ОКРЕМІ НАПРЯМКИ УДОСКОНАЛЕННЯ ЗБЕРЕЖЕННЯ МАТЕРІАЛІВ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

ГОРДУЗ Г.В. - аспірантка кафедри кримінального процесу та криміналістики Одеського державного університету внутрішніх справ

ТЕТЕРЯТНИК Г.К. - завідувачка кафедри кримінального процесу та криміналістики Одеського державного університету внутрішніх справ, доктор юридичних наук, професор

УДК 343.1:343.98.3

DOI: https://doi.org/10.71404/NP.2025.2.49

У статті розглянуто актуальні питання удосконалення порядку збереження матеріалів кримінального провадження, які постають у контексті цифровізації правосуддя та викликів, спричинених воєнними діями на території України. Збереження матеріалів кримінального провадження визначається як необхідна процесуальна передумова дотримання принципів законності, забезпечення доказової бази, захисту прав сторін та ефективного функціонування судочинства. Увагу зосереджено на відсутності уніфікованих процедур збереження, цифрового дублювання, архівування та передачі матеріалів, що створює правову невизначеність.

У контексті національних та міжнародних стандартів підкреслюється необхідність формалізації вимог до збереження доказів, включаючи використання концепції «ланцюга зберігання доказів» (Chain of Custody). Вказано, що навіть за наявності норми частини 14 статті 615 КПК України, яка встановлює обов'язок зберігання матеріалів провадження у період воєнного стану, залишаються неврегульованими численні аспекти: строки зберігання, порядок оцифрування, способи передачі між органами досудового розслідування.

Особлива увага приділяється стану впровадження інформаційної системи досудового розслідування (іКейс) у діяльності НАБУ, САП та ВАКС, що вже сприяє збереженню окремих матеріалів.

Окремо охарактеризовано концепцію електронного кримінального провадження, яка передбачає не лише оцифрування документів, а й забезпечення захисту та контролю за рухом матеріалів, інтеграцію з реєстрами (ЄРДР, ЄСІТС, ЄДРСР). Увага акцентується на потребі комплексного забезпечення технічної бази, електронної ідентифікації, використання хеш-кодування та QR-маркування для збереження доказів.

Частина статті присвячена концепції Chain of Custody, як процедурі, що забезпечує простежуваність доказів від моменту їх отримання до використання у судовому розгляді. Автори обґрунтовують необхідність впровадження цієї процедури на законодавчому рівні в КПК України, розробку типових протоколів, а також створення єдиної електронної системи зберігання та обліку доказів.

У результаті дослідження зроблено висновок про необхідність системного перегляду та доповнення процесуального законодавства з урахуванням сучасних технологічних викликів, а також актуалізовано завдання з розробки нормативного забезпечення щодо цифрової фіксації, дублювання, передачі та відновлення доказової інформації у випадку її втрати.

Ключові слова: збереження доказів, ланцюг зберігання, електронне кримінальне провадження, іКейс, цифрове дублювання, доказова інформація, кримінальне провадження, матеріали кримінального провадження, документи, взаємодія.

Постановка проблеми

Сучасний етап трансформації кримінального процесуального законодавства України, обумовлений як загальною цифровізацією

правосуддя, так і викликами, спричиненими збройною агресією проти України, актуалізує питання ефективного збереження матеріалів кримінального провадження. Збереження матеріалів провадження становить не лише технічну або організаційну, але і процесуальну проблему, адже забезпечує основу для доказування, захисту прав сторін, дотримання розумних строків та законності судових рішень. Недостатність регламентації порядку їх зберігання, архівування, цифрового дублювання або передавання між органами провадження у чинному КПК України зумовлює правову невизначеність.

Національні та міжнародні стандарти (зокрема стандарти щодо chain of custody, належного документування та зберігання доказів) вимагають від держави створення таких процедурних гарантій, які дозволять як запобігати втратам матеріалів, так і своєчасно виявляти, відновлювати та легітимізувати їх походження. Водночас відсутність системного підходу до формалізації та уніфікації дій слідчих, прокурорів, судів в аспектах збереження процесуальних матеріалів залишається слабким місцем правозастосування.

У цьому контексті потреба в удосконаленні порядку збереження матеріалів кримінального провадження постає як не лише актуальне, а й стратегічне завдання правової реформи, спрямованої на зміцнення довіри до правосуддя, гарантування права на справедливий суд, а також мінімізацію ризиків втрати кримінальних проваджень.

Аналіз останніх публікацій

Окремі аспекти відновлення втрачених матеріалів кримінального провадження висвітлюються у роботах О. В. Лазукової, В.В. Навроцької, А. Б. Романюка, Г.К. Тетерятник, Т. Г. Фоміної та ін. Натомість питання забезпечення збереження матеріалів кримінального провадження здебільшого досліджені фрагментарно, лише публікація Т. Г. Фоміної та окремі тези доповідей на науково-практичних заходах торкаються деяких питань цієї проблематики.

Метою статті є досягнення наукового результату у вигляді теоретико обґрунтованих положень щодо окремих напрямків удосконалення збереження матеріалів кримінального провадження та напрацювання на їх підставі пропозицій до вдосконалення чинного законодавства і практики його реалізації.

Виклад основного матеріалу

Спроба нормативного врегулювання цього питання в умовах воєнного стану наведена у ч. 14 ст. 615 КПК України, у якій зазначається обов'язок зберігання матеріалів кримінальних проваджень, досудове розслідування яких здійснюється у таких умовах, у дізнавача, слідчого чи прокурора. Попри наявність цієї норми детально не регламентований порядок оцифрування таких матеріалів, строки їх зберігання, передання від одно суб'єкта до іншого тощо.

Т. Г. Фоміна, досліджуючи питання зберігання матеріалів кримінального провадження, виділяє декілька можливих за чинним за чинним законодавством способів. Перший – виготовлення в електронній формі з використанням кваліфікованого електронного підпису службової особи; друга – створення з використанням інформаційно-телекомунікаційної системи досудового розслідування; третя – оцифрування, тобто переведення матеріалів кримінального провадження в електронний формат [1].

На сьогодні кваліфікований електронний підпис є уже розповсюдженим у багатьох сферах життя. Зокрема, завдяки цифровому застосунку «Дія» та іншим можливостям генерування криптографічних підписів. Крім того, відповідно до ч. 4 ст. 106-1 КПК України «Документи, підписані, погоджені в інформаційно-телекомунікаційній системі досудового розслідування з використанням кваліфікованого електронного підпису, їх примірники в електронній та паперовій формах визнаються оригіналами документів». А також до «воєнних» новел кримінального процесуального законодавства належить можливість виготовлення постанови в електронній формі з використанням кваліфікованого електронного підпису службової особи, яка прийняла відповідне процесуальне рішення, або створюється з використанням Інформаційно-телекомунікаційної системи досудового розслідування відповідно до статті

106-1 КПК України (ч. 6 ст. 110 КПК України). Втім, інформаційно-телекомунікаційна система досудового розслідування не функціонує на сьогоднішній день в органах досудового розслідування повноцінно. Певний прогрес системи електронного документообігу вбачається здебільшого в НАБУ та САП. Крім того, можливість винесення постанови в електронній формі не знімає питань збереження та електронної форми інших матеріалів кримінального провадження.

Щодо цієї форми слід зауважити, що КПК України було доповнено відповідно до Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування» від 01.06.2021 №1498-IX статтею 106 -1 «Інформаційно-телекомунікаційна система досудового розслідування» [2]. Відповідно до пояснювальної записки: «Кінцевою метою запровадження інформаційно-телекомунікаційної системи досудового розслідування є мінімізація та, як наслідок, повна відмова у майбутньому від паперового провадження на стадіях досудового розслідування та розгляду справи в суді» [3].

16 грудня 2021 року Національне антикорупційне бюро України (НАБУ) разом із Спеціалізованою антикорупційною прокуратурою (САП) вперше зареєстрували кримінальне провадження в електронній системі іКейс. Ця система впроваджується для поступового переходу до електронного документообігу між НАБУ, САП та Вищим антикорупційним судом (ВАКС). Станом на кінець 2023 року до системи внесли понад 500 кримінальних проваджень, а за 7 місяців 2024 року їх кількість збільшилась у 2,5 раза – до 1242 [4].

У доктрині кримінального процесу концепція електронного кримінального провадження на досудовому розслідуванні була розроблена у дисертаційній роботі на здобуття наукового ступеня доктора юридичних наук А. В. Столітнім. Основною ідеєю концепції є перехід від паперового документообігу в кримінальних провадженнях до електронного формату. Це передбачає створення електронних файлів через відомчі системи (ЄРДР, реєстри адвокатів, судових рішень, експертів тощо) для електронного оформлення, зберігання, захисту, обліку, пошуку, аналізу кримінально-процесуальної інформації та електронної комунікації між учасниками досудового розслідування. Метою є впровадження єдиної інтегрованої електронної системи кримінальної юстиції, пов'язаної з загальнодержавними реєстрами, для: переведення в електронну форму заходів забезпечення кримінального провадження та результатів слідчих дій; електронного накопичення, систематизації, передачі та дослідження доказів, а також прийняття процесуальних рішень, забезпечення дотримання розумних строків досудового розслідування та ефективного використання ресурсів. Електронний формат кримінального провадження розглядається як умова для запровадження електронного процесуального контролю, який мінімізує суб'єктивне втручання та корупційні ризики, сприяючи дотриманню належної правової процедури [5].

І. Г. Каланча у дисертаційному дослідженні «Судове провадження в умовах електронного реформування кримінальної юстиції» (2017 рік) визначає електронне кримінальне судочинство як інноваційну форму правозастосовної практики, здійснювана уповноваженими суб'єктами кримінального провадження в електронному правореалізаційному середовищі за допомогою електронних кримінальних процесуальних правореалізаційних засобів, зафіксована в офіційному електронному процесуальному документі [6].

На теперішній час багато наукових досліджень присвячені питанням цифровізації кримінального провадження, адже попри багато позитивних аспектів, які вона може забезпечити, постає не менше гострих питань, як потребують вирішення. Наприклад, щодо збереження таємниці досудового розслідування, конфіденційної інформації, забезпечення безпеки цілісного функціонування таких систем від хакерських атак, витоку інформації, можливості використання інформації як доказів тощо.

Як можна визначити із прикладів тих судових рішень, які проаналізовані нами у роботі, на сьогоднішній день велике зна-

чення у відновленні втрачених матеріалів кримінального провадження відіграють уже запроваджені інформаційні системи та підсистеми, бази даних, у яких може зберігатися інформація по кримінальним провадженням та окремі процесуальні документи: ЄРДР, АРМОР, ЄСІТС, ЄДРСР та інші.

Вчені справедливо зазначають, що «… кримінальний процес найбільш чутливий до швидкості обміну інформацією, що впливає на його ефективність, результативність здійснення досудового розслідування та судового слідства. Застарілі методи обміну інформацією за допомогою паперу, часові розбіжності в здійсненні слідчої дії чи прийняття процесуального рішення з моментом їх документальної фіксації, що досить часто викликає неможливість достовірного встановлення моменту виникнення юридичного факту, – все це перешкоджає темпу розвитку кримінального процесу, який суттєво відстає від розвитку інформаційного суспільства. Нагальна необхідність переведення документування кримінального провадження в електронний сегмент є базовою передумовою розробки електронного кримінального провадження» [7, с.120].

У своєму дослідженні Н.В. Глинська та Д. І. Клепка досить детально визначають не тільки напрямки цифровізації кримінального провадження, а й ті виклики, які постають у ході реалізації цих напрямів. Авторки вказують, що наразі зазначений процес знаходиться на початковому етапі, торкається особливостей оперування цифровою інформацією, забезпечення її безпеки, приведення у відповідність кримінального процесуального законодавства та зміни загальної філософії щодо використання таких матеріалів, формування цифрової грамотності учасників кримінального провадження [8].

Окремий сегмент у цій сфері, на нашу думку, становить цифровізація процесуальних документів, які стосуються негласних слідчих (розшукових) дій, збереження цифрових носіїв інформації, які створюються під час здійснення кримінального провадження (флеш-носії, вилучені носії цифрової інформації, електронні докази) тощо, упорядкування процедур, які стосуються речових доказів та ін. І знову-таки, головним чином, забезпечення унеможливлення доступу та використання такої інформації сторонніми суб'єктами. Адже в контексті відновлення втрачених матеріалів кримінального провадження мають бути створені такі гарантії для інформаційно-комунікаційних систем, які використовуються та використовуватимуться у кримінальному провадженні, що не тільки забезпечать належне зберігання матеріалів кримінального провадження, а й унеможливлять доступ до них.

Необхідним є забезпечення органів та установ ліцензійним апаратним та програмним забезпеченням, забезпечення необхідною ресурсною базою правоохоронної системи, добудова національної телекомунікаційної мережі, розробкою та побудовою якої свого часу займалась Державна служба спеціального зв'язку та захисту інформації, що дозволить створити можливість ефективної комунікації між державними органами, як у відкритому (відкрита інформація) так і у закритому (ДСК, службова інформація тощо) сегментах [9, с. 107 – 108].

У частині вдосконалення порядку зберігання матеріалів кримінального провадження не можна, на нашу думку, оминути «ланцюг зберігання доказів» (Chain of Custody), який являє собою послідовне документування, яке враховує послідовність зберігання, контролю, передачі, аналізу та утилізації фізичних або електронних доказів. Мета полягає у встановленні того, що докази пов'язані з ймовірним злочином, були зібрані з місця події та перебували в своєму первісному/незміненому стані, а не були підроблені або «підкинуті» обманним шляхом, щоб змусити когось виглядати винним. Ланцюг зберігання зберігає цілісність зразка. Відстежуваність запису контролю, передачі та аналізу зразків свідчить про прозорість процедури [10].

Документація ланцюга зберігання служить трьом основним цілям: ставити відповідні запитання щодо доказів аналітичній лабораторії, вести облік ланцюга зберігання та документувати, що зразок/докази оброблялися лише уповноваженим персоналом і не були доступні для фальсифікації перед аналізом. Слідчий або особа, відповідальна за збір доказів, повинна заповнити етикетки контейнера/мішків для зразків та форми

ланцюга зберігання, щоб можна було відстежувати зразок. Кожна етикетка контейнера для зразків повинна мати унікальний ідентифікаційний код та іншу відповідну інформацію, таку як місцезнаходження, дата та час збору, ім'я та підпис особи, яка зібрала зразок, та підпис свідка(ів). Вкрай важливо, щоб докази були належним чином упаковані, щоб уникнути пошкодження під час транспортування, і бажано запечатані в пакети, стійкі до несанкціонованого втручання/захисні від несанкціонованого втручання, або за допомогою стрічки, що запобігає несанкціонованому втручанню. Окрема форма ланцюга зберігання має супроводжувати різні пакети з доказами. Форма ланцюга зберігання повинна містити щонайменше таку інформацію: унікальний ідентифікатор, ім'я та підпис особи, яка збирала пробу, офіційна адреса та контактний номер, ім'я одержувача, адреса лабораторії, деталі кожного зразка, включаючи: унікальний ідентифікатор та матриця, дата та час отримання відповідних зразків, підписи всіх учасників ланцюжка володіння з датою та часом, дата та спосіб доставки, дозвіл на аналіз зразка, будь-яка інша інформація про зразок [11].

У разі запровадження електронного кримінального провадження такий ланцюжок може бути забезпечений відповідним цифровим кодуванням на всіх етапах проходження речових доказів, що також підвищить ймовірність його збереження, а у разі втрати – віднаходження (якщо такий не знищено).

М. І. Пашковський вказує, що на важливість ланцюга зберігання доказів звертається увага у Протоколі Берклі та релевантних технічних стандартах щодо цифрових доказів: Державний стандарт України «Інформаційні технології . Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» розрізняє запис (протокол) ланцюга зберігання як документа, що визначає хронологію руху та поводження (історії) з потенційними цифровими доказами, який повинен вестися з моменту виявлення чи збирання або отримання відповідного об'єкта до його поточного статусу та місцеперебування [12, с. 158].

Задля забезпечення такого ланцюга для речових доказів перспективним є створення єдиної електронної системи для уніфікації, реєстрації, супроводу і контролю руху речових доказів від моменту їх вилучення до знищення або повернення. Вона передбачатиме: електронну реєстрація кожного доказу; автоматичне присвоєння унікального цифрового ID та QR-коду; хешування цифрових зображень; відображення історії переміщень і дій з доказом; інтеграція з ЄРДР, ЄСІТС, базами Національної поліції, прокуратури та судів.

Необхідним є встановлення обов'язкових вимог до пакування, маркування, пронумерування і пломбування речових доказів; визначення температурного, вологісного, протипожежного і протизламного режимів зберігання; обладнання спеціальних приміщень, оцифровувати (3D-сканування, фото, відео, експертні описи) всі речові докази до моменту поміщення на зберігання; зберігати цифрові копії в електронному архіві з хешкодами; у випадку втрати або знищення доказу через об'єктивні обставини – використовувати цифрову копію як підтверджений доказ у провадженні (адже щодо наявності і характеристик такого доказу можна буде допитати осіб, яким він передавався та якими він досліджувався за ланцюгом). І хоча фізично відновлення речових доказів у разі їх втрати, знищення не можливо фізично, однак у випадку наявності інформації з такого ланцюга є можливість створити відновлене досьє доказу, яке міститиме фотокопії, експертні висновки, протоколи вилучення, показання свідків, які працювали з ним. А з урахуванням того, що докази оцінюються у сукупності та взаємозв'язку, це може стати запорукою можливості відновлення принаймні частини доказової інформації. Chain of Custody забезпечує ретроспективну фіксацію, яка може бути використана для формування доказової бази у разі фізичної втрати оригіналу.

Таким чином, запровадження та дотримання цієї процедури запобігає фальсифікації; забезпечує відстежуваність кожного контакту з доказом; дозволяє точно встановити джерело походження доказу, його цілісність, місце зберігання та відповідальних осіб; підвищує доказову цінність у суді, особливо у випадках втрати матеріалів провадження.

У разі втрати речових доказів (наприклад, унаслідок бойових дій або техногенних катастроф), наявність повного ланцюга зберігання може дозволити частково або повністю відновити інформацію про такі об'єкти: ким, коли і де вони були вилучені, у якій упаковці зберігались; чи проводились з ними слідчі (розшукові) дії; які цифрові копії, фотографії або протоколи щодо них наявні.

Висновки

Хоча зазначена тематика потребує додаткового доктринального та нормативного опрацювання, вважаємо, що перспективним стане доповнення КПК України окремою статтею «Процедура ланцюга зберігання доказів», в якій доцільно передбачити: обов'язкове ведення ланцюга для кожного доказу; уніфіковану форму протоколу зберігання та передачі; чіткі вимоги до маркування, пакування та передачі.

Крім того, доцільно передбачити положення, згідно з яким у разі втрати речового доказу може використовуватись його цифровий еквівалент (знімок, 3D-модель, хеш-код), за умови наявності безперервного ланцюга зберігання. Необхідною є інтеграція системи Chain of Custody в іКейс з автоматичним створенням цифрової картки на кожен доказ. Доцільно також розробити підзаконний нормативний акт, який регулює технічні вимоги до документації ланцюга доказів, його зберігання і цифрового кодування (положення чи інструкцію).

На сьогоднішній день оцифрування матеріалів кримінального провадження є основною умовою для забезпечення їх збереження та можливості подальшого відновлення. Перспективним є перехід до електронного кримінального провадження, однак ця процедура залишається частково врегульованою та фактично реалізується лише в окремих органах, таких як НАБУ, САП, ВАКС. Відтак потребує подальшої розробки та впровадження система електронного кримінального провадження «іКейс». Перспективною є розробка єдиної електронної системи обліку речових доказів, інтегрованої з ЄРДР, ЄСІТС та іншими державними базами, яка забезпечить не лише збереження доказів, а й дасть змогу частково або повністю відновити інформацію щодо них у випадку втрати.

Література

1. Фоміна Т.Г. Особливості збереження матеріалів кримінальних проваджень в умовах воєнного стану. Вісник ХНУВС. 2022. № 2(97). С. 250 – 260.

2. Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування: Закон України від 01.06.2021 №1498-IX. URL: https://zakon.rada.gov.ua/laws/show/1498-20#n6.

3. Пояснювальна записка до проекту Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування». URL: https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=5246&conv=9.

4. Як працює система електронного кримінального провадження ікейс. URL: https://ti-ukraine.org/research/yak-pratsyuye-systema-elektronnogo-kryminalnogo-provadzhennya-ikejs/.

5. Столітній А.В. Електронне кримінальне провадження на досудовому розслідуванні: дис…канд. юрид. наук : 12.00.09. Київ, 2018. 648 с.

6. Каланча І.Г. Судове провадження в умовах електронного реформування кримінальної юстиції: дис…канд. юрид. наук : 12.00.09. Київ, 2017. 277 с.

7. Жученко О. Д. До питання про передумови розроблення електронного кримінального провадження в Україні. Правова держава. 2019. № 33 С. 116–122.

8. Глинська Н.В., Клепка Д.І. Цифровізація кримінального провадження: сучасні аспекти концептуалізації. Питання боротьби зі злочинністю : зб. наук. пр. / редкол.: В. С. Батиргареєва (голов. ред.) та ін. Харків : Право, 2022. Вип. 43. С. 24 – 45.

9. Мазурков Д.Д. Проблеми запровадження та функціонування електронного кримінального провадження. Цифровізація кримінального провадження: стан та перспективи : матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.:

Н. В. Глинська (голов. ред.), Д. І. Клепка, А. А. Барабаш] ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України ; Від. дослідж. проблем кримін. процесу та судоустрою. – Харків : Право, 2024. С. 102 – 108.

10. Bórquez P. [Importance of chain of custody of evidences]. Rev Med Chil. 2011 Jun;139(6):820-1.

11. Ashish Badiye; Neeti Kapoor; Ritesh G. Menezes. Chain of Custody. https://www.ncbi.nlm.nih.gov/books/NBK551677/.

12. Пашковський М.І. Ланцюг зберігання доказів (Chain of Custody): процесуальна форма. *Матеріали конференцій МЦНД*, (06.12.2024; Могилів-Подільський, Україна), 157–161.

Horduz H.V., Teteriatnyk H.K.

CERTAIN APPROACHES TO ENHANCING THE PRESERVATION OF MATERIALS IN CRIMINAL PROCEEDINGS

The article addresses pressing issues concerning the improvement of procedures for the preservation of materials in criminal proceedings, which arise in the context of the digitalization of justice and the challenges caused by military actions in Ukraine. The preservation of materials in criminal proceedings is defined as a necessary procedural prerequisite for ensuring the principles of legality, the formation of an evidentiary base, the protection of the rights of the parties, and the effective functioning of the judiciary. The study highlights the lack of unified procedures for the preservation, digital duplication, archiving, and transfer of procedural materials, which results in legal uncertainty.

Within the framework of national and international standards, the article emphasizes the need to formalize requirements for the preservation of evidence, including through the application of the "Chain of Custody" concept. It is noted that even with the provision of Part 14 of Article 615 of the Criminal Procedure Code of Ukraine, which establishes the obligation to preserve materials during martial law, multiple aspects remain unregulated — including the duration of preservation, the process of digitization, and the methods for transferring materials between pre-trial investigation bodies.

Special attention is given to the current state of implementation of the pre-trial investigation information system (iCase) in the activities of the National Anti-Corruption Bureau of Ukraine (NABU), the Specialized Anti-Corruption Prosecutor's Office (SAPO), and the High Anti-Corruption Court (HACC), which has already contributed to the preservation of certain types of materials.

The article also characterizes the concept of electronic criminal proceedings, which entails not only the digitization of documents, but also the protection and control of material circulation, integration with national registers (such as the Unified Register of Pre-Trial Investigations, the Unified Judicial Information and Telecommunication System, and the Unified State Register of Court Decisions). Emphasis is placed on the need for comprehensive technical support, electronic identification, and the use of hash-coding and QR marking to ensure the secure preservation of evidence.

A separate section of the article is devoted to the Chain of Custody concept as a procedural mechanism ensuring the traceability of evidence from the moment of collection through its use in judicial proceedings. The authors argue for the necessity of implementing this procedure at the legislative level by amending the Criminal Procedure Code of Ukraine, developing standard protocols, and creating a unified electronic system for the storage and accounting of evidence.

As a result of the research, the article concludes that there is a need for a systemic revision and supplementation of procedural legislation in light of current technological challenges. It also emphasizes the importance of developing regulatory support for the digital recording, duplication, transfer, and restoration of evidentiary information in the event of its loss.

Keywords: preservation of evidence, chain of custody, electronic criminal proceedings, iCase, digital duplication, evidentiary information, criminal proceedings, case materials, documents, inter-agency cooperation.