://doi.org/10.32782/2524-0374/2020-8/103.

9. Крет Г. Р. Міжнародні стандарти доказування у кримінальному процесі України: теоретико-правові та практичні основи : дис. … д-ра юрид. наук : 12.00.09. Одеса, 2020. 530 с.

10. Литвин О. В. Кримінально-процесуальне доказування у стадії судового розгляду : дис. … канд. юрид. наук : 12.00.09. Одеса, 2016. 214 с.

11. Метелев О. П. Гносеологічна і правова природа цифрових доказів у кримінальному провадженні. *Правова позиція*. 2018. № 1. С. 75–86.

12. Метелев О. П. Проблеми визначення допустимості і належності електронних (цифрових) доказів у кримінальному процесі. *Вісник кримінального судочинства*. 2019. № 3. С. 224–238. DOI: https://doi.org/10.17721/2413-5372.2019.3/224-238.

13. Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльне правознавство*. 2013. № 3–2. С. 313–315.

14. Слюсарчук Х. Р. Стандарти доказування у кримінальному провадженні : дис. … канд. юрид. наук : 12.00.09. Львів, 2017. 258 с.

15. Степаненко А. С. Стандарт доказування «поза розумним сумнівом» у кримінальному провадженні : дис. … канд. юрид. наук : 12.00.09. Одеса, 2017. 234 с.

16. Фігурський В. М. Докази в електронній формі у кримінальному провадженні. *Галицькі студії: юридичні науки*. 2023. № 4. С. 97–105. DOI: https://doi.org/10.32782/galician_studies/law-2023-4-14.

17. Цехан Д. М. Цифрові докази: поняття, особливості та місце в системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2013. № 5. С. 256–260.

18. Чупрікова І. Л. Допустимість доказів у світлі нового Кримінального процесуального кодексу : дис. … канд. юрид. наук : 12.00.09. Одеса, 2016. 191 с.

19. Шабаровський Б. В. Перевірка доказів у кримінальному процесі України : дис. … канд. юрид. наук : 12.00.09. Львів, 2019. 217 с.

20. Ablamskyi S. Ye., Havryliuk L. V., Drozd V. G., Nenia O. V. Substantial Violation of Human Rights and Freedoms as a Prerequisite for Inadmissibility of Evidence. *Justicia.* 2021. Vol. 26, No. 39. Pp. 47–56. DOI: https://doi.org/10.17081/just.26.39.4819.

Надійшла до редакції: 29.03.2024

Прийнята до опублікування: 18.06.2024

REFERENCES

1. Ablamskyi, S. Ye., & Koniushenko, Ya. Yu. (2023). Strategic Management of Crime Prevention in Ukraine. *Forum of Law, 1*(74), 122–131. https://doi.org/10.5281/zenodo.769951.

2. Ablamskyi, S. Ye., Havryliuk, L. V., Drozd, V. G., & Nenia, O. V. (2021). Substantial Violation of Human Rights and Freedoms as a Prerequisite for Inadmissibility of Evidence. *Justicia, 26*(39), 47–56. https://doi.org/10.17081/just.26.39.4819.

3. Bilousov, A. S. (2008). *Forensic analysis of computer malware objects* [Candidate thesis, Taras Shevchenko Kyiv National University].

4. Chuprikova, I. L. (2017). *Admissibility of evidence in light of the new Criminal Procedure Code* [Candidate dissertation, National University "Odesa Law Academy"].

5. Fihurskyi, V. M. (2023). Evidence in electronic form in criminal proceedings. *Galician Studies: Legal Sciences, 4*, 97–105. https://doi.org/10.32782/galician_studies/law-2023-4-14.

6. Hutnyk, A. V., Khytra, A. Ya. (2022). *Criminal procedural and forensic basics of using electronic documents in evidence*. LvSUIA.

7. Kalancha, I. H., & Stolitnii, A. V. (2019). Formation of the institute of electronic evidence in the criminal process of Ukraine. *Problems of Legality, 146*, 179–191. https://doi.org/10.21564/2414-990x.146.171218.

8. Kovalenko, A. V. (2018). Electronic evidence in criminal proceedings: current state and prospects of use. *Bulletin of the E. O. Didorenko Luhansk State University of Internal Affairs, 4*, 237–245.

9. Kozytska, O. H. (2020). On the concept of electronic evidence in criminal proceedings. *Juridical Scientific and Electronic Journal, 8*, 418–421. https://doi.org/10.32782/2524-0374/2020-8/103.

10. Kret, H. R. (2020). *International standards of evidence in the criminal process of Ukraine: theoretical, legal and practical foundations* [Doctoral dissertation, National University "Odesa Law Academy"].

11. Lytvyn, O. V. (2016). *Criminal procedural evidence at the stage of trial* [Candidate dissertation, National University "Odesa Law Academy"].

12. Metelev, O. P. (2018). Epistemological and legal nature of digital evidence in criminal proceedings. *Legal Position, 1*, 75–86.

13. Metelev, O. P. (2019). Problems of determining the admissibility and appropriateness of digital (electronic) evidence in criminal proceedings. *Herald of Criminal Justice, 3*, 224–238. https://doi.org/10.17721/2413-5372.2019.3/224-238.

14. Muradov, V. V. (2013). Electronic Evidence: A Forensic Aspect of Use. *Comparative Jurisprudence, 3–2*, 313–315.

15. Shabarovskyi, B. V. (2019). *Verification of evidence in the criminal process of Ukraine* [Candidate dissertation, Ivan Franko Lviv National University].

16. Sliusarchuk, Kh. R. (2017). *Standards of proof in criminal proceedings* [Candidate dissertation, Ivan Franko Lviv National University].

17. Stepanenko, A. S. (2017). *The "beyond a reasonable doubt" standard of proof in criminal proceedings* [Candidate dissertation, National University "Odesa Law Academy"].

18. Tsekhan, D. M. (2013). Digital evidence: concepts, features and place in the evidence system. *Scientific Bulletin of the International Humanitarian University. Series: Jurisprudence, 5*, 256–260.

19. Vapniarchuk, V. V. (2017) *Theory and practice of criminal procedural evidence*. Yurait.
20. Zinchenko, V. M. (2020). *Sufficiency of evidence in criminal proceedings computer* [Candidate dissertation, National University "Odesa Law Academy"].

Received the editorial office: 29 March 2024

Accepted for publication: 18 June 2024

VITALII VOLODYMYROVYCH ROMANIUK,
Candidate of Law, Associate Professor,
Kharkiv National University of Internal Affairs,
Faculty No. 1;
ORCID: https://orcid.org/0000-0001-6077-4591,
e-mail: romaniukukraine@gmail.com;

SERHIY YEVHENOVYCH ABLAMSKYI,
Candidate of Law, Associate Professor,
Kharkiv National University of Internal Affairs,
Department of Criminal Procedure and Organization of Pre-trial Investigation,
ORCID: https://orcid.org/0000-0003-4716-3985,
e-mail: ablamu4@gmail.com

CRITERIA FOR THE ADMISSIBILITY OF DIGITAL (ELECTRONIC) EVIDENCE IN CRIMINAL PROCEEDINGS

The article is devoted to consideration of modern problems of determining the admissibility of digital (electronic) evidence in criminal proceedings. Given the importance of the outlined issues, the main purpose of the study is to characterize each component of the admissibility of such evidence, namely: the proper source of receipt, the proper subject, and the proper method of collection. It is emphasized that the biggest doctrinal problem that creates an obstacle in the definition of such criteria is the lack of a unified scientific vision regarding the concept of digital (electronic) evidence and the definition of its source. The existence of three scientific approaches to the solution of this problem was established, taking into account the author's position on possible ways of its elimination. Some practical aspects related to the problems of compliance with the criteria of admissibility of digital (electronic) evidence during the investigation of criminal offenses are disclosed.

On the basis of a systematic analysis of scientific work and judicial practice, it was determined that the difficulty of solving problematic aspects of the admissibility of digital (electronic) evidence is related to their complex technical nature. This is due to the fact that digital (electronic) evidence contains abstract technical and mathematical models, characterized by specific conditions of origin, existence, copying and storage, which significantly differ from other types of evidentiary information.

It has been proven that when determining digital (electronic) evidence, such a mandatory feature as relevance to a certain criminal proceeding should be displayed. This is explained by the fact that in a criminal trial, digital (electronic) evidence can only be the information that is of direct importance for a certain criminal proceeding. Another mandatory component of the definition of "digital (electronic) evidence" should be an indication of its specific nature. At the same time, it is inappropriate to recognize the approach when the definitions simultaneously indicate the electronic nature of such information and its concentration on a certain electronic medium. Information that is on a certain electronic medium is electronic and not any other. Otherwise, it leads to duplication and is a logical fallacy. It is suggested that the source of digital (electronic) evidence be considered a digital (electronic) object by means of which this evidentiary information was created, recorded or transmitted.

The lack of official definition of digital (electronic) evidence and their sources, in contrast to civil and administrative procedural legislation, is among the shortcomings of the current criminal procedural legislation of Ukraine. However, the definitions proposed by the legislator contain shortcomings, in particular, the fixed definitions of digital (electronic) evidence contain an unjustified opposition of related concepts, such as "information", "data" and "facts".

Key words: *criminal proceedings, digital (electronic) evidence, admissibility of evidence, criteria for admissibility of evidence, electronic document, investigator, inquirer, prosecutor.*

Цитування (ДСТУ 8302:2015): Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право і безпека*. 2024. № 2 (93). С. 140–150. DOI: https://doi.org/10.32631/pb.2024.2.13.

Citation (APA): Romaniuk, V. V., & Ablamskyi, S. Ye. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Law and Safety, 2*(93), 140–150. https://doi.org/10.32631/pb.2024.2.13.