DOI https://doi.org/10.18524/2411-2054.2025.60.348090
УДК 343.14

Б. М. Орловський, доктор юридичних наук, доцент, професор
Одеський національний університет імені І. І. Мечникова
Кафедра кримінального права, кримінального процесу та криміналістики
Французький бульвар, 24/26, Одеса, 65058, Україна
e-mail: b.orlovskyi@onu.edu.ua
ORCID iD: https://orcid.org/0000-0002-9161-2904

КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНІ АСПЕКТИ ВИКОРИСТАННЯ ЦИФРОВИХ ДОКАЗІВ ТА ЕЛЕКТРОННИХ НОСІЇВ ІНФОРМАЦІЇ

Статтю присвячено комплексному аналізу кримінально-процесуальних аспектів використання цифрових (електронних) доказів та електронних носіїв інформації у кримінальному провадженні, що є актуальною темою в умовах стрімкого розвитку цифрових технологій і проникнення їх у всі сфери життєдіяльності суспільства. Сучасне кримінальне правопорушення майже завжди залишає свій цифровий слід у вигляді даних мобільних пристроїв, інформації із хмарних сховищ, IP-адрес під час інтернет-комунікацій чи активності в соціальних мережах, які об'єднуються єдиним поняттям цифрових доказів (електронної інформації) та мають важливе значення в процесі доказування. Дослідження розглядає недостатню адаптацію чинних норм Кримінального процесуального кодексу (далі — КПК) України, що створює системні перешкоди для забезпечення законності, достовірності та допустимості отриманої електронної інформації.

Автором здійснено теоретичний аналіз правової природи цифрових (електронних) доказів та встановлено їхню гібридну процесуальну природу, яка поєднує ознаки як документа, так і речового доказу, що ускладнює єдине правозастосування. Для подолання цієї колізії запропоновано власні науково обґрунтовані дефініції, які доцільно додати до КПК України.

Зокрема, пропонується сформулювати поняття «цифровий (електронний) доказ» у статті 99 КПК як «фактичні дані про обставини, що підлягають доказуванню у кримінальному провадженні, створені, передані, збережені або витягнуті у формі, придатній для сприйняття й обробки комп'ютерною системою, незалежно від їхнього фізичного місця розташування за умови дотримання процедури їхньої цілісності та автентичності». Фізичне місце розташування таких доказів може охоплювати електронні носії, комп'ютерні мережі, хмарні сховища або інформаційно-телекомунікаційні системи.

Також для уникнення плутанини запропоновано визначити поняття «електронний носій інформації» як «матеріальний об'єкт (пристрій, апаратний чи програмно-апаратний комплекс), призначений для створення, збирання, зберігання, обробки, відтворення чи передачі цифрових (електронних) доказів, що може бути вилучений як речовий доказ у кримінальному провадженні».

Особливу увагу приділено практичним проблемам, що виникають на етапах отримання, фіксації та зберігання цифрових доказів у разі проведення обшуку та тимчасового доступу, особливо щодо даних, вилучених із мобільних пристроїв, соціальних мереж і хмарних сховищ, де інформація є найбільш вразливою. Обґрунтовано, що для забезпечення допустимості цифрових доказів необхідна законодавча вимога про обов'язкове застосування криптографічних методів захисту на стадії їх фіксації.

Це забезпечить їхню автентичність і має бути відображено в протоколах слідчих дій та ухвалах слідчого судді.

Звернено увагу на критичну важливість дотримання ланцюга недоторканності, оскільки цифровий доказ потребує забезпечення недоторканності (цілісності) самої інформації, а не лише фізичного носія. Запропоновано законодавчо закріпити вимогу про створення захищених цифрових депозитаріїв або спеціальних електронних сховищ в органах досудового розслідування для належного зберігання великих обсягів даних, отриманих за ухвалами слідчих суддів.

Наголошується на важливості дотримання автентичності цифрового (електронного) доказу для забезпечення реалізації його належності та допустимості під час долучення до матеріалів кримінального провадження. У висновку підкреслено, що адаптація процесуальних норм до цифрових реалій є критично необхідною умовою для створення єдиного понятійного апарату і процесуальних стандартів, що забезпечить законність, справедливість та ефективність сучасного кримінального провадження.

Ключові слова: цифровий доказ, електронний доказ, електронний носій інформації, допустимість доказів, належність доказів, автентичність доказів, фіксація доказів, тимчасовий доступ.

Постановка проблеми. Стрімкий розвиток цифрових технологій і проникнення їх у всі сфери життєдіяльності суспільства радикально трансформували як способи вчинення кримінальних правопорушень, так і методи їхнього розкриття та розслідування. Сучасне кримінальне правопорушення, незалежно від його виду (від кіберзлочинів до традиційних злочинів), майже завжди залишає свій цифровий слід у вигляді даних мобільних пристроїв, інформації із хмарних сховищ, IP-адрес під час інтернет-комунікацій чи активності в соціальних мережах. Ці дані об'єднуються єдиним поняттям цифрових доказів (електронної інформації) та мають важливе значення у процесі доказування, оскільки часто є ключовими й важливими джерелами для виявлення особи, що скоїла кримінальне правопорушення, та встановлення істини в кримінальному провадженні.

Актуальність дослідження цифрових (електронних) доказів і процесуальних аспектів їх використання обумовлена значним розривом між динамікою технологічного прогресу та статичністю кримінально-процесуального законодавства, яке повільно видозмінюється в наш час. Чинний Кримінальний процесуальний кодекс України (далі – КПК України) було прийнято до масового використання цифрових технологій, він містить лише загальні норми про описання доказів, які недостатньо деталізують характеристику цифрових доказів та електронних носіїв інформації, а також порядок їх отримання, фіксації, зберігання й допустимості. Це створює певні практичні проблеми для органів досудового розслідування та суду, пов'язані із складнощами належного опису, вилучення і зберігання цифрових доказів та електронних носіїв, отриманих під час обшуку, огляду або інших слідчих дій, а також визнання інформації, що розміщена на цих носіях належним і допустимим доказом у кримінальному провадженні. Тому дослідження кримінально-процесуальних аспектів використання цифрових доказів та електронних носіїв інформації є важливим і актуальним питанням у сфері кримінально-процесуальної науки.

Аналіз останніх досліджень і публікацій. Дослідження ґрунтується на науковому доробку провідних українських вчених, які присвятили свої праці проблемам доказування в умовах цифрової трансформації. Питанням сутності, класифікації та процесуального статусу цифрових (електронних) доказів активно займалися різні вчені-правознавці: В. Д. Гавловський, А. В. Гутник, М. В. Гуцалюк, М. В. Деєв, А. В. Захарко, І. В. Краснобрижий, О. С. Матюшенко, В. В. Рогальська, Я. В. Свистун, О. В. Сіренко, К. С. Фомічов, А. В. Форостяний, В. Г. Хахановський та інші. Аналіз їхніх наукових позицій дав змогу окреслити проблемне поле, пов'язане з відсутністю чіткої легальної дефініції цифрових (електронних) доказів та уніфікованого підходу до місця електронних даних у системі джерел доказів. Наявні дискусії щодо природи цифрових доказів (документ, речовий доказ чи окреме джерело) потребують комплексного осмислення теоретичних засад доказового права у світлі сучасних технологічних викликів.

Теоретичною основою цього дослідження виступають ключові положення Кримінального процесуального кодексу України, які регламентують інститут доказів і доказування, а також міжнародно-правові акти, передусім Конвенція Ради Європи про кіберзлочинність, що закладає універсальні стандарти роботи з комп'ютерною інформацією. Фундаментальне значення мають також узагальнення судової практики Верховного Суду, що окреслюють межі допустимості й оцінки належності електронних джерел інформації.

Методи дослідження. У процесі роботи було застосовано низку методів наукового пізнання: діалектичний, системно-структурний, формально-юридичний (догматичний), порівняльно-правовий. Зокрема, діалектичний метод використовувався для пізнання процесуальних аспектів функціонування цифрового доказу як явища, що перебуває у постійній зміні, обумовленій розвитком інформаційних технологій. Формально-юридичний (догматичний) метод був ключовим для детального тлумачення чинних норм КПК України, виявлення їхньої недостатньої деталізації у питанні регламентації цифрових (електронних) доказів тощо.

Метою статті є комплексний аналіз понятійного апарату «цифрових (електронних) доказів» та «електронних носіїв інформації» і кримінально-процесуальних механізмів їх отримання, фіксації, зберігання, а також розробка науково обґрунтованих пропозицій щодо вдосконалення чинного законодавства України для забезпечення їхньої належності та допустимості.

Відповідно до визначеної мети, **завданнями дослідження** стали: 1) проведення комплексного теоретичного аналізу понять «цифровий (електронний) доказ» та «електронний носій інформації», встановлення їхньої правової природи й місця в системі джерел доказів КПК України; 2) здійснення кримінально-процесуального аналізу механізмів отримання, фіксації та зберігання цифрових доказів під час проведення слідчих дій, виявлення ключових проблем, що ставлять під загрозу їхню належність і допустимість; 3) розроблення науково обґрунтованих пропозицій щодо вдосконалення норм КПК України в цьому напрямі.

Виклад основного матеріалу. Розвиток кримінально-процесуального законодавства про докази й доказове право в умовах цифрової епохи потребує чіткого визначення сутності та місця цифрових (електронних) доказів у кримінальному процесі. Відповідно до статті 84 КПК України, доказами є будь-

які фактичні дані, отримані в законному порядку, на підставі яких встановлюються обставини кримінального провадження [2, с. 38], проте процесуальні джерела доказів, перелічені у цій статті, а саме показання, речові докази, документи та висновки експертів, не повністю охоплюють специфіку електронної інформації. Ключова теоретична проблема, що виникає на цьому етапі, полягає саме у визначенні, до якої з перелічених категорій джерел належать цифрові докази з огляду на їхню гібридну природу.

З одного боку, стаття 99 КПК України частково вирішує цю проблему, відносячи до документів електронні носії інформації, що створює процесуальне підґрунтя для використання таких даних як доказів. Однак, згідно із цією ж статтею, документ може набувати ознак речового доказу, якщо він є незмінним, і саме цей підхід викликає дискусії, оскільки основною характеристикою цифрового світу є саме його мінливість та нематеріальність інформації як такої, на відміну від матеріального носія, який її зберігає. З іншого боку, відповідно до статті 98 КПК, речові докази – це матеріальні об'єкти, які зберегли на собі сліди правопорушення [2, с. 42], і якщо електронний носій, як-от жорсткий диск чи смартфон, виступає як знаряддя злочину або об'єкт, що містить сліди, він, беззаперечно, є речовим доказом. Однак варто пам'ятати, що більшість цінних доказів, як-от дані з хмарних сховищ чи логів віддалених серверів, є саме нематеріальною інформацією, яку вилучають шляхом копіювання, а не оригінальним матеріальним об'єктом.

Таким чином, на практиці цифрові докази демонструють подвійну правову природу: сам носій інформації, наприклад смартфон чи сервер, є речовим доказом як матеріальний об'єкт, тоді як сама інформація, що на ньому міститься, наприклад листування, є різновидом документа – фактичними даними, зафіксованими електронними засобами [5, с. 25]. Це потребує від слідчого (дізнавача) суворого дотримання подвійного процесуального режиму, що передбачає як правила вилучення речових доказів, так і правила фіксації та дослідження електронних документів.

Варто також наголосити на необхідності легальної дефініції, адже хоча терміни «цифрові докази» й «електронні докази» використовуються паралельно через відсутність чіткого законодавчого розмежування, їхнє спільне значення випливає з міжнародного та національного законодавства. Зокрема, Конвенція про кіберзлочинність дає найбільш універсальне визначення «комп'ютерних даних» як будь-якого представлення фактів, придатного для обробки в комп'ютерній системі, що охоплює всі форми цифрових слідів, від тексту до логів [1]. Оскільки кіберзлочинність, як суспільно небезпечне діяння, відбувається в кіберпросторі, стає очевидним, що цифрові докази є головним інструментом доказування таких діянь. Тому для усунення правової невизначеності та підвищення рівня допустимості цих даних, видається доцільним або ввести в КПК України окреме поняття «цифрові докази» як самостійне джерело доказів, або ж деталізувати статтю 99 КПК, визначивши їхню головну особливість – залежність допустимості цифрового доказу від дотримання процедури забезпечення його цілісності, тобто його збереження в первісному недоторканому вигляді.

З огляду на викладене для покращення кримінально-процесуального врегулювання прогалин у чинному КПК України щодо роботи із цифровою інформацією можна сформулювати поняття «цифровий (електронний) доказ»

у сучасному його розумінні у статті 99 КПК, а саме як «фактичні дані про обставини, що підлягають доказуванню в кримінальному провадженні, створені, передані, збережені або витягнуті у формі, придатній для сприйняття й обробки комп'ютерною системою, незалежно від їхнього фізичного місця розташування за умови дотримання процедури їхньої цілісності та автентичності». Фізичне місце розташування цифрових (електронних) доказів може бути на електронних носіях, у комп'ютерних мережах, хмарних сховищах або інформаційно-телекомунікаційних системах тощо.

Також, на думку автора, у КПК України доцільно надати визначення поняття «електронний носій інформації» як «матеріальний об'єкт (пристрій, апаратний чи програмно-апаратний комплекс), призначений для створення, збирання, зберігання, обробки, відтворення чи передачі цифрових (електронних) доказів, що може бути вилучений як речовий доказ у кримінальному провадженні».

Варто зауважити, що процесуальний порядок отримання та фіксації цифрових доказів є найбільш вразливою ланкою доказування, оскільки саме на цьому етапі найчастіше порушується вимога щодо допустимості доказу. Чинний КПК України передбачає два основні шляхи отримання доступу до електронної інформації, які, однак, потребують суттєвої деталізації стосовно цифрової специфіки: це тимчасовий доступ до речей і документів (статті 160–166 КПК) та обшук (статті 234–236 КПК).

Тимчасовий доступ до речей і документів є найбільш поширеним інструментом для отримання цифрових доказів, що зберігаються у третіх осіб [4, с. 79], зокрема в операторів мобільного зв'язку, провайдерів інтернет-послуг або адміністраторів соціальних мереж і хмарних сховищ. Згідно зі статтею 162 КПК, електронні носії інформації визнаються оригіналами документів. Проте суттєва проблема полягає в тому, що ухвала слідчого судді про доступ найчастіше стосується не фізичного носія, а інформації, яка зберігається віддалено (трафік, метадані, зміст повідомлень). Практика потребує чіткої регламентації того, як саме має бути забезпечена цілісність (автентичність) інформації, переданої провайдером. Якщо інформація передається не на фізичному носії, а в електронному вигляді (наприклад, поштою чи через захищені канали), критично важливою є процедура збереження її автентичності як провайдером перед відправленням, так і слідчим (дізнавачем) під час її отримання.

Проведення обшуку (ст. 234 КПК) має специфічні особливості, коли предметом пошуку є електронна інформація [3, с. 21]. На відміну від традиційного обшуку, де вилучається фізичний об'єкт, під час обшуку комп'ютерних систем слідчий (дізнавач) має право: а) вилучити фізичний носій (комп'ютер, сервер, мобільний пристрій), і тоді він набуває статусу речового доказу (стаття 98 КПК); б) здійснити копіювання інформації без вилучення носія. Саме останній варіант є більш бажаним, оскільки він мінімізує втручання в господарську діяльність підприємства, установи, організації чи в приватну діяльність особи. У разі копіювання інформації, згідно із частиною 6 ст. 236 КПК, що передбачає можливість доступу слідчого (дізнавача) до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, складений протокол обшуку має максимально детально відображати всі здійснені дії. У контексті цифрових доказів це означає: обов'язкову фіксацію у протоколі технічних засобів, використаних

для копіювання (програмне забезпечення, обладнання); обов'язкове копіювання інформації у вигляді «образу», тобто побайтового копіювання, що забезпечує максимальне збереження метаданих; обов'язкове підтвердження ідентичності копії оригіналу (наприклад, шляхом зрівняння хеш-суми) [3, с. 22]. Критичною проблемою в цьому аспекті є те, що чинний КПК не містить чіткої вимоги щодо збереження автентичності доказу, залишаючи це на розсуд слідчого (дізнавача). Наслідком цього є те, що суд часто не може перевірити, чи не було змінено електронний доказ після його вилучення, що ставить під сумнів його належність і допустимість [4, с. 83]. Таким чином, для забезпечення допустимості цифрових доказів, отриманих шляхом обшуку чи тимчасового доступу, необхідна законодавча вимога про обов'язкове застосування криптографічних методів захисту на етапі їх фіксації, що забезпечить їх автентичність і має бути відображено в протоколах слідчих дій та ухвалах слідчого судді.

Питання зберігання та подальшої допустимості цифрових доказів є логічним продовженням процесу їхнього отримання, оскільки навіть ідеально вилучена інформація може втратити свою доказову силу через порушення умов її зберігання. По-перше, на відміну від традиційних речових доказів, які зберігаються у спеціальних приміщеннях, цифровий доказ, що є, по суті, копією (образом даних), потребує забезпечення недоторканності (цілісності) самої інформації, а не лише фізичного носія. Це означає, що слідчий або прокурор мають гарантувати, що з моменту фіксації і до моменту дослідження судом електронні дані не були змінені, видалені чи пошкоджені. Для цих цілей потрібно законодавчо закріпити вимогу про створення захищених цифрових депозитаріїв або спеціальних електронних сховищ в органах досудового розслідування. Це дасть змогу зберігати великі обсяги даних, отриманих за ухвалами про тимчасовий доступ, із застосуванням постійного криптографічного контролю цілісності.

Висновки. Підсумовуючи результати проведеного дослідження, слід зазначити, що норми чинного КПК недостатньо повно та чітко регламентують поняття цифрових (електронних) доказів та особливості процедури їх допустимого отримання. На підставі проведеного аналізу було запропоновано авторські визначення понять «цифровий (електронний) доказ» та «електронний носій інформації», що усувають процесуальну невизначеність. Встановлено, що проблемою правозастосування в процесі збирання, фіксації та зберігання цифрових доказів є відсутність їх автентичності й цілісності, що можна законодавчо врегулювати шляхом закріпленого обов'язку застосування криптографічних методів захисту під час отримання та збереження таких доказів. Таким чином, потрібна комплексна адаптація КПК України, що передбачає деталізацію процедур обшуку та тимчасового доступу, а також чітку регламентацію забезпечення недоторканності й автентичності цифрових доказів.

Список використаної літератури

1. Конвенція про кіберзлочинність : ратифіковано із застереженнями і заявами Законом № 2824-IV від 07.09.2005. *Офіційний вісник України*. 2007. № 65. С. 107. Ст. 2535.
2. Кримінальний процесуальний кодекс України : зі змінами та доповненнями станом на 01.07.2025 (офіційний текст). Київ : Видавництво «Паливода А.В.», 2025. 552 с.
3. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг.

ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Національної академії внутрішніх справ, 2020. 104 с.
4. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів : методичні рекомендації / авт. колектив: А. В. Захарко, А. Г. Гаркуша, В. В. Рогальська, І. В. Краснобрижий, О. В. Брягін. Дніпро : Дніпропетровський державний університет внутрішніх справ, 2019. 73 с.
5. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : колективна монографія / А. В. Гутник, А. Я. Хитра. Львів : ЛьвДУВС, 2022. 204 с.

References

1. *Konventsiia pro kiberzlochynnist: ratyfikovano iz zasterezhenniamy i zaiavamy Zakonom No. 2824-IV vid 07.09.2005* [Convention on Cybercrime: ratified with reservations and statements by Law No. 2824-IV of September 7, 2005]. (2007). Ofitsiinyi visnyk Ukrainy, (65), Art. 2535 [in Ukrainian].
2. *Kryminalnyi protsesualnyi kodeks Ukrainy: zi zminamy ta dopovnienniamy stanom na 01.07.2025 (ofitsiinyi tekst)* [Criminal Procedure Code of Ukraine: with amendments and additions as of July 1, 2025 (official text)]. (2025). Kyiv: Vydavnytstvo "Palyvoda A. V." [in Ukrainian].
3. Hutsaliuk, M. V., Havlovskyi, V. D., Khakhanovskyi, V. H., & et al. (2020). *Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh: metod. rekom.* [Use of electronic (digital) evidence in criminal proceedings: guidelines] (O. V. Korneiko, Ed.; 2nd ed.). Kyiv: Vyd-vo Natsionalnoi akademii vnutrishnikh sprav [in Ukrainian].
4. Zakharko, A. V., Harkusha, A. H., Rohalska, V. V., Krasnobryzhyi, I. V., & Briahin, O. V. (2019). *Vykorystannia elektronnykh nosiiv informatsii z media-kontentom u yakosti dzherel dokaziv: metodychni rekomendatsii* [Use of electronic information carriers with media content as sources of evidence: guidelines]. Dnipro: Dnipropetrovskyi derzhavnyi universytet vnutrishnikh sprav [in Ukrainian].
5. Hutnyk, A. V., & Khytra, A. Ya. (2022). *Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni: kolektyvna monohrafiia* [Criminal procedural and forensic bases of using electronic documents in evidence: collective monograph]. Lviv: LvDUVS [in Ukrainian].

Дата надходження статті: 27.11.2025
Дата прийняття статті: 22.12.2025
Опубліковано: 30.12.2025

B. M. Orlovskyi, Doctor of Juridical Sciences, Associate Professor, Professor
Odesa I. I. Mechnikov National University
Department of Criminal Law, Criminal Procedure and Criminalistics
24/26 Frantsuzkyi Blvd, Odesa, 65058, Ukraine
e-mail: b.orlovskyi@onu.edu.ua
ORCID iD: https://orcid.org/0000-0002-9161-2904

CRIMINAL PROCEDURAL ASPECTS OF USING DIGITAL EVIDENCE AND ELECTRONIC INFORMATION CARRIERS

Summary

The article is devoted to a comprehensive analysis of the criminal procedural aspects of using digital (electronic) evidence and electronic information carriers in criminal proceedings, a highly relevant topic given the rapid development of digital technologies and their penetration into all spheres of society. The modern criminal offense almost invariably leaves its digital

trace in the form of mobile device data, information from cloud storage, IP addresses during internet communications, or activity on social networks, all unified under the concept of digital evidence (electronic information) which holds crucial significance in the evidentiary process. The research examines the insufficient adaptation of the current norms of the Criminal Procedural Code (CPC) of Ukraine, which creates systematic obstacles to ensuring the legality, reliability, and admissibility of the electronic information obtained.

The author conducts a theoretical analysis of the legal nature of digital (electronic) evidence and establishes its hybrid procedural nature, which combines the features of both a document and material evidence, complicating uniform application of the law. To overcome this legal conflict, original, scientifically grounded definitions are proposed for potential inclusion in the CPC of Ukraine.

Specifically, it is proposed to formulate the concept of "digital (electronic) evidence" in Article 99 of the CPC as: "factual data about circumstances subject to proof in criminal proceedings, created, transmitted, stored, or extracted in a form suitable for perception and processing by a computer system, regardless of their physical location, provided that the procedure for their integrity and authenticity is adhered to". The physical location of such digital (electronic) evidence may include electronic carriers, computer networks, cloud storage, or information and telecommunication systems.

Furthermore, to avoid confusion, it is proposed to define the concept of "electronic information carrier" as: "a material object (device, hardware, or software-hardware complex) intended for the creation, collection, storage, processing, reproduction, or transmission of digital (electronic) evidence, which may be seized as material evidence in criminal proceedings".

Particular attention is devoted to practical challenges arising during the stages of collection, recording, and storage of digital evidence during searches and temporary access, especially concerning data extracted from mobile devices, social networks, and cloud storage, where information is most vulnerable. It is substantiated that, to ensure the admissibility of digital evidence, a legislative requirement for the mandatory application of cryptographic protection methods at the stage of their recording is necessary. This will ensure their authenticity and must be reflected in the protocols of investigative actions and the rulings of the investigating judge.

Emphasis is placed on the critical importance of maintaining the chain of custody, as digital evidence requires ensuring the integrity (inviolability) of the information itself, and not merely the physical carrier. A legislative requirement is proposed for the creation of secure digital repositories or specialized electronic storage facilities within pre-trial investigation bodies for the proper storage of large volumes of data obtained under investigating judges' rulings.

The importance of maintaining the authenticity of digital (electronic) evidence to ensure its relevance and admissibility when appended to the criminal case materials and during subsequent consideration in the court of first instance is underscored. The conclusion emphasizes that adapting procedural norms to digital realities is a critically necessary condition for creating a unified conceptual apparatus and procedural standards that will ensure the legality, fairness, and effectiveness of modern criminal proceedings.

Keywords: digital evidence, electronic evidence, electronic information carrier, admissibility of evidence, relevance of evidence, authenticity of evidence, recording of evidence, temporary access.