

Олексій Гусєв

Київський національний університет імені Тараса Шевченка, Україна

ДОТРИМАННЯ ПОРЯДКУ ОДЕРЖАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ЯК УМОВА ЇХ ДОПУСТИМОСТІ У ЦИВІЛЬНОМУ ПРОЦЕСІ УКРАЇНИ

Oleksii Husiev

Taras Shevchenko National University of Kyiv, Ukraine

MAINTENANCE OF THE PROCEDURE FOR OBTAINING ELECTRONIC EVIDENCE AS THE CONDITION FOR ITS ADMISSIBILITY IN THE CIVIL PROCESS OF UKRAINE

The article observes the peculiarities of the electronic evidence obtaining an order in connection with the assessment of its admissibility. The concept of evidence obtaining is considered as the unity of four consecutive stages: the search for evidential data, its extraction, procedural implementation and submission to the court. The author substantiates the idea that the maintenance of special rules and requirements during each of the stages significantly affects the assessment of electronic evidence admissibility by the court. It is proved that the civil procedural legislation of Ukraine generally meets the leading world standards in matters of legal regulation of the procedure for obtaining electronic evidence, with the exception of some shortcomings. It is determined that in some cases overcoming of law deficiencies needs legislative intervention, other gaps can be eliminated by generalizing judicial practice, but some legislative provisions need to be detailed in the by-laws.

Keywords: civil procedure, admissibility of evidence, obtaining of evidence, electronic evidence.

Постановка проблеми. Поява в процесуальному законодавстві України поняття електронних доказів викликала жваву дискусію серед правників, одним із питань якої стала допустимість інформації в електронній формі, що визначає її здатність бути легальним засобом доказування в суді. У фаховій юридичній літературі висловлюються різноманітні думки з приводу умов допустимості електронних доказів, ключовим критерієм якої вважається достовірність.

Видається, що робота із забезпечення достовірності електронних доказів повинна починатися з моменту вилучення фактичних даних із джерела й тривати до їх остаточної оцінки судом. Таким чином, дотримання спеціального порядку збирання та подання до суду електронних доказів набуває актуальності у контексті питання про їх допустимість і прагнення до забезпечення в Україні справедливого судового розгляду для всіх заінтересованих осіб.

Аналіз останніх досліджень і публікацій. Проблематика допустимості електронних доказів у різних галузях процесуального права України, а також їх збирання та подання до суду в цілях доказування входила до сфери наукових інтересів багатьох учених, зокрема, Блажівської Н.Є., Грабовської О.О., Дрогозюк К.Б., Єсімова С.С., Каламайка А.Ю., Крицької І.О., Лазька О.М., Павлової Ю.С., Петренка В.С., Фурси С.Я., Цехана Д.М.

Метою статті є обґрунтування наявності взаємозв'язку між допустимістю електронних доказів та дотриманням певного порядку їх одержання шляхом розкриття деяких особливостей вилучення даних в електронно-цифровій формі, їх процесуального оформлення та передачі до суду з метою використання в цілях доказування у цивільному процесі.

Виклад основного матеріалу. Перш за все, слід з'ясувати суть термінів і понять, вжитих у цій роботі. В теорії цивільного процесу перший етап доказування часто називають «збиранням доказів». Учені тлумачать це поняття як вилучення доказових відомостей з місць їхнього знаходження з метою наступного подання

до суду¹. Такий підхід видається дещо неповним, й інші науковці стверджують, що більш прийнятним терміном для позначення цього етапу є «отримання доказів», під яким розуміють цілеспрямовану пізнавально-практичну діяльність суб'єктів доказування щодо пошуку, вилучення відомостей про факти та обставини справи, а також їх процесуального закріплення². Очевидно, що крім відшукування і безпосереднього вилучення фактичних даних, судово доказування також потребує їх процесуального оформлення, тобто надання одержаним відомостям передбаченої законом форми з метою наділення їх властивістю допустимості. Проте, зважаючи на те, що суд – обов'язковий суб'єкт доказування у цивільному процесі, який надає фактичним даним офіційну оцінку, видається, що поняття «одержання доказів» має глибший зміст³. Зокрема, воно охоплює не лише вилучення доказових відомостей із джерела та їх процесуальне оформлення, але й передачу отриманих даних до суду, оскільки кінцевим суб'єктом, який одержує фактичні дані для надання їм остаточної оцінки, є саме суд. Отже, вжите у цій роботі поняття «одержання доказів» слід розуміти як складне і таке, що включає в себе щонайменше чотири компоненти: пошук відомостей, які мають доказове значення, їх вилучення, процесуальне оформлення та подання до суду.

Суворе дотримання спеціального порядку одержання доказів, детальне законодавче регулювання процедури вилучення та процесуального оформлення фактичних даних, засоби, методи і тактика якої є предметом вивчення окремої прикладної науки – все це ознаки кримінального судочинства⁴. На відміну від кримінального процесу, де одержання доказів має неабияке значення, в науці цивільного процесу цьому приділяється значно менше уваги⁵. Порядок збирання відомостей доказового характеру в цивільному судочинстві, здебільшого, регламентується поверхнево, крім хіба що показань свідків і випадків забезпечення доказів. Таким чином, науковці справедливо зазначають, що збирання фактичних даних у цивільному процесі здійснюється учасниками справи чи не в будь-який спосіб, обраний ними самостійно⁶. Попри це, порядок одержання доказів суттєво впливає на їх допустимість. Розглянемо це більш детально по кожній складовій цього поняття.

Для початку слід визнати, що здатність суб'єкта судового процесу до точної ідентифікації відомостей, які мають доказове значення в конкретній справі, та їх відмежування від решти суттєво підвищує ймовірність визнання цих даних допустимими доказами в суді. Суть першого етапу одержання доказів полягає у пошуку та виявленні слідів минулої дії або події, що залишились на предметах матеріального світу⁷. Проте, шукаючи доказові відомості серед електронних даних, варто пам'ятати про деякі особливості.

Перш за все, для швидкого та ефективного виявлення розшукуваних даних серед значного обсягу електронних відомостей заінтересованій особі слід дотримуватись певного алгоритму. З метою полегшення та підвищення точності пошуку даних, які можуть мати доказове значення в суді, фахівці з США розробили спеціальний стандарт роботи з електронною інформацією – Довідкову модель електронного розкриття (англ. – *Electronic Discovery Reference Model*)⁸. Одна з її частин присвячена способам і методам точного та швидкого знаходження даних, необхідних для розгляду судової справи. Запропоновані алгоритми дій спрямовані на підвищення ефективності роботи зі значними масивами інформації в цифровій формі та пришвидшення ідентифікації

¹ Грабовська, О.О. (2016). *Доказування у цивільному процесі України: проблеми теорії і практики*: монографія. Київ: Юрінком Інтер, 372.

² Погорєцький, М.А. (2007). *Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі*: монографія. Харків: Арсіс, ЛТД, 506.

³ Дрогозюк, К.Б. (2018). *Предмет та суб'єкти доказування у цивільному процесі України та Франції*. Автореф дис. канд. юрид. наук. Одеса, 13.

⁴ Чупрікова, І.Л. (2016). *Допустимість доказів у світлі нового Кримінального процесуального кодексу*. Автореф. дис. канд. юрид. наук. Одеса, 12.

⁵ Малюга, Р.В. (2013). *Доказування в кримінальному процесі: проблеми визначення структурних елементів. Наукові записки Львівського університету бізнесу та права*, 11, 281-282.

⁶ Грабовська, О.О. (2016). *Доказування у цивільному процесі України: проблеми теорії і практики*: монографія. Київ: Юрінком Інтер, 372.

⁷ Погорєцький, М.А. (2007). *Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі*: монографія. Харків: Арсіс, ЛТД, 504-506.

⁸ EDRM Model, 2019. *ERDM*. <<https://www.edrm.net/frameworks-and-standards/edrm-model/>> (2019, квітень, 19).

необхідних даних. Серед питань, на які заінтересована особа повинна відповісти, ключовими є наступні: 1) які типи та види даних є належними й чи можна виключити з пошуку інші типи та види; 2) чи є належними резервні копії даних, відомості систем аварійного відновлення чи копіювання даних застарілого обладнання; 3) на яких типах носіїв зберігаються відповідні дані (як-от, змінних, незмінних, віддалених); 4) чи можливе існування інших джерел необхідних даних (наприклад, серверів електронної пошти, програм обміну миттєвими повідомленнями, портативних пристроїв працівників); 5) де фізично знаходяться технічні носії з даними та який порядок доступу до них¹. Хоча цей стандарт був розроблений насамперед для великих організацій зі складною внутрішньою структурою, більшість описаних в ньому ідей може бути використана будь-якою заінтересованою особою. На жаль, в Україні не розроблялись подібні стандарти чи моделі поведінки з електронною інформацією, тому для кращого розуміння питань, пов'язаних із пошуком доказових відомостей та необхідністю вжиття заходів забезпечення доказів, вітчизняним фахівцям було б корисно ознайомитися з положеннями цього стандарту чи його аналогів.

Далі, варто наголосити на необхідності розмежування цифрових даних і властивостей електронних носіїв, а також відокремлення різних даних, які зберігаються на одному технічному носіїві. Для досягнення цього важливим є максимально точне визначення складу предмета доказування у цивільній справі, щоб заінтересовані особи краще усвідомлювали, які саме доказові відомості їм потрібно зібрати². Сьогодні є очевидним, що у справах, в матеріалах яких є електронні докази, безпосереднє доказове значення мають лише їх цифрові дані. Проте історичний досвід показує, що доказами в різних країнах іноді вважали сукупність усіх електронних даних на одному носію чи єдність технічного носія зі збереженими на ньому даними як цілісну одиницю. Така практика була поширена, зокрема, в Англії, Австралії та Канаді до середини 2000-х років, коли вищі судові інстанції цих країн дійшли обґрунтованих висновків, що кожна частина інформації на жорсткому диску, компакт-диску або іншому носіїві повинна вважатись самостійним елементом, який може бути окремим доказом³. Наріжним каменем, що змінив вектор судової практики, виявилось питання допустимості доказів. Коротко пояснюючи, матеріальний носій не завжди має доказове значення у справі, а самі цифрові дані, як правило, мають складну внутрішню структуру: на одному носію може зберігатись безліч даних різного характеру, одні з яких можуть бути, наприклад, неналежними, а інші – недопустимими.

Щодо недопустимих даних, то на електронних носіях, які в США подавали до суду, часто містились відомості з обмеженим доступом, наприклад, персональні дані, комерційні таємниці, особисті листи та інші види кореспонденції, записи телефонних розмов та інше. Оцінюючи такі докази як єдність усіх даних на одному носію суди визнавали їх недопустимими, оскільки деякі дані не могли бути вилучені та передані до суду без спеціального дозволу, якого в заінтересованих осіб не було⁴. Це породжувало численні конфлікти під час розгляду цивільних справ, вирішити які вдалося лише після зміни підходу до формування предмета доказування та посилення вимог щодо точності пошуку та виявлення доказових відомостей. Таким чином, судовою практикою дійшла висновку, що поняття електронних доказів загалом не може охоплювати собою сукупність різних даних, які зберігаються на одному матеріальному носіїві.

Щодо неналежних відомостей слід зазначити, що під час дослідження доказів часто виникало питання, чи можна вважати сукупність усіх фактичних даних в електронній формі допустимими в цілому як єдиний доказ, якщо частина з цих відомостей не стосується обставин справи? Формальна логіка, на законах якої побудована юридична наука, дає негативну відповідь на це питання, оскільки не можна зробити істинний висновок про ціле на підставі знання про його частину⁵. Умовиводи, зроблені в такий спосіб, не мають того ж ступеня достовірності, що й вихідні

¹ EDRM Identification Guide, 2010. *ERDM*. <<https://www.edrm.net/frameworks-and-standards/edrm-model/identification/>> (2019, квітень, 19).

² Грабовська, О.О. (2016). *Доказування у цивільному процесі України: проблеми теорії і практики*: монографія. Київ: Юрінком Інтер, 304-307.

³ Stanfield, A. (2016). *The Authentication of Electronic Evidence. PhD thesis*. Brisbane, 98-103.

⁴ Decision in the case 'Sony Music Entertainment (Australia) Limited v University of Tasmania' [2003]. *The Federal Court of Australia*. <<https://jade.io/article/107130>> (2019, квітень, 19).

⁵ Конверський, А.Є. (2008). *Логіка (традиційна та сучасна)*: підручник для студентів вищих навчальних закладів. Київ: Центр учбової літератури, 269.

твердження, тому в процесі пізнання індукція має завжди поєднуватися з дедукцією¹. Це означає, що якщо хоча б частина з даних, збережених на електронному носію, не має зв'язку з предметом доказування, то єдність усіх цих даних як один, цілісний доказ не може вважатись належною, а відтак і допустимою, оскільки в англо-американській правовій системі неналежні відомості апріорі не можуть стати допустимими доказами.

В Україні частина перша статті 100 Цивільного процесуального кодексу вказує, що «електронними доказами є інформація ...», проте наступне речення цієї ж частини зазначає: «Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, в інших місцях збереження даних в електронній формі»². Видається, що таке формулювання може призвести до заплутування, й існує високий ризик того, що внаслідок недостатності спеціальних знань про середовище існування електронно-цифрових даних у читача сформується хибне уявлення про те, що електронний доказ – це нерозривна єдність електронної інформації та її носія. На жаль, вітчизняні правники іноді наділяють доказовим значенням сукупність електронних носіїв і збережених на них відомостей³. Але, на щастя, останні юридичні дослідження обґрунтовано доводять, що електронна інформація та її носії – це самостійні види доказів⁴.

З огляду на попередні висновки, стає зрозумілим, що поняття електронних доказів не стосується властивостей електронних носіїв, оскільки електронно-цифрові дані за своєю природою – не атрибути певних речей, не фізичні характеристики технічного носія, а самостійний матеріальний об'єкт, визнаний законом і наділений власним процесуально-правовим статусом. Іншими словами, електронні докази – це лише дані, що мають електронно-цифрову форму, і більше нічого. Для прикладу, спроможність відновити видалені з електронного носія дані характеризує його технічні властивості. В такому разі об'єктом дослідження буде сам носій як речовий доказ. Але у випадку успішного відновлення втрачених відомостей одержані дані, які стосуються фактів чи обставин справи, вважатимуться електронними доказами.

Таким чином, ефективний пошук і точна ідентифікація відомостей, які мають доказове значення у конкретній справі, істотно впливають на оцінку їх допустимості як судових доказів, а вичерпність і повнота одержаних даних можуть позначитись на справедливості судового розгляду та обґрунтованості судового рішення. Тому заінтересованим особам слід відповідально підійти до пошуку та виявлення електронної інформації в цілях доказування.

Повертаючись до порядку одержання доказів, наступним його етапом є вилучення відомостей, які можуть мати доказове значення. Необхідність дотримання спеціальних правил вилучення фактичних даних загалом виходить із законодавчої заборони суду брати до уваги докази, одержані з порушенням порядку, встановленого законом⁵. Не вдаючись у дискусію з приводу змісту терміну «одержані», варто зазначити, що це обмеження слугує гарантією законності доступу до джерела відомостей, а також відсутності порушень прав і свобод усіх заінтересованих осіб. Для прикладу, оприлюднення в судовому засіданні звукозапису діалогу, зробленого без згоди одного з учасників, майже в будь-якій країні світу вважатиметься порушенням конституційних або цивільних прав і неминуче призведе до визнання таких даних недопустимими. Дотримання цієї заборони під час збирання електронних доказів, крім указанного, слугує також запорукою повноти та достовірності зібраних даних, запобіжником проти можливих втручань і несанкціонованих змін. Коротко кажучи, якщо електронні докази зібрані абияк, це може мати негативний вплив на їх достовірність, а відтак і допустимість.

Найсучаснішими досягненнями у питаннях вилучення цифрових даних можуть похизуватись фахівці з США. Вже згаданий раніше стандарт роботи з електронними доказами, EDRM, описує

¹ Шинкарук, В.І. та ін. (ред.). (2002). *Філософський енциклопедичний словник*. Київ: Абрис, 241.

² *Цивільний процесуальний кодекс України 2004* (Верховна Рада України). *Відомості Верховної Ради України*, 40, 492.

³ Алексеева-Процик, Д.О., Брисковська, О.М. (2018). Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*, 2, 249.

⁴ Каламайко, А.Ю. (2016). *Електронні засоби доказування в цивільному процесі*: Автореф. дис. канд. юрид. наук. Харків.

⁵ *Цивільний процесуальний кодекс України, ст. 78. 2004* (Верховна Рада України). *Відомості Верховної Ради України*, 40, 492.

цілу низку сучасних способів вилучення електронної інформації та її оформлення¹. Серед новітніх методів узагальнено можна назвати такі: створення криміналістичного образу (англ. – *forensic image*), створення вибіркового образу (англ. – *targeted image*), несудове копіювання (англ. – *non-forensic copy*), вилучення даних шляхом віддаленого доступу (англ. – *non-email exports*) та вилучення даних, переданих електронною поштою (англ. – *email harvesting*). Хоча більшість методів призначені для застосування в кримінальному судочинстві, вони можуть також легко використовуватись у цивільних справах. Тому науковцям, а також іншим заінтересованим особам слід звернути увагу на передовий іноземний досвід використання різних технік для фактичного вилучення цифрових даних з електронних сховищ пам'яті для потреб доказування.

В Україні чинне цивільне процесуальне законодавство, як і в більшості іноземних держав, не регламентує безпосередній порядок збирання електронних доказів. Вітчизняний Цивільний процесуальний кодекс містить лише декілька положень, присвячених фіксації цифрових даних, зокрема про огляд електронних доказів судом за їх місцем знаходженням. Ані конкретних способів вилучення даних, ані засобів фіксації чи збереження цілісності, ані загальних вимог до них у Законі не передбачено.

Загалом спеціальні способи, засоби, методи та прийоми вилучення чи копіювання цифрових даних у цілях доказування детально вивчаються в межах прикладних юридичних і технічних наук². Зважаючи на те, що відповідні знання часто мають спеціальний характер, вести далі мову про способи вилучення електронної інформації як елемент її одержання в цілях доказування видається недоцільним і пропонується зосередити увагу на інших юридично значущих аспектах збирання електронних доказів.

Складовою процесу одержання доказів є також їх процесуальне оформлення. Воно передбачає надання одержаним фактичним даним процесуальної форми доказів. Процесуальною формою доказів у доктрині називають порядок фіксації даних на технічних носіях, що забезпечує можливість перевірки процесу їх одержання та який наділяє зібрані фактичні дані властивістю допустимості³. Такий підхід можна назвати «широким», адже він першочергово включає вилучення доказових відомостей, а вже потім надання їм визначеної форми. На противагу цьому підходу, більш поширеному в науці кримінального процесу, в теорії цивільного процесу домінує «вузьке» розуміння, згідно з яким поняття процесуальної форми доказів позначає лише порядок оформлення конкретного засобу доказування⁴. Попри спрощеність такого розуміння процесуальної форми доказів, юридичне оформлення фактичних даних все одно відіграє важливу роль для оцінки допустимості доказів.

Подібно до порядку вилучення фактичних даних, необхідність виконання спеціальних вимог щодо процесуального оформлення будь-яких засобів доказування виникає з заборони брати до уваги докази, одержані з порушенням порядку, встановленого законом⁵. Це означає, що такі правила забезпечують можливість передачі зібраних даних у часі та просторі в незмінному вигляді. Для електронних доказів додержання спеціальних вимог щодо їх оформлення є не лише гарантією законності, але й додатковим підтвердженням достовірності цифрових даних, яка, до речі, є ключовим елементом допустимості цього виду доказів. Отже, якщо електронні докази оформлені з порушенням порядку, встановленого законом, вони з високим ступенем вірогідності будуть визнані судом недопустимими.

У зв'язку з тим, що процесуальна форма доказів має неабияке значення для їх допустимості, більшість юрисдикцій світу приділяють значну увагу її правовій регламентації. Так, у Німеччині федеральний уряд та уряди окремих земель уповноважені встановлювати відповідно до своєї

¹ EDRM Collection Standards, 2014. *EDRM*. <<https://www.edrm.net/frameworks-and-standards/edrm-model/edrm-stages-standards/edrm-collection-standards/>> (2019, квітень, 19).

² Білоусов, А.С. (2008). *Криміналістичний аналіз об'єктів комп'ютерних злочинів*: Автореф. дис. канд. юрид. наук. Київ.

³ Погорєцький, М.А. (2007). *Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі*: монографія. Харків: Арсіс, ЛТД, 489.

⁴ Штефан, А. (2016). Допустимість доказів у цивільному судочинстві. *Теорія і практика інтелектуальної власності*, 2 (88), 70-71.

⁵ Цивільний процесуальний кодекс України, ст. 78. 2004 (Верховна Рада України). *Відомості Верховної Ради України*, 40, 492.

компетенції вимоги до форми електронних документів як доказів з метою забезпечення їх придатності для обробки в суді¹. В Канаді заінтересованим особам надано повну свободу вибору способів оформлення електронних доказів. Національний Закон про докази дозволяє подавати до суду електронні документи як докази відповідно до будь-яких стандартів, процедур, практик або способів застосування щодо їх створення чи зберігання з урахуванням організаційно-правової форми особи власника, виду його діяльності, витрачених на створення, збереження чи застосування електронних документів зусиль, а також характеру та призначення самих документів².

Вітчизняний Цивільний процесуальний кодекс містить незначну кількість положень, присвячених процесуальній формі електронних доказів, як-от щодо протоколювання цифрових даних, зібраних під час огляду доказів за їх місцезнаходженням. Окрім цього, відповідні правила можна знайти у статті 43 Кодексу, згідно з якою документи, що подаються до суду в електронній формі, повинні бути скріплені електронним цифровим підписом, та статті 100, яка вимагає подання електронних доказів лише в оригіналі чи копіях, посвідчених в установленому законом порядку³.

Проте в цілому протягом останніх років кількість легальних інструментів фіксації цифрових даних зросла. Зокрема, положення Закону України «Про електронну комерцію» 2015 року встановлюють вимоги до форми електронних договорів і комерційних повідомлень, які можуть бути доказами в суді⁴. А в 2018 році набрав чинності Закон України «Про електронні довірчі послуги», яким було врегульовано відносини щодо автентифікації веб-сайтів, застосування електронних цифрових підписів і печаток, формування електронної позначки часу та використання реєстрованої електронної доставки⁵. Більшість з цих послуг стосується оформлення цифрових даних, але вони одночасно є законними засобами фіксації електронної інформації в цілях судочинства. Крім цього, Державна судова адміністрація України веде активну роботу з розробки положення про Єдину судову інформаційно-телекомунікаційну систему⁶. Норми цього положення повинні хоча б частково врегулювати порядок подання до суду електронних доказів, що опосередковано визначатиме способи та засоби їх збирання. В цілому ж підзаконні нормативно-правові акти містять обмаль нормативного матеріалу, присвяченого формі електронних доказів: ані форматів електронних документів, ані вимог до їх реквізитів, ані засобів збереження цілісності даних у них не визначено.

Передача електронних даних до суду з метою визнання їх допустимими доказами також вимагає дотримання спеціальних правил їх подання, що повинні враховувати технічні особливості інформації в електронно-цифровій формі та її технічних носіїв. Очевидно, що одразу після фіксації доказових відомостей заінтересована особа повинна передати їх до суду. При цьому надзвичайно важливо забезпечити їх цілісність і недоторканність, чого можна досягти лише дотримуючись особливого режиму. Таким чином, спеціальний порядок подання електронних доказів є ще однією умовою їх достовірності та допустимості.

Сучасні правила подання доказів, які стосуються електронних засобів доказування, не завжди визнають і враховують унікальні характеристики цифрових даних та їх електронних носіїв, тому способи передачі електронної інформації до суду часто мають риси паперового документообігу. До прикладу, в окремих юрисдикціях законодавство не регламентує жодного спеціального способу подання електронних доказів, залишаючи це питання на розсуд заінтересованої особи, але обмежує свободу вибору вимогами про необхідність забезпечення умов для збереження автентичності даних та ідентифікації автора. Зокрема, стаття 336 Кодексу цивільного судочинства Естонії вказує, що процесуальні та інші документи в електронному вигляді повинні бути подані до суду в безпечний

¹ The Code of Civil Procedure 2005. *Bundesministerium der Justiz und für Verbraucherschutz*. <https://www.gesetze-im-internet.de/englisch_zpo/englisch_zpo.html> (2019, квітень, 19).

² The Canada Evidence Act 1985. *Justice Laws Website*. <<http://laws.justice.gc.ca/eng/acts/C-5/>> (2019, квітень, 19).

³ Цивільний процесуальний кодекс України 2004 (Верховна Рада України). *Відомості Верховної Ради України*, 40, 492.

⁴ Закон про електронну комерцію 2015 (Верховна Рада України). *Офіційний веб-сайт Верховної Ради України*. <<https://zakon.rada.gov.ua/laws/show/675-19/print>> (2019, квітень, 19).

⁵ Закон про електронні довірчі послуги 2017 (Верховна Рада України). *Відомості Верховної Ради України*, 45, 400.

⁶ ДСА України оголосила про створення та функціонування Єдиної судової інформаційно-телекомунікаційної системи 2018. *Державна судова адміністрація України*. <<https://dsa.court.gov.ua/dsa/pres-centr/news/611253/>> (2019, квітень, 21).

спосіб, який дозволяє ідентифікувати відправника документа, а спеціальний порядок подання електронних документів та вимоги до їх оформлення можуть встановлюватись уповноваженим міністерством¹.

У деяких державах законодавство взагалі не містить положень про порядок подання електронних доказів до суду, а піклування про їх достовірність цілком покладено на заінтересованих осіб. Так, згідно зі статтею 34 Федеральних правил цивільного судочинства США електронна інформація за загальним правилом подається до суду у вигляді, придатному для використання в суді, якщо протилежна сторона не вимагає іншого. При цьому володілець не зобов'язаний подавати одну й ту ж електронну інформацію понад один раз². Видається, що за такого підходу оригінальність і недоторканність цифрових даних залежать від умінь заінтересованої особи чи її представника сформулювати вимоги до володільца інформації щодо її належного оформлення та порядку передачі до суду.

Бувають випадки, коли законодавством визначено лише один спосіб передачі електронних доказів до суду. Зокрема, згідно зі статтею 181С Кодексу організації та цивільного судочинства Мальти подання документів в електронній формі здійснюється за допомогою електронної пошти, а реєстратор, який одержав електронного листа, зобов'язаний повідомити про це відправника шляхом надсилання зворотного повідомлення³. Такий порядок подання електронних доказів нагадує надсилання письмових документів рекомендованими листами з повідомленням про вручення. Достовірність електронних даних тут забезпечується лише фіксацією факту їх отримання безвідносно до цілісності змісту, хоча закон не забороняє вимагати інших, допоміжних гарантій збереження автентичності, наприклад, застосування електронних цифрових підписів або печаток.

Специфічний порядок подання електронних доказів до суду передбачено законодавством Японії. Відповідно до статті 132-10 національного Кодексу цивільного судочинства заява чи інший документ, пов'язаний із провадженням у цивільній справі, може бути складений і поданий до суду з використанням спеціальної електронної системи обробки даних. Це система, що з'єднує комп'ютер (включно з усіма входними та вихідними пристроями), який використовується судом, із комп'ютером, який використовуються особою, яка подає заяву чи інший документ, через лінії телекомунікацій. Заява чи інший документ вважаються такими, що надійшли до суду, з моменту, коли їх зберегли на комп'ютері, який використовується судом⁴. Описане є прикладом запровадження автоматизованої інформаційно-телекомунікаційної системи органів судової влади для обміну документами та іншими даними в електронній формі між судом та учасниками справи. Але такий порядок подання електронних доказів є ефективним, якщо рівень інформатизації суспільства і матеріально-технічне забезпечення органів судової влади дозволяють це зробити.

Аналіз положень чинної редакції ЦПК України показує, що в регламентації порядку подання електронних доказів вітчизняне законодавство загалом не поступається найбільш сучасним іноземним зразкам, а заінтересовані особи забезпечені чи не всіма нині можливими способами подання цифрових даних до суду. Відповідно до статті 83 ЦПК докази подаються безпосередньо до суду⁵. Зробити це можна чотирма способами, прямо визначеними процесуальним законом: 1) подати разом із позовною заявою, відзивом або письмовими поясненнями; 2) передати через канцелярію суду; 3) надіслати з використанням Єдиної судової інформаційно-телекомунікаційної системи, або 4) в судовому засіданні з клопотанням про їх приєднання до матеріалів справи. Стаття 100 ЦПК встановлює вимоги до форми, в якій електронні докази можуть бути подані

¹ *The Code of Civil Procedure 2005. Riigi Teataja*. <<https://www.riigiteataja.ee/en/eli/513122013001/consolide>> (2019, квітень, 21).

² *The Federal Rules of Civil Procedure 2018. The Administrative Office of the U.S. Courts*. <https://www.uscourts.gov/sites/default/files/cv_rules_eff_dec_1_2018_0.pdf> (2019, квітень, 21).

³ *The Code of Organization and Civil Procedure 1855. The Ministry for Justice, Culture and Local Government*. <<http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8577&l=1>> (2019, квітень, 21).

⁴ *The Code of Civil Procedure 1996. Japanese Law Translation Database System*.

<<http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=2&x=61&y=12&co=1&ia=03&yo=&gn=&sy=&ht=&no=&bu=&ta=&al%5B%5D=C&ky=code+of+civil+procedure&page=32&id=2834&lvm=02&vm=02>> (2019, квітень, 21).

⁵ *Цивільний процесуальний кодекс України 2004* (Верховна Рада України). *Відомості Верховної Ради України*, 40, 492.

до суду¹. Таким чином, процесуальне законодавство України передбачає можливості подання електронних даних як разом із матеріальним носієм, так і шляхом їх надсилання каналами електрозв'язку. Таке розмаїття способів подання електронних доказів видається цілком прогресивним і відповідає сьогоdnішньому перехідному етапу розвитку вітчизняного судочинства, коли електронні інформаційні технології тільки починають поширюватись. Але підзаконне регулювання потребує деталізації. Зокрема, слід унормувати питання фіксації моментів надсилання та одержання судом інформації в електронній формі, конкретизувати способи і засоби збереження цілісності отриманих даних, а також розробити детальну процедуру обробки даних після їх одержання працівниками суду.

Висновки. Розглянуті вище особливості одержання електронних доказів можуть мати суттєвий вплив на їх оцінку в суді. Так, пошук та виокремлення фактичних даних, які мають значення для розгляду та вирішення конкретної справи, є вагомою запорукою допустимості електронних доказів. До складу цього поняття не варто включати електронні носії цифрових даних, оскільки їх слід кваліфікувати як речові докази, а також усю сукупність електронної інформації, збереженої на одному носію, через високий ризик визнання такого комплексного доказу неналежним або недопустимим у цілому. Будь-яке намагання вмістити в одному доказі фактичні дані з кількох різних джерел є також неприпустимим, оскільки це є одночасним порушенням норм права і законів логіки. Недотримання цих правил може тягнути за собою порушення принципу законності, що є безсумнівною підставою для визнання одержаних доказів недопустимими. Заінтересовані особи повинні якомога швидше, точніше і в повному обсязі знаходити ті фактичні дані, які підтверджують їх вимоги чи заперечення, для чого в пригоді їм можуть стати різноманітні стандарти та алгоритми роботи з електронною інформацією.

Безпосереднє вилучення фактичних даних має здійснюватись у межах спеціальних процедур, що гарантують точність і повноту зібраної інформації. Одержані відомості повинні набувати допустимої процесуальної форми, здатної забезпечити їх цілісність і недоторканність від будь-яких посягань. Передача ж фактичних даних до суду має відбуватись у спосіб, що дозволяє запобігти несанкціонованому доступу до них і розголошенню конфіденційної інформації. Таким чином, дотримання спеціальних вимог щодо одержання електронних доказів можна вважати умовами їх допустимості, які слід брати до уваги як у процесі правозастосування, так і в нормотворчій діяльності.

Цивільне процесуальне законодавство України в цілому відповідає провідним світовим зразкам у питаннях правового регулювання порядку одержання електронних доказів. За винятком деяких недоліків регламентації вимог до процесуальної форми електронних доказів, ЦПК України на достатньому рівні забезпечує всіх учасників цивільного процесу ефективними інструментами оперування електронною інформацією в цілях доказування. Хоча деякі прогалини потребують втручання законодавця, інші можуть бути усунені шляхом узагальнення судової практики. Крім того, окремі законодавчі положення потребують деталізації у підзаконних актах для забезпечення повноцінного функціонування новел процесуального законодавства.

References:

1. Hrabovska, O.O. (2016). *Dokazuvannia u tsyvilnomu protsesi Ukrainy: problemy teorii i praktyky*: monohrafiia [Evidence in the Civil Process of Ukraine: Problems of Theory and Practice: Monograph]. Kyiv: Yurinkom Inter [in Ukrainian].
2. Pohoretskyi, M.A. (2007). *Funktsionalne pryznachennia operatyvno-rozshukovoi diialnosti u kryminalnomu protsesi*: Monohrafiia [The Functional Purpose of Operational-Search Activity in Criminal Proceedings: Monograph]. Kharkiv: Arsis, LTD [in Ukrainian].
3. Drohoziuk, K.B. (2018). *Predmet ta subiekty dokazuvannia u tsyvilnomu protsesi Ukrainy ta Frantsii* [The Subject and Subjects of Proving in the Civil Process of Ukraine and France]. Avtoreferat dysertatsii. Odesa [in Ukrainian].
4. Chuprikova, I.L. (2016). *Dopustymist dokaziv u svitli novoho Kryminalnoho protsesualnoho kodeksu* [Admissibility of Evidence in the Light of the New Criminal Procedural Code]. Avtoreferat dysertatsii. Odesa [in Ukrainian].
5. Maliuha, R.V. (2013). *Dokazuvannia v kryminalnomu protsesi: problemy vyznachennia strukturnykh elementiv* [Evidence in Criminal Process: the Problems of Determining the Structural Elements]. *Naukovi zapysky Lvivskoho*

¹ Цивільний процесуальний кодекс України 2004 (Верховна Рада України). *Відомості Верховної Ради України*, 40, 492.

- universytetu biznesu ta prava* [Scientific Notes of the Lviv University of Business and Law], no. 11, 280-283. [in Ukrainian].
6. *Tsyvilnyi protsesualnyi kodeks Ukrainy* 2004 (The Verkhovna Rada of Ukraine). [Civil Procedure Code of Ukraine, 2004 (Verkhovna Rada of Ukraine)]. *Vidomosti Verkhovnoyi Rady Ukrayiny* [Bulletin of the Verkhovna Rada of Ukraine], no. 40, 492 [in Ukrainian].
 7. EDRM Collection Standards, 2014. *EDRM*. <<https://www.edrm.net/frameworks-and-standards/edrm-model/edrm-stages-standards/edrm-collection-standards/>> [in English]. (2019, April, 19).
 8. Bilousov, A.S. (2008). *Kryminalistychnyi analiz ob'ektiv kompiuternykh zlochyniv* [Forensic Analysis of the Computer Crime Objects]. *Avtoreferat dysertatsii*. Kyiv [in Ukrainian].
 9. Shtefan, A. (2016). *Dopustymist dokaziv u tsyvilnomu sudochynstvi* [Admissibility of Evidence in Civil Procedure]. *Teoriia i praktyka intelektualnoi vlasnosti* [Theory and Practice of Intellectual Property], no.2 (88), 69-77 [in Ukrainian].
 10. The Code of Civil Procedure 2005. *Bundesministerium der Justiz und für Verbraucherschutz* [The Federal Ministry of Justice and Consumer Protection]. <https://www.gesetze-im-internet.de/englisch_zpo/englisch_zpo.html> [in English]. (2019, April, 19).
 11. The Canada Evidence Act 1985. *Justice Laws Website*. <<http://laws.justice.gc.ca/eng/acts/C-5/>> [in English]. (2019, April, 19).
 12. *Zakon pro elektronnu komertsiiu* 2015 (Verkhovna Rada Ukrainy). [E-Commerce Law, 2015 (Verkhovna Rada of Ukraine)]. *Ofitsiinyi veb-sait Verkhovnoi Rady Ukrainy*. [The official website of the Verkhovna Rada of Ukraine]. <<https://zakon.rada.gov.ua/laws/show/675-19/print>> [in Ukrainian]. (2019, April, 19).
 13. The Code of Civil Procedure 2005. *Riigi Teataja* [State Gazette]. <<https://www.riigiteataja.ee/en/eli/513122013001/consolide>> [in English]. (2019, April, 21).
 14. The Federal Rules of Civil Procedure 2018. *The Administrative Office of the U.S. Courts*. <https://www.uscourts.gov/sites/default/files/cv_rules_eff_dec_1_2018_0.pdf> [in English]. (2019, April, 21).
 15. The Code of Organization and Civil Procedure 1855. *The Ministry for Justice, Culture and Local Government*. <<http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8577&l=1>> [in English]. (2019, April, 21).
 16. The Code of Civil Procedure 1996. *Japanese Law Translation Database System*. <<http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=2&x=61&y=12&co=1&ia=03&yo=&gn=&sy=&ht=&no=&bu=&ta=&al%5B%5D=C&ky=code+of+civil+procedure&page=32&id=2834&lv=02&vm=02>> [in English]. (2019, April, 21).
 17. *Zakon pro elektronni doverchi posluhy* 2017 (Verkhovna Rada Ukrainy). [Electronic Trust Services Act 2017 (Verkhovna Rada of Ukraine)]. *Vidomosti Verkhovnoi Rady Ukrainy* [Bulletin of the Verkhovna Rada of Ukraine], no. 45, 400 [in Ukrainian].
 18. DSA Ukrainy oholosyla pro stvorennia ta funktsionuvannia Yedynoi sudovoi informatsiino-telekomunikatsiinoi systemy 2018. [SJA of Ukraine Announced the Creation and Operation of a the United Judicial Information and Telecommunication System]. *Derzhavna sudova administratsiia Ukrainy* [State Judicial Administration of Ukraine]. <<https://dsa.court.gov.ua/dsa/pres-centr/news/611253/>> [in Ukrainian]. (2019, April, 21).
 19. EDRM Model, 2019. *EDRM*. <<https://www.edrm.net/frameworks-and-standards/edrm-model/>> [in English]. (2019, April, 19).
 20. EDRM Identification Guide, 2010. *EDRM*. <<https://www.edrm.net/frameworks-and-standards/edrm-model/identification/>> [in English]. (2019, April, 19).
 21. Stanfield, A. (2016). *The Authentication of Electronic Evidence*. *PhD thesis*. Brisbane [in English].
 22. Decision in the case 'Sony Music Entertainment (Australia) Limited v University of Tasmania' [2003] of the Federal Court of Australia. <<https://jade.io/article/107130>> [in English]. (2019, April, 21).
 23. Konverskyi, A.Ye. (2008). *Lohika (tradytsiina ta suchasna): Pidruchnyk dlia studentiv vyshchykh navchalnykh zakladiv* [Logics (Traditional and Modern): a Textbook for Students of Higher Educational Institutions]. Kyiv: Tsentru uchbovoi literatury [in Ukrainian].
 24. Shynkaruk, V.I. ta in. (Eds.). (2002). *Filosofskyi entsyklopedychnyi slovnyk* [Philosophical Encyclopedic Dictionary]. Kyiv: Abrys [in Ukrainian].
 25. Aleksieieva-Protsyk, D.O., Bryskovska, O.M. (2018) *Elektronni dokazy v kryminalnomu sudochynstvi: poniattia, oznaky ta problemni aspekty zastosuvannia* [Electronic Evidence in Criminal Procedure: the Concept, Features and Problem Aspects of Application]. *Naukovyi visnyk publichnoho ta pryvatnoho prava* [Scientific Bulletin of Public and Private Law], no. 2, 247-253 [in Ukrainian].
 26. Kalamaiko, A.Yu. (2016). *Elektronni zasoby dokazuvannia v tsyvilnomu protsesi* [Electronic Means of Proof in Civil Process]. *Avtoreferat dysertatsii*. Kharkiv [in Ukrainian].