

УДК 343.14

DOI https://doi.org/10.32782/galician_studies/law-2023-4-14**Фігурський Володимир Михайлович,**

кандидат юридичних наук, доцент,

доцент кафедри кримінального процесу і криміналістики
Львівського національного університету імені Івана Франка

ORCID ID: 0000-0002-5329-8985

ДОКАЗИ В ЕЛЕКТРОННІЙ ФОРМІ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Стаття присвячена висвітленню суті доказів в електронній формі та з'ясуванню, до якого з видів процесуальних джерел доказів у кримінальному провадженні вони належать.

Зазначено, що поняття «цифрові докази» та «електронні докази» у спеціальній літературі та офіційних документах переважно вживають як синоніми. Утім технічно коректним є використання категорії «цифрові докази». Водночас, цифровим є електронний доказ, згенерований у числовому форматі, або перетворений у нього.

Аргументовано, що у правовій доктрині та у правовому регулюванні сформовано декілька підходів до тлумачення суті електронних доказів. Більшість учених під електронними доказами розуміють дані або інформацію, яка з'явилася внаслідок використання цифрової техніки і відповідного програмного забезпечення, та може бути використана в судовому процесі. Інші дослідники визначають електронні докази як об'єкти цифрового (електронного) виміру, що можуть мати значення для кримінального провадження. Третій підхід до трактування електронних доказів – будь-які докази, отримані з даних, що містяться в будь-якому пристрої або вироблені ним, функціонування якого залежить від програмного забезпечення або даних, що зберігаються або передаються через комп'ютерну систему чи мережу.

Обгрунтовано, що докази, про які йдеться, коректніше називати «доказами в електронній формі», оскільки ця назва відображає середовище створення, використання, зберігання, демонстрації, виявлення, фіксації, вилучення та дослідження інформації, яка має значення для кримінального провадження. Електронна форма інформації становить нематеріальну версію інших форм інформації (письмової, графічної, аудіовізуальної та їх поєднанні). Вона може відтворювати абсолютно всі елементи інформації в матеріальній формі. Понад те, електронна форма має перевагу, адже містить параметри, недоступні іншим формам (наприклад, метадані).

Сформульовано авторське визначення доказів в електронній формі – це інформація, створена, оброблена, збережена або передана за допомогою аналогових чи цифрових сигналів, що має значення для кримінального провадження.

Констатовано, що КПК України поки не виокремлює докази в електронній формі. Розглядаючи їх у контексті документів, законодавець поширив на докази в електронній формі загальні правила використання доказів у кримінальному провадженні.

Підкреслено, що через особливості доказів в електронній формі точаться дискусії щодо їх приналежності до процесуальних джерел доказів. Зроблено висновок, що докази в електронній формі є новим соціально-правовим явищем в інформаційну епоху. У порівнянні з доказами у поза електронній формі, вони мають власну природу, яка зумовлює їх особливості, потребують іншого механізму доказування, що свідчить про самостійне місце у системі процесуальних джерел доказів.

Ключові слова: кримінальне провадження, доказування, засоби доказування, докази, процесуальні джерела доказів, докази в електронній формі.

Fihurskyi V. M. Evidence in electronic form in criminal proceedings

The article is aimed at highlighting the essence of evidence in electronic form and determining which type of procedural sources of evidence in criminal proceedings they belong to.

The author notes that the concepts of “digital evidence” and “electronic evidence” are mostly used as synonyms in the specialised literature and official documents. However, it is technically correct to use the category of “digital evidence”. At the same time, digital evidence is electronic evidence generated in a numerical format or converted into it.

The author argues that several approaches to the interpretation of the essence of electronic evidence have been formed in legal doctrine and legal regulation. Most scholars understand electronic evidence to be data or information that has emerged as a result of the use of digital technology and relevant software and can be used in court proceedings. Other researchers define electronic evidence as objects of digital (electronic) dimension that may be relevant to criminal proceedings. The third approach to the interpretation of electronic evidence is any evidence obtained from data contained in or produced by any device whose functioning depends on software or data stored or transmitted through a computer system or network.

It is substantiated that the evidence in question should be more correctly called “evidence in electronic form”, since this name reflects the environment for creating, using, storing, displaying, detecting, recording, retrieving and examining information relevant to criminal proceedings. The electronic form of information is an intangible version of other forms of information (written, graphic, audiovisual and their combination). It can reproduce absolutely all elements of information in a tangible form. Moreover, the electronic form has the advantage of containing parameters that are not available in other forms (e.g. metadata).

The author’s definition of evidence in electronic form is formulated – it is information created, processed, stored or transmitted by means of analogue or digital signals which is relevant for criminal proceedings.

The author notes that the CPC of Ukraine does not yet distinguish evidence in electronic form. Considering them in the context of documents, the legislator has extended the general rules for the use of evidence in criminal proceedings to electronic evidence.

It is emphasised that due to the peculiarities of electronic evidence, there are ongoing discussions about its belonging to procedural sources of evidence. The author concludes that electronic evidence is a new social and legal phenomenon in the information age. Compared to non-electronic evidence, it has its own nature which determines its peculiarities and requires a different mechanism of proof, which indicates an independent place in the system of procedural sources of evidence.

Key words: *criminal proceedings, proof, means of proof, evidence, procedural sources of evidence, evidence in electronic form.*

Актуальність проблеми. Докази в електронній формі вже відіграють важливу роль у розслідуванні та судовому розгляді кримінальних проваджень нарівні з аналоговими доказами. Адже ми живемо в час, коли більшість дій, які люди раніше робили вручну, тепер здійснюються за допомогою електронних гаджетів і комп’ютерних мереж. Діяльність, що відбувається за допомогою сучасних електронних пристроїв, зазвичай залишає цифрові сліди, які можуть слугувати доказами в кримінальному процесі. А це означає можливість їх виявлення, фіксації та вилучення для використання у кримінальному процесуальному доказуванні.

Аналіз останніх досліджень і публікацій. Проблематиці використання доказів в електронній формі у кримінальному провадженні присвячено чимало робіт як в українській, так і зарубіжній кримінальній процесуальній доктрині. Водночас, досі відсутній єдиний підхід до розуміння суті такого роду доказів, їх приналежності до процесуальних джерел доказів.

Мета дослідження – висвітлити суть доказів в електронній формі та з’ясувати, до якого з видів процесуальних джерел доказів у кримінальному провадженні вони належать.

Виклад основного матеріалу дослідження. З розвитком комп’ютерних технологій та їх широким використанням, у середині минулого століття сформувалася концепція комп’ютерних доказів (*computer evidence*), які генерують електромагнітні сигнали під час роботи комп’ютерної системи і використовуються для встановлення елементів предмету доказування. Згодом, із застосуванням мережевих технологій, з’явилося поняття мережевих доказів (*network evidence*), яке стосується електромагнітних сигналів у мережевому середовищі. Наприкінці ХХ ст., окрім комп’ютера та мережі, з’явилася чимала кількість цифрових пристроїв, призначених для передавання цифрових сигналів телефонного, телеграфного і телевізійного зв’язку. У правничих колах результати застосування таких цифрових пристроїв назвали «цифровими доказами» (*digital evidence*) або «електронними доказами» (*electronic evidence*) [1, с. 112].

Поняття «цифрові докази» та «електронні докази» у спеціальній літературі та офіційних документах переважно вживають як синоніми. Технічно коректним є використання категорії «цифрові докази» [2, с. 41]. Слово «цифровий» позначає тип сигналу, що використовується у пристрої, відмінний від аналогового. Цифровий сигнал є непостійним, дискретним у вигляді хвиль квадратної форми, натомість аналоговий – завжди постійний, безперервний у формі синусоїди. Пристрої працюють як з аналоговими, так і з цифровими сигналами, але більшість мікропроцесорів, комп’ютерів і логічних блоків є суто цифровими компонентами [3; 4]. Проте, незалежно від виду сигналу, його створення, передачу, збереження, використання забезпечує відповідний електронний пристрій. Прикметник «електронний» означає створений, записаний, переданий чи збережений в цифровій або іншій нематеріальній формі за допомогою електронного, магнітного, оптичного або будь-якого іншого способу, що має можливості для створення, запису, передачі або збереження даних. Вживання одиниці мови «електронний» для позначення виду доказу не обмежує тип електроніки (цифрової, аналогової, мікроелектроніки, оптоелектроніки) чи інтегральних схем, результати застосування яких можуть мати значення для кримінального провадження. Тож цифровим є електронний доказ, згенерований у числовому форматі, або перетворений у нього. Водночас, з появою нових технологій використання цифрових доказів невпинно зростатиме.

Нині чинне українське кримінальне процесуальне регулювання не містить легальної дефініції електронних доказів. Не є винятком й іноземне кримінальне процесуальне законодавство.

З огляду на це, у правовій доктрині та у правовому регулюванні сформовано декілька підходів до тлумачення суті електронних доказів.

Більшість учених під електронними доказами розуміють дані або інформацію, яка з'явилася внаслідок використання цифрової техніки і відповідного програмного забезпечення, та може бути використана в судовому процесі [5, с. 72; 6, с. 257; 7, с. 250; 8, с. 301, 304; 9, с. 29; 10, с. 82; 11; 12, с. 235; 13; 14; 15, с. 367; 2, с. 43]. Інші дослідники визначають електронні докази як об'єкти цифрового (електронного) виміру, що можуть мати значення для кримінального провадження [16, с. 64; 17, с. 191; 18, с. 43]. Третій підхід до трактування електронних доказів сформулював Комітет Міністрів Ради Європи – будь-які докази, отримані з даних, що містяться в будь-якому пристрої або вироблені ним, функціонування якого залежить від програмного забезпечення або даних, що зберігаються або передаються через комп'ютерну систему чи мережу [19].

Доречно зазначити, що згідно з ч. 1 ст. 96 ГПК України, ч. 1 ст. 99 КАС України та ч. 1 ст. 100 ЦПК України електронні докази визначені як «інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосні повідомлення, метадані, бази даних та інші дані в електронній формі» [20; 21; 22]. Так само, у ч. 1 ст. 100¹ законопроекту «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» під електронним доказом розуміється «інформація в електронній (цифровій) формі з відомостями, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження» [23]. У цих положеннях відображений перший підхід до розуміння електронних доказів.

Водночас, у наведених дефініціях електронних доказів привертає увагу невідповідне протиставлення суміжних понять «інформація», «дані» та «відомості». Відповідно до ст. 1 Закону України «Про інформацію» інформацією вважаються «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [24].

Крім того, уявляється, що докази, про які йдеться, коректніше називати «доказами в електронній формі», оскільки ця назва відображає середовище створення, використання, зберігання, демонстрації, виявлення, фіксації, вилучення та дослідження інформації, яка має значення для кримінального провадження. Електронна форма інформації становить нематеріальну версію інших форм інформації (письмової, графічної, аудіовізуальної та їх поєднанні). Вона може відтворювати абсолютно всі елементи інформації в матеріальній формі. Понад те, електронна форма має перевагу, адже містить параметри, недоступні іншим формам (наприклад, метадані).

Тож докази в електронній формі – це інформація, створена, оброблена, збережена або передана за допомогою аналогових чи цифрових сигналів, що має значення для кримінального провадження.

Через особливості доказів в електронній формі точаться дискусії щодо їх приналежності до процесуальних джерел доказів. Загалом існують такі позиції.

Перша. Вважається, що докази в електронній формі є різновидом документів. Ця думка ґрунтується на чинному правовому регулюванні. Так, відповідно до п. 1 ч. 2 ст. 99 КПК України до документів можуть належати «матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані)». До того ж, у ч. 4 цієї ж статті зазначено, що «дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що містяться 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».

У п. б ст. 1 Конвенції про кіберзлочинність 2001 р. термін «комп'ютерні дані» визначений 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». Своєю чергою, термін «комп'ютерна система» витлумачений як «будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних» [25].

З вищенаведеного випливає, що інформація, яка має значення для кримінального провадження і зберігається в електронній формі, незалежно від електронного носія даних, може бути використана як документ. Понад те, кримінальний процесуальний закон не зобов'язує суб'єктів доказування перетворювати таку інформацію з електронної форми в будь-яку іншу форму, наприклад, у роздруківку.

Однак аналізований підхід не враховує того, що докази в електронній формі також можуть бути знаряддям вчинення кримінального правопорушення (для прикладу, спеціально розроблена програма для несанкціонованого проникнення у комп'ютер), зберегти на собі його сліди (приміром, метадані, що засвідчують копіювання інформації з комп'ютера на інший пристрій), бути об'єктом кримінально протиправних дій (скажімо, криптовалюта, викрадена з криптогаманця), містити інші відомості про факти і обставини, що встановлюють під час кримінального провадження (зокрема канал у Telegram, створений для розповсюдження порнографічного контенту), тобто, не будучи матеріальними об'єктами, належати до тих категорій, про які йдеться у ч. 1 ст. 98 КПК України.

Друга. Деякі дослідники не відносять докази в електронній формі до жодного з джерел доказів, оскільки вважають, що вони – лише спосіб відображення доказів, а джерело доказів може бути продемонстроване у цифровому форматі [26, с. 186–188]. Зокрема цифрові матеріали розглядаються як різновид речових доказів [27, с. 14], а також водночас як різновид речових доказів і документів в електронній формі [28, с. 320; 29, с. 276].

Третя. Інші науковці вважають, що докази в електронній формі є новим процесуальним джерелом доказів. Стверджують, що такі докази істотно відрізняються від документів. Лист, графік або малюнок можна безпосередньо продемонструвати на видимому носії, тоді як докази в електронній формі створюються, зберігаються і передаються шляхом перетворення інформації в цифровий код, а також демонструються і зчитуються за допомогою спеціальних пристроїв і програмного забезпечення. Спосіб зберігання та відображення інформації між ними докорінно різний. З іншого боку, факт редагування документа в електронній формі не завжди можливо виявити лише ознайомившись із його змістом, на відміну від паперового документа, де зміна залишає матеріальні сліди. Відмінність також простежується між доказами в електронній формі та аудіовізуальними матеріалами. Останні відтворюються за допомогою відео- чи аудіопристрою, а інформація сприймається на зір або на слух, або обома способами одночасно. Звук відтворюється одним носієм, тоді як відео може бути відтворене одним або кількома носіями. Докази в електронній формі, з іншого боку, демонструються за допомогою кількох носіїв, які не зберігаються так само як аудіовізуальні матеріали. Аудіовізуальні матеріали не можуть включати докази в електронній формі, натомість останні можуть охоплювати аудіовізуальні дані. Тож пропонується, щоб докази в електронній формі були віднесені до процесуальних джерел доказів на рівні з показаннями, речовими доказами, документами та висновками експертів [6, с. 259; 30, с. 242; 10, с. 83; 31, с. 216].

Уявляється, що з погляду перспективи розвитку українського доказового права представники третьої з вищенаведених позицій мають рацію. Докази в електронній формі є новим соціально-правовим явищем в інформаційну епоху. У порівнянні з доказами у поза електронній формі, вони мають власну природу, яка зумовлює їх особливості, потребують іншого механізму доказування, що свідчить про самостійне місце у системі процесуальних джерел доказів.

Доказам в електронній формі властиві унікальні ознаки, що відрізняють їх від інших джерел доказів та зумовлені їх природою: 1) їх творцем є як людина, так і комп'ютерна система; 2) мають нематеріальний вираз, що дає їм можливість зберігатися на відповідному носії (приміром смарт-годиннику, смартфоні, планшеті, ноутбучі, жорстких дисках, флеш-накопичувачах) чи кількох носіях одночасно, проте без нероздільного зв'язку з ними або перебувати у цифровому середовищі (зокрема хмарному сховищі) без такого носія; 3) внаслідок цього підлягають сприйняттю лише завдяки використанню спеціальних технічних засобів і програмного забезпечення; 4) можуть зберігатися без змін упродовж тривалого часу, бути скопійовані чи переслані, не зазнаючи коригування їх змісту, та не мають обмежень у кількості разів використання; 5) з іншого боку, через свою природу докази в електронній формі піддатливі до маніпуляцій та знищення; 6) копії деяких доказів в електронній формі (документів) за наявності обов'язкових реквізитів (зокрема електронного підпису) прирівнюються до оригіналу та можуть використовуватися у кількох справах одночасно.

Людство перебуває в ері стрімкого розвитку інформаційних технологій та широкого застосування електронних продуктів. Інформація, створена, збережена чи передана за їх допомогою є скрізь. Доказове право та теорія доказів не можуть невідрефлексувати на такі факти. При цьому, чимало

цифрових даних не мають аналогів у вигляді доказів в поза електронній формі. Записи смартфонів, пам'ять принтера та історія версій документів – декілька прикладів доказів в електронній формі, щодо використання яких у доказуванні положення традиційної теорії доказів навряд чи можуть бути повністю актуальними. Понад те, не лише процесуальна доктрина, але й правове регулювання стикається з низкою викликів, пов'язаних з особливостями такого роду доказів, зокрема вразливістю до змін і знищення. Виклики значно ускладнюються, коли залучаються такі розподілені та мережеві технології, як хмарні обчислення і технології блокчейн. Ще одну складність становить висока ємність сховищ даних, що підлягають аналізу під час кримінального провадження. Своєю чергою, це потребує достатньої кількості технічних ресурсів. Хоча певні правові позиції ККС про використання доказів в електронній формі сформульовані, вони все ще не можуть задовольнити потреби судової практики. У підсумку – традиційні правила кримінального процесуального доказування вимагають осучаснення.

Водночас нормативно закріпити вичерпний перелік джерел отримання доказів в електронній формі як це пропонують деякі дослідники [32, с. 117; 31, с. 216] навряд чи можливо з огляду на швидкий розвиток, зміну і удосконалення комп'ютерних технологій.

Як уже було зазначено вище, КПК України поки не виокремлює докази в електронній формі. Розглядаючи їх у контексті документів, законодавець поширив на докази в електронній формі загальні правила використання доказів у кримінальному провадженні.

Водночас, нині діє значна кількість міжнародних, регіональних та національних правових актів і передових практик, пов'язаних з правовим регулюванням застосування доказів в електронній формі.

Зокрема Міжнародна організація з комп'ютерних доказів (*International Organization on Computer Evidence – IOCE*) сформулювала низку принципів, які мають бути дотримані під час розслідувань злочинів, вчинених з використанням комп'ютерів: після вилучення цифрових доказів, вчинені дії не повинні змінювати такі докази; коли особі необхідно отримати доступ до оригіналу цифрового доказу, ця особа має бути компетентною в цьому аспекті; усі дії, пов'язані з вилученням, доступом, зберіганням або передачею цифрових доказів, мають бути повністю задокументовані, збережені та доступні для перегляду; особа несе відповідальність за всі дії, вчинені щодо цифрових доказів, поки такі докази перебувають у її розпорядженні; будь-який орган, відповідальний за вилучення, доступ, зберігання або передачу цифрових доказів, несе відповідальність за дотримання цих принципів [33].

Рекомендації щодо використання доказів в електронній формі у національних правових системах сформульовані й Комітетом Міністрів Ради Європи. Серед цих рекомендацій привертають увагу такі. Вирішувати потенційну доказову силу електронних доказів відповідно до національного законодавства мають суди. Електронні докази повинні оцінюватися так само, як і інші види доказів, зокрема щодо їх допустимості, автентичності, точності та цілісності. Обробка електронних доказів не повинна бути не вигідною для сторін або надавати несправедливу вигоду одній із них. У принципі, суди не повинні заперечувати юридичну силу електронних доказів лише через відсутність вдосконаленого, кваліфікованого або аналогічного захищеного електронного підпису. Суди повинні знати про доказову силу метаданих і потенційні наслідки їх невикористання. Сторонам має бути дозволено подавати електронні докази в оригінальному електронному форматі без необхідності надання роздруківок. Беручи до уваги вищий ризик потенційного знищення або втрати електронних доказів порівняно з неелектронними доказами, держави-члени повинні встановити процедури безпечного вилучення та збору електронних доказів. Суди повинні знати про конкретні проблеми, які виникають під час вилучення та збору електронних доказів за кордоном, у тому числі в транскордонних справах. Електронні докази слід збирати, структурувати та управляти у спосіб, аби полегшити їх передачу до інших судів, зокрема до апеляційного суду. Слід заохочувати та сприяти передачі електронних доказів електронними засобами з метою підвищення ефективності судового розгляду. Системи та пристрої, що використовуються для передачі електронних доказів, повинні бути здатними зберігати їх цілісність. Суди можуть вимагати дослідження електронних доказів експертами, особливо коли порушуються складні доказові питання або якщо є підозри про маніпулювання електронними доказами. Суди повинні вирішувати, чи мають такі особи достатній досвід у цій справі. Що стосується достовірності, суди повинні враховувати всі відповідні чинники джерела та автентичності електронних доказів. Наскільки це дозволяє національна правова система та на розсуд суду, електронні дані повинні прийматися як докази, якщо достовірність таких даних не оспорується однією зі сторін. Наскільки це дозволяє національна правова система та на розсуд суду, слід презюмувати достовірність електронних даних за умови, що особу підписанта можна підтвердити, а цілісність даних захищено, якщо і доки не буде є обґрунтовані сумніви в протилежному. Наскільки це

передбачає національна правова система, якщо державний орган передає електронні докази незалежно від сторін, такі докази є переконливими щодо їх змісту, якщо і доки не буде доведено протилежне. Електронні докази слід зберігати таким чином, щоб зберігали читабельність, доступність, цілісність, автентичність, достовірність і, де це можливо, конфіденційність і приватність. Електронні докази слід зберігати зі стандартизованими метаданими, щоб контекст їх створення був зрозумілим. Суди повинні архівувати електронні докази відповідно до національного законодавства. Електронні архіви повинні відповідати всім вимогам безпеки та гарантувати цілісність, автентичність, конфіденційність і якість даних, а також повагу до приватного життя. Судді та юристи-практики повинні знати про еволюцію інформаційних технологій, яка може вплинути на доступність та цінність електронних доказів. Правова освіта повинна включати модулі з електронних доказів [19].

Ще одним прикладом регіонального акту, присвяченого правовому регулюванню використання доказів в електронній формі є Проект модельного закону Співдружності держав Карибського басейну про електронні докази 2017 р. (*Commonwealth Draft Model Law on Electronic Evidence*). Серед основних положень цього документу доцільно зазначити такі. На електронні докази поширюються властивості належності, допустимості та достовірності, за винятком випадків, визначених цим актом. Доказ не може бути визнаний недопустимим лише на тій підставі, що він має електронну форму. З метою перевірки допустимості електронних даних, можуть бути подані докази щодо будь-якого стандарту або практики того, як ці електронні дані повинні бути записані або збережені, беручи до уваги тип діяльності, у межах якої їх використовували, а також характеру та мети електронних даних. Сторона, яка подає електронний доказ, несе тягар доказування його достовірності. За відсутності доказів протилежного, цілісність електронних даних або системи, в якій записано чи зберігаються такі дані, презюмується в будь-якому судовому процесі: а) за наявності доказів, які підтверджують висновок про те, що в усі істотні моменти часу комп'ютерна система або аналогічний пристрій працював належним чином, або, якщо це не так, то такі обставини не вплинули на цілісність даних, а також немає інших розумних сумнівів у їх цілісності; б) якщо буде встановлено, що електронні дані були записані або зберігалися стороною, інтереси якої не відповідають інтересам сторони, яка прагне їх подати; або в) якщо встановлено, що електронні дані були записані або зберігалися в звичайному процесі ведення діяльності особою, яка не є стороною провадження, і яка не записувала провадження та не здійснювала запис або зберігання під контролем сторони, яка бажає подати ці дані. З метою перевірки допустимості і достовірності електронних даних особа, яка їх подала, може бути піддана перехресному допиту стороною з протилежними інтересами. Якщо інше не передбачено будь-яким іншим законом, електронні дані можуть бути визнані допустимими на розсуд суду, якщо сторони судового провадження прямо погодилися, що їх допустимість не може бути оспорена. Угода між сторонами щодо допустимості електронних даних не робить їх допустимими у кримінальному провадженні, якщо на момент укладення цієї угоди обвинувачений не мав захисника [34].

Висновки. Ці та інші рекомендації доцільно взяти до уваги при удосконаленні положень законопроекту від 31 серпня 2020 р. № 4004, яким пропонується запровадження у кримінальне провадження електронних доказів як самостійного процесуального джерела доказів. З огляду на невпинний розвиток технологій, що породжує появу нових прийомів з'ясування фактів та обставин, що мають значення для кримінального провадження і підлягають доказуванню, розширення системи процесуальних джерел доказів уявляється неминучим.

Література

1. Jin Du, Liping Ding. Research on the Rules of Electronic Evidence in Chinese Criminal Proceedings. *International Journal of Digital Crime and Forensics*. 2020. Vol. 12. Issue 3. P. 111–121.
2. Lewulis P. Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law. *Criminal Law Forum*. 2022. № 33. P. 39–62.
3. Difference between Analog and Digital Signal. URL: <https://byjus.com/physics/difference-between-analog-and-digital/>
4. Analog vs. Digital. URL: <https://learn.sparkfun.com/tutorials/analog-vs-digital/all>
5. Perrin B., Rémy M., Roubaty R. Electronic Evidence in Swiss Criminal Procedure. *Digital Evidence and Electronic Signature Law Review*. 2011. Vol. 8. P. 70–75.
6. Цехан Д.М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2013. № 5. С. 256–260.

7. Алексєєва-Процюк Д.О., Брисковська О.М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти правозастосування. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. С. 247–253.
8. Вернидубов І., Белікова С. Електронні докази: поняття, особливості та проблеми щодо їх дослідження судом. *European Political and Law Discourse*. 2018. Vol. 5. Issue 2. С. 299–305.
9. Столітній А.В. Електронне кримінальне провадження на досудовому розслідуванні: автореф. дис. ... докт. юрид. наук: 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018. 42 с.
10. Метелев О.П. Гносеологічна і правова природа цифрових доказів у кримінальному провадженні. *Правова позиція*. 2018. № 1. С. 75–86.
11. Novak M. Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration. *Journal of Digital Forensics, Security and Law*. 2020. Vol. 14. № 4. URL: <https://commons.erau.edu/jdfsl/vol14/iss4/3>
12. Nikoloska S., Gjoshеva M. Electronic Evidence and its Significance in Investigations. *Хоризонти*. 2021. № 2. Р. 231–239.
13. Moussa A.F. Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*. 2021. № 11. URL: <https://ejfs.springeropen.com/articles/10.1186/s41935-021-00234-6>
14. General Principles for Digital Evidence. Conference of International Investigators (CII 2021). URL: <https://www.ciiinvestigators.org/wp-content/uploads/2021/11/CII-General-Principles-for-Digital-Evidence-21stCII.pdf>
15. Свистун Я.В. До питання правової природи електронних доказів. *Сучасні тенденції розвитку криміналістики та кримінального процесу в умовах воєнного стану*. Тези доповідей Міжнародної науково-практичної конференції (м. Харків, 25 листопада 2022 року). Харків, 2022. С. 363–368.
16. Tsvetkova A. Electronic evidence in Bulgaria – one step further, one step back. *Digital Evidence and Electronic Signature Law Review*. 2018. Vol. 15. Р. 60–69.
17. Oręziak B. Dowody elektroniczne a sprawiedliwość procesu karnego. *Prawo w Działaniu*. 2020. № 41. S. 187–196.
18. Рябущенко Д.Ю. Концептуально-теоретична проблематика категорії «цифрових (електронних)» доказів у кримінальному провадженні. *Економіка. Фінанси. Право*. 2023. № 5. С. 42–47.
19. Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings. *Adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers' Deputies*. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168_0902e0c
20. Господарський процесуальний кодекс від 6 листопада 1991 р. № 1798-XII. URL: <https://zakon.rada.gov.ua/laws/show/1798-12#Text>
21. Кодекс адміністративного судочинства України від 6 липня 2005 р. № 2747-IV. URL: <https://zakon.rada.gov.ua/laws/show/2747-15#Text>
22. Цивільний процесуальний кодекс України від 18 березня 2004 р. № 1618-IV. URL: <https://zakon.rada.gov.ua/laws/show/1618-15#Text>
23. Проект закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів від 31 серпня 2020 р. № 4004. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771
24. Закон України «Про інформацію» від 2 жовтня 1992 р. № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
25. Конвенція про кіберзлочинність від 23 листопада 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
26. Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. 2016. Вип. 146. С. 186–188.
27. Білоусов А.С. Криміналістичний аналіз об'єктів комп'ютерних злочинів: автореф. дис. ... канд. юрид. наук: 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність / Київський національний університет імені Тараса Шевченка. К., 2008. 18 с.
28. Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 8. С. 418–421.
29. Дегтярова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Юридичний вісник*. 2021. № 6. С. 273–278.
30. 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.
31. Ангеленюк А.-М.Ю. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2023. Вип. 79. Ч. 2. С. 214–218.

32. Чернявський С.С., Орлов Ю.Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства*. 2017. № 2. С. 112–124.
33. International principles for computer evidence. URL: <https://www.thefreelibrary.com/International+principles+for+computer+evidence.-a0137863426>
34. Commonwealth Draft Model Law on Electronic Evidence. LMM(02)12. URL: https://www.oas.org/juridico/spanish/cyber/cyb4_evidence_law.pdf

References

- Jin Du, & Liping Ding (2020). Research on the Rules of Electronic Evidence in Chinese Criminal Proceedings. *International Journal of Digital Crime and Forensics*, 12 (3), 111–121 [in English].
- Lewulis, P. (2022). Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law. *Criminal Law Forum*, 33, 39–62 [in English].
- Difference between Analog and Digital Signal. Retrieved from: <https://byjus.com/physics/difference-between-analog-and-digital/> [in English].
- Analog vs. Digital. Retrieved from: <https://learn.sparkfun.com/tutorials/analog-vs-digital/all> [in English].
- Perrin, B., Rémy, M., & Roubaty, R. (2011). Electronic Evidence in Swiss Criminal Procedure. *Digital Evidence and Electronic Signature Law Review*, 8, 70–75. [in English].
- Tsekhan, D.M. (2013). Tsyfrovі dokazy: poniattia, osoblyvosti ta mistse u systemi dokazuvannia [Digital evidence: concept, features and place in the system of evidence]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriya: Yurysprudentsiia [Scientific Bulletin of the International Humanitarian University. Series: Jurisprudence]*, 5, 256–260 [in Ukrainian].
- Aliexsieieva-Protsiuk, D.O., & Bryskovska, O.M. (2018). Elektronni dokazy v kryminalnomu sudochynstvi: poniattia, oznaky ta problemni aspekty pravozastosuvannia [Electronic Evidence in Criminal Proceedings: Concept, Signs and Problematic Aspects of Law Enforcement]. *Naukovyi visnyk publicznego ta pryvatnoho prava [Scientific Bulletin of Public and Private Law]*, 2, 247–253 [in Ukrainian].
- Vernyubov, I., & Belikova, S. (2018). Elektronni dokazy: poniattia, osoblyvosti ta problemy shchodo yikh doslidzhennia sudom [Electronic Evidence: Concept, Peculiarities and Problems of its Examination by the Court]. *European Political and Law Discourse*, 5 (2), 299–305 [in Ukrainian].
- Stolitnii, A.V. (2018). Elektronne kryminalne provadzhennia na dosudovomu rozsliduvanni [Electronic criminal proceedings at the pre-trial investigation]. *Doctor's thesis*. Dnipro State University of Internal Affairs [in Ukrainian].
- Metev, O.P. (2018). Hnoseolohichna i pravova pryroda tsyfrovyykh dokaziv u kryminalnomu provadzhenni [Epistemological and legal nature of digital evidence in criminal proceedings]. *Pravova pozytsiia*, 1, 75–86 [in Ukrainian].
- Novak, M. (2020). Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration. *Journal of Digital Forensics, Security and Law*, 14 (4). Retrieved from: <https://commons.erau.edu/jdfsl/vol14/iss4/3> [in English].
- Nikoloska, S., & Gjosheva, M. (2021). Electronic Evidence and its Significance in Investigations. *Хоризонти*, 2, 231–239 [in English].
- Moussa, A.F. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, 11. Retrieved from: <https://ejfs.springeropen.com/articles/10.1186/s41935-021-00234-6> [in English].
- General Principles for Digital Evidence. Conference of International Investigators (CII 2021). Retrieved from: <https://www.ciinvestigators.org/wp-content/uploads/2021/11/CII-General-Principles-for-Digital-Evidence-21stCII.pdf> [in English].
- Svystun, Ya.V. (2022, November 25, Kharkiv). Do pytannia pravovoi pryrody elektronnykh dokaziv. *Suchasni tendentsii rozvytku kryminalistyky ta kryminalnoho protsesu v umovakh voiennoho stanu. Tezy dopovidei Mizhnarodnoi naukovo-praktychnoi [On the legal nature of electronic evidence. Modern trends in the development of criminalistics and criminal procedure under martial law. Abstracts of the International Scientific and Practical Conference]*, 363–368 [in Ukrainian].
- Tsvetkova, A. (2018). Electronic evidence in Bulgaria – one step further, one step back. *Digital Evidence and Electronic Signature Law Review*, 15, 60–69 [in English].
- Oręziak, B. (2020). Dowody elektroniczne a sprawiedliwość procesu karnego. *Prawo w Działaniu*, 41, 187–196 [in Polish].
- Riabushchenko, D.Yu. (2023). Kontseptualno-teoretychna problematyka katehorii “tsyfrovyykh (elektronnykh)” dokaziv u kryminalnomu provadzhenni [Conceptual and theoretical issues of the category of “digital (electronic)” evidence in criminal proceedings]. *Ekonomika. Finansy. Pravo*, 5, 42–47 [in Ukrainian].
- Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings. *Adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers' Deputies*. Retrieved from: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c [in English].
- Verkhovna Rada of Ukraine (1991). Hospodarskyi protsesualnyi kodeks vid 6 lystopada 1991 r. № 1798-XII [Commercial Procedure Code of 6 November 1991, No. 1798-XII]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/1798-12#Text> [in Ukrainian]

21. Verkhovna Rada of Ukraine (2005). Kodeks administratyvnoho sudochynstva Ukrainy vid 6 lypnia 2005 r. № 2747-IV [Code of Administrative Procedure of Ukraine of 6 July 2005 No. 2747-IV]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2747-15#Text> [in Ukrainian]
22. Verkhovna Rada of Ukraine (2003). Tsyvilnyi kodeks Ukrainy: Zakon Ukrainy vid 16 sichnyia 2003 r. No 435-IV [Civil Code of Ukraine: Law of Ukraine of January 16, 2003 No. 435-IV]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/1618-15#Text> [in Ukrainian]
23. Proiekt zakonu pro vnesennia zmin do Kryminalnoho protsesualnoho kodeksu Ukrainy shchodo pidvyshchennia efektyvnosti borotby z kiberzlochynnistiu ta vykorystannia elektronnykh dokaziv vid 31 serpnia 2020 r. № 4004 [Draft Law on Amendments to the Criminal Procedure Code of Ukraine on Improving the Effectiveness of Combating Cybercrime and the Use of Electronic Evidence of 31 August 2020 No. 4004]. Retrieved from: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771 [in Ukrainian]
24. Verkhovna Rada of Ukraine (1992). Zakon Ukrainy “Pro informatsiiu” vid 2 zhovtnia 1992 r. № 2657-XII [Law of Ukraine “On Information” of 2 October 1992, No. 2657-XII]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> [in Ukrainian]
25. Konventsiia pro kiberzlochynnist vid 23 lystopada 2001 r. [Convention on Cybercrime of 23 November 2001]. Retrieved from: https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukrainian]
26. Stolitnii, A.V., & Kalancha, I.H. (2016). Formuvannia instytutu elektronnykh dokaziv u kryminalnomu protsesi Ukrainy [Formation of the Institute of Electronic Evidence in the Criminal Procedure of Ukraine]. *Problemy zakonnosti*, 146, 186–188 [in Ukrainian]
27. Bilousov, A.S. (2008). Kryminalistychnyi analiz ob’iektiv komp’iuternykh zlochyniv [Forensic analysis of objects of computer crimes]. *Extended abstract of candidate’s thesis*. Kyivskiy natsionalnyi universytet imeni Tarasa Shevchenka [in Ukrainian]
28. Kozytska, O.H. (2020). Shchodo poniattia elektronnykh dokaziv u kryminalnomu provadzhenni [On the concept of electronic evidence in criminal proceedings]. *Yurydychnyi naukovyi elektronnyi zhurnal*, 8, 418–421 [in Ukrainian]
29. Dehtiarova, O. (2021). Evidence in criminal proceedings on the basis of electronic evidence [Dokazuvannia u kryminalnomu provadzhenni na pidstavi elektronnykh dokaziv]. *Yurydychnyi visnyk*, 6, 273–278 [in Ukrainian]
30. Kovalenko, A.B. (2018). Elektronni dokazy v kryminalnomu provadzhenni: suchasnyi stan ta perspektyvy vykorystannia [Electronic Evidence in Criminal Proceedings: Current Status and Prospects for Use]. *Visnyk Luhanskoho derzhavnogo universytetu vnutrishnikh sprav imeni E.O. Didorenka*, 4, 237–245 [in Ukrainian]
31. Anhelenuk, A.-M.Yu. (2023). Vykorystannia elektronnykh dokaziv u kryminalnomu protsesualnomu pravi Ukrainy (problemni pytannia) [The Use of Electronic Evidence in the Criminal Procedure Law of Ukraine (Problematic Issues)]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriya PRAVO*, 79 (2), 214–218 [in Ukrainian]
32. Cherniavskiy, S.S., & Orlov, Yu.Yu. (2017). Elektronne vidobrazhennia yak dzherelo dokaziv u kryminalnomu provadzhenni [Electronic display as a source of evidence in criminal proceedings]. *Visnyk kryminalnoho sudochynstva*, 2, 112–124 [in Ukrainian]
33. International principles for computer evidence. Retrieved from: <https://www.thefreelibrary.com/International+principles+for+computer+evidence.-a0137863426> [in English]
34. Commonwealth Draft Model Law on Electronic Evidence. LMM(02)12. Retrieved from: https://www.oas.org/juridico/spanish/cyber/cyb4_evidence_law.pdf [in English]