Кримінальний процес та криміналістика

УДК 343.9:004:343.98

DOI https://doi.org/10.5281/zenodo.18800053

Процесуальний та криміналістичний аспект використання цифрових доказів під час досудового розслідування в умовах воєнного стану із урахуванням судової практики

Головкін Сергій Вікторович,
кандидат юридичних наук, доцент, старший науковий співробітник,
доцент кафедри кримінального процесу та криміналістики,
Донецький державний університет внутрішніх справ,
Кропивницький, Україна, https://orcid.org/0000-0002-3204-2286

Квашук Олександр Дмитрович,
кандидат юридичних наук,
старший викладач кафедри кримінального процесу та криміналістики,
Донецький державний університет внутрішніх справ,
Кропивницький, Україна, https://orcid.org/0009-0008-5969-4576

Дробенко Діна Федорівна,
старший викладач кафедри кримінального процесу та криміналістики,
Донецький державний університет внутрішніх справ,
Кропивницький, Україна, https://orcid.org/0009-0005-9950-6283

Прийнято: 11.02.2026 | Опубліковано: 27.02.2026

Анотація. Стрімка цифровізація суспільних відносин та інтенсифікація використання електронних засобів фіксації інформації зумовили суттєве

зростання ролі цифрових доказів у кримінальному процесі, що особливо виразно проявляється в умовах воєнного стану. Правовий режим воєнного стану істотно впливає на процесуальні та криміналістичні умови отримання цифрових доказів, їх перевірки й оцінки, актуалізуючи низку теоретичних і прикладних проблем правозастосування.

Мета статті полягає у комплексному аналізі процесуальних та криміналістичних аспектів використання цифрових доказів під час досудового розслідування в умовах воєнного стану з урахуванням актуальної судової практики та у формулюванні обґрунтованих напрямів удосконалення правового регулювання і практичної діяльності органів досудового розслідування.

У дослідженні використовувалися системно-структурний, формально-юридичний, порівняльно-правовий та формально-логічний **методи**, а також узагальнення судової практики місцевих судів, апеляційних інстанцій і Верховного Суду, що дозволило виявити типові проблеми допустимості та оцінки цифрових доказів.

Результати дослідження свідчать, що в умовах воєнного стану зберігається фрагментарність підходів судів до визначення процесуального статусу цифрової інформації, спостерігається нерівномірність стандартів доказування та підвищена увага до обґрунтування відступів від загальних процесуальних процедур. Установлено, що сам по собі режим воєнного стану не визнається судами універсальною підставою для нівелювання процесуальних гарантій, натомість посилюється значення криміналістичної коректності фіксації, збереження й перевірки автентичності цифрових даних.

Наукова новизна дослідження полягає у комплексному поєднанні процесуального та криміналістичного підходів до аналізу цифрових доказів саме в умовах воєнного стану, уточненні їх процесуального статусу в системі джерел доказів, а також у формуванні узагальнених критеріїв оцінки автентичності та допустимості цифрової інформації з урахуванням сучасної

судової практики. Уперше систематизовано підходи Верховного Суду щодо допустимості цифрових матеріалів, отриманих в умовах обмеженого доступу до інфраструктури та змінених процедур доказування. Окрім цього, в роботі уточняються поняття «цифрова інформація», «цифрові сліди» та «цифрові докази» у контексті кримінального процесу; обґрунтовується необхідність посилення криміналістичних стандартів фіксації та збереження цифрових даних в умовах воєнного стану; формуються практичні рекомендації щодо забезпечення безперервності ланцюга збереження цифрових доказів; визначаються напрями удосконалення кримінального процесуального законодавства з урахуванням актуальної судової практики.

Висновки полягають у тому, що подальший розвиток практики використання цифрових доказів потребує поєднання нормативного уточнення їх процесуального статусу з виробленням стабільних судових орієнтирів та впровадженням криміналістичних стандартів роботи з цифровою інформацією. Обґрунтовано, що лише за умов системного підходу можливе забезпечення балансу між ефективністю досудового розслідування та дотриманням засад кримінального процесу в умовах воєнного стану.

Ключові слова: кримінальний процес, криміналістика, цифрові докази, досудове розслідування, воєнний стан, судова практика.

Procedural and forensic aspects of the use of digital evidence during pre-trial investigation under martial law with due regard to judicial practice

Serhii Holovkin,

Candidate of Legal Sciences, Associate Professor, Senior Research Fellow,

Associate Professor of the Department of Criminal Procedure and Criminalistics,

Donetsk State University of Internal Affairs,

Kropyvnytskyi, Ukraine, https://orcid.org/0000-0002-3204-2286

 ISSN: 3041-2110

Oleksandr Kvashuk,
Candidate of Legal Sciences,
Senior Lecturer of the Department of Criminal Procedure and Criminalistics,
Donetsk State University of Internal Affairs,
Kropyvnytskyi, Ukraine, https://orcid.org/0009-0008-5969-4576

Dina Drobenko,
Senior Lecturer of the Department of Criminal Procedure and Criminalistics,
Donetsk State University of Internal Affairs,
Kropyvnytskyi, Ukraine, https://orcid.org/0009-0005-9950-6283

Abstract. The rapid digitalization of social relations and the intensification of the use of electronic means of recording information have led to a significant increase in the role of digital evidence in criminal proceedings, which is particularly evident under conditions of martial law. The legal regime of martial law has a substantial impact on the procedural and forensic conditions for obtaining digital evidence, as well as on its verification and evaluation, thereby actualizing a range of theoretical and applied problems of law enforcement.

The **purpose** of the article is to conduct a comprehensive analysis of the procedural and forensic aspects of the use of digital evidence during pre-trial investigation under conditions of martial law, considering current judicial practice, and to formulate well-grounded directions for improving legal regulation and the practical activities of pre-trial investigation bodies.

The study employed systemic-structural, formal-legal, comparative-legal, and formal-logical **methods**, as well as the generalization of judicial practice of local courts, appellate instances, and the Supreme Court, which made it possible to identify typical problems related to the admissibility and evaluation of digital evidence.

The **results** of the study indicate that under conditions of martial law, the fragmentation of judicial approaches to determining the procedural status of digital information persists, there is an unevenness of evidentiary standards, and increased attention is paid to substantiating deviations from general procedural procedures. It has been established that the regime of martial law in itself is not recognized by courts as a universal ground for nullifying procedural guarantees; instead, the significance of forensic correctness in the recording, preservation, and verification of the authenticity of digital data is strengthened.

The scientific novelty of the research lies in the comprehensive combination of procedural and forensic approaches to the analysis of digital evidence precisely under conditions of martial law, in clarifying their procedural status within the system of sources of evidence, as well as in forming generalized criteria for assessing the authenticity and admissibility of digital information, taking into account contemporary judicial practice. For the first time, the approaches of the Supreme Court regarding the admissibility of digital materials obtained under conditions of restricted access to infrastructure and modified procedures of proof have been systematized. In addition, the paper clarifies the concepts of “digital information”, “digital traces”, and “digital evidence” in the context of criminal procedure; substantiates the necessity of strengthening forensic standards for the recording and preservation of digital data under conditions of martial law; formulates practical recommendations for ensuring the continuity of the chain of custody of digital evidence; and identifies directions for improving criminal procedural legislation taking into account current judicial practice.

The **conclusions** indicate that the further development of the practice of using digital evidence requires a combination of normative clarification of their procedural status with the development of stable judicial guidelines and the implementation of forensic standards for working with digital information. It is substantiated that only under the conditions of a systemic approach is it possible to ensure a balance

 ISSN: 3041-2110

between the effectiveness of pre-trial investigation and the observance of the principles of criminal procedure under conditions of martial law.

Keywords: criminal procedure, criminalistics, digital evidence, pre-trial investigation, martial law, judicial practice.

Постановка проблеми. Триваюча збройна агресія та запровадження режиму воєнного стану істотно впливає на організацію досудового розслідування та судового розгляду кримінальних проваджень. Застосування цифрових технологій у повсякденній комунікації й обігу інформації стало причиною появи великого обсягу цифрових (електронних) даних, які мають значення для встановлення фактичних обставин злочинів. Цифрові докази, як новий компонент системи джерел доказів, викликають низку складних процесуально-криміналістичних питань щодо їх належності, допустимості, автентичності та оцінки, особливо в умовах воєнного стану, коли стандартні механізми кримінального провадження змінюються під впливом зовнішніх і внутрішніх обставин.

Аналіз останніх досліджень і публікацій. У науковій літературі розвивається низка концептуальних підходів до розуміння цифрових доказів. Наукові пошуки з цього питання мають міждисциплінарний характер. Так, у цивільному судочинстві використання цифрових доказів як засобу доказування, у тому числі в умовах воєнного стану, досліджують І. Татулич [1], Л. Кондрат'єва [2], Ю. Завгородня, В. Грудницький [3] та ін. У кримінальному процесі та криміналістиці дослідження окремих питань використання цифрових доказів формує комплекс наукових результатів, які орієнтовані як на теоретичне опанування обраного об'єкту пізнання, так й на вирішення конкретних практичних завдань. Так, Н. Братішко досліджує погляди вчених на поняття та місце цифрової криміналістики в системі криміналістичної науки [4]; А. Скрипник вивчає актуальні питання використання цифрової інформації в кримінальному процесуальному

доказуванні [5]; В. Фігурський досліджує докази в електронній формі у кримінальному провадженні [6], а А. Крижановський визначає критерії віднесення електронної інформації до видів доказів [7]. Пізнавальною є праця А.-М. Ангеленюк, де авторкою розглядаються проблемні питання щодо використання електронних доказів у кримінальному процесуальному праві України [8].

Частина досліджень зосереджена на аналізі процесуальних аспектів вилучення, фіксації і збереження електронних слідів злочину в кримінальному провадженні загалом. Так, О. Манжай, А. Потильчак та І. Манжай розглядають основні процедурні проблеми обігу електронних доказів у кримінальних провадженнях та питання їхньої правової природи [9]. Інші автори акцентують увагу на правових механізмах забезпечення балансу між ефективністю використання цифрових даних та захистом прав людини, зокрема права на приватність [10]. Також формується фундамент для розуміння критеріїв допустимості та правових стандартів доказів цифрового походження в кримінальному судочинстві, включно з аналізом процедурних умов, встановлених кримінальним процесуальним законодавством [11].

Частина робіт безпосередньо присвячена аналізу проблем використання цифрових доказів під час досудового розслідування в умовах воєнного стану. Зокрема, Н. Сенченко та Н. Костюченко [12] акцентують увагу на трансформації доказового процесу в умовах обмежених процесуальних можливостей. Автори переважно зосереджені на процедурних аспектах збирання та фіксації доказів, а також на допустимості використання цифрових джерел інформації в умовах спрощених або модифікованих процедур. При цьому криміналістичні механізми забезпечення автентичності цифрових даних часто залишаються поза межами комплексного аналізу.

М. Капустіна, Є. Демидова, К. Латиш [13], В. Стратонов [14], С. Болвінов [15] розглядають цифрові інструменти передусім як засіб підвищення ефективності розслідування воєнних злочинів, приділяючи

 ISSN: 3041-2110

значну увагу технологічним можливостям фіксації фактів збройної агресії, використанню відкритих джерел (OSINT), супутникових зображень, даних з безпілотних літальних апаратів тощо. У межах цього підходу цифрові дані аналізуються здебільшого як інформаційний ресурс, що має потенціал доказового значення, однак питання їх процесуальної легітимації, забезпечення безперервності ланцюга збереження та оцінки судами часто висвітлюються фрагментарно.

Таким чином, на підставі аналізу цих та інших праць, ми можемо простежити формування окремих напрямів дослідження використання цифрових доказів під час досудового розслідування в умовах воєнного стану процесуально-нормативного або технологічно-прикладного характеру. Вважаємо, що при опанування цієї теми бракує системного підходу, що поєднує процесуальні гарантії допустимості з криміналістичними стандартами роботи з цифровою інформацією в умовах воєнного стану.

Авторська концепція ґрунтується на інтегративному розумінні цифрових доказів як комплексного правового явища, що потребує одночасного врахування 1) процесуальних вимог законності отримання та допустимості; 2) криміналістичних стандартів фіксації, збереження та верифікації автентичності; 3) специфіки судової оцінки таких доказів у справах, пов’язаних із воєнними злочинами та злочинами проти основ національної безпеки. Саме поєднання цих елементів дозволяє сформувати узгоджену модель використання цифрових доказів у досудовому розслідуванні в умовах воєнного стану.

Виділення невирішених раніше частин загальної проблеми. Наявні дослідження демонструють недостатню увагу до процедурно-криміналістичної специфіки поводження із цифровими доказами саме в умовах воєнного стану, коли загальні підходи недостатні для вирішення проблем, пов’язаних з особливостями доказування у справах, що виникають у зв’язку з агресією та бойовими діями. Зокрема, сучасні праці все ще не в

 ISSN: 3041-2110

повній мірі досліджують питання забезпечення автентичності, безперервності ланцюга збереження цифрових слідів, їхнього впливу на якість доказування, а також специфіки оцінки цифрових даних у практиці Верховного Суду та нижчих судових інстанцій у воєнний період. Така невизначеність у теоретичних та практичних підходах зумовлює низку пробілів у кримінальному процесуальному законодавстві та судовій практиці, створюючи ризики непослідовного застосування норм у кримінальних провадженнях.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження процесуально-криміналістичних аспектів використання цифрових доказів під час досудового розслідування в умовах воєнного стану з урахуванням судової практики України, що дозволить вирішити низку ключових науково-практичних завдань. Серед таких завдань: 1) окреслити понятійно-категоріальний апарат цифрових доказів у контексті кримінального процесу; 2) проаналізувати криміналістичні особливості їхнього виявлення та збереження під час досудового розслідування в умовах воєнного стану; 3) з'ясувати процесуальні гарантії належності й допустимості електронних даних під час досудового розслідування в умовах воєнного стану; 4) узагальнити позиції Верховного Суду та інших судових інстанцій щодо оцінки цифрових доказів під час досудового розслідування в умовах воєнного стану і визначити напрями вдосконалення законодавства та практики.

Виклад основного матеріалу дослідження. Упровадження цифрових технологій в різні сфери суспільного життя зумовило істотну трансформацію доказової діяльності у кримінальному провадженні. В умовах воєнного стану це стало звичною практикою, оскільки значна частина інформації про кримінальні правопорушення фіксується та зберігається саме в цифровому середовищі. На сьогодні наукове осмислення поняття, правової природи та процесуального статусу цифрових доказів залишається дискусійним, що

зумовлює необхідність звернення як до теоретичних підходів, так і до чинного кримінального процесуального законодавства.

Для коректного наукового аналізу цифрових доказів доцільним є розмежування суміжних понять, що використовуються у кримінальному процесі та криміналістиці. Поняття «цифрова інформація» має найбільш загальний характер і охоплює будь-які дані, представлені у двійковому коді, незалежно від їх доказового значення. Те, що ми називаємо «цифрові сліди» традиційно розглядається в криміналістиці як результат взаємодії особи з цифровим середовищем. Лог-файли, метадані, записи дій користувача та інші сліди присутності особи у цифровому середовищі відображають механізм вчинення правопорушення. Натомість «електронні докази» або «цифрові докази» набувають процесуального значення лише за умови їх належного залучення до кримінального провадження та оцінки відповідно до вимог допустимості, належності й достовірності.

В умовах воєнного стану співвідношення зазначених понять ускладняється специфікою отримання та використання інформації. Фактичні обставини часто фіксуються за допомогою безпілотних літальних апаратів, супутникових систем, мобільних пристроїв цивільного населення або військовослужбовців, що зумовлює зростання ролі цифрових слідів як первинного інформаційного ресурсу. Однак перетворення такої інформації на процесуально повноцінний доказ потребує дотримання встановлених процедур, що не завжди є можливим у надзвичайних умовах. Саме ця обставина є такою, що породжує головну наукову дискусію щодо допустимих меж процесуального визнання цифрових доказів та їх використання під час досудового розслідування в умовах воєнного стану.

Наша позиція полягає у тому, що цифрові докази слід розглядати як комплексне правове явище, що перебуває на перетині кримінального процесу та криміналістики. Їх правова природа визначається не лише формальною належністю до певного джерела доказів, а й специфікою формування,

збереження та відтворення цифрової інформації. В умовах воєнного стану зазначені особливості обумовлюють потребу у подальшому уточненні процесуального статусу цифрових доказів та виробленні узгоджених підходів до їх використання під час досудового розслідування.

Важливим є належне правове регулювання використання цифрових доказів під час досудового розслідування в умовах воєнного стану. Кримінально-процесуальне законодавство України безпосередньо визнає можливість використання «електронних документів» як доказів у кримінальному провадженні. Так, Кримінальний процесуальний кодекс України (далі – КПК України) відносить електронні матеріали до категорії документів, якщо вони відповідають ознакам документу, а їхній зміст може бути використаний для підтвердження обставин, що мають значення для справи [16, ч. 1 ст. 99]. При цьому копії електронних документів та їхні дублікати, виготовлені з дотриманням встановлених процедур, визнаються судом як оригінали документів.

Окрему увагу потребує питання правового регулювання цифрових доказів в умовах воєнного стану, коли обмеження звичайного доступу до цифрових носіїв, руйнування інфраструктури та масові порушення зв’язку ускладнюють процес здобуття та фіксації інформації. Законодавець не розробив спеціального кримінального процесуального механізму для таких ситуацій, але у цьому випадку слід реалізовувати діючі норми з урахуванням стандартів, напрацьованих міжнародними організаціями, які враховують особливості збору та автентифікації цифрової інформації.

Незважаючи на відсутність прямої спеціальної норми про цифрові докази, КПК України встановлює загальні принципи допустимості та оцінки доказів, які поширюються й на цифрові матеріали, а саме: надходження доказів законним шляхом, їхня належність, достовірність, достатність і допустимість [16]. Саме ці процесуальні гарантії стають визначальними під

час досудового розслідування в умовах воєнного стану, коли підвищується ризик порушення процедури.

Оскільки правове регулювання використання цифрових доказів під час досудового розслідування в умовах воєнного стану містить певні прогалини, вагому роль у формуванні розуміння процесуального статусу цифрових доказів відіграє судова практика Верховного Суду. Так, у постановах Об'єднаної палати Касаційного кримінального суду Верховного Суду у справі № 554/5090/16-к та справі № 208/2160/18 підкреслюється, що неправомірне відмовлення в прийнятті електронного документа як доказу винятково через його електронну форму є неправомірним, якщо такі матеріали відповідають вимогам ст. 99 КПК України. Водночас суд уточнює, що ідентичність копій електронних документів може бути підтверджена технічними засобами (наприклад, обчисленням контрольних хеш-суми), що дозволяє встановити їхню автентичність [17; 18].

Практика Верховного Суду також містить рішення, які конкретизують оцінювання цифрових доказів у кримінальних справах, пов'язаних із національною безпекою та злочинами в умовах воєнного стану. Зокрема, у постанові від 12 червня 2024 р. у справі № 569/1908/23 Касаційний кримінальний суд Верховного Суду підтвердив допустимість таких цифрових доказів як скріншоти й відеофайли з месенджерів та відкритих джерел, за умови дотримання процедурної чистоти їх добору, автентифікації та фіксації джерела отримання. Суд підкреслив, що матеріали цифрової інформації, зібрані з відкритих чи закритих мереж, можуть бути вирішальними в кримінальному провадженні щодо злочинів проти основ національної безпеки України, якщо їх подано у спосіб відповідно до вимог законодавства [19].

Використання цифрових доказів під час досудового розслідування в умовах воєнного стану вимагає більш детального дослідження їх правової природи. На відміну від класичних матеріальних джерел доказової інформації, цифрові докази мають нематеріалізовану природу. Вони представляють собою

 ISSN: 3041-2110

дані, що можуть бути відтворені, передані, змінені чи скопійовані без впливу на первинний носій фізичної форми. Така природа зумовлює необхідність застосування криміналістичних методів та технічних засобів для їх виявлення, фіксації й інтерпретації в ході досудового розслідування. Важливо відрізняти носій інформації (наприклад, мобільний телефон, сервер, хмарне сховище) від доказу як інформаційного контенту, що має значення для встановлення обставин злочину. Ми цілком погоджуємося із думкою В. Романюка та С. Абламського [11, с. 140] про те, що правова кваліфікація цифрових доказів має бути спрямована не на матеріальний носій, а на інформацію у цифровому вигляді та її значення для кримінального провадження.

Криміналістична цінність цифрових доказів визначається через їх інформаційну насиченість, здатність фіксувати цифрові сліди діяльності суб'єктів злочину, а також можливість реконструкції подій за допомогою технічних і аналітичних методів. За таких умов цифрові докази слід розглядати як окремий вид доказових елементів, що вимагатимуть відповідних процедурних гарантій та спеціальних знань для правильної інтерпретації в судовому процесі.

За умов воєнного стану криміналістична практика стикається з унікальними обставинами, що істотно впливають на порядок виявлення та вилучення цифрових доказів. По-перше, доступ до місця події на передовій або в зоні бойових дій може бути обмежений або небезпечний, що створює ризики для збереження цієї інформації. По-друге, на деокупованих територіях частина цифрових носіїв може бути пошкоджена, видалена або недоступна через технічні проблеми (відсутність електропостачання, пошкодження мереж). Це вимагає адаптації криміналістичних методик збору та фіксації цифрових доказів під час досудового розслідування, зокрема використання автономних засобів копіювання та застосування оперативних методів вивчення дисків, флеш-носіїв, мобільних терміналів без традиційної інфраструктури технічної підтримки оперативно-розшукових підрозділів.

Особлива увага в таких умовах приділяється фіксації цифрових слідів у відкритих джерелах (open-source intelligence, OSINT), тобто доступної інформації з інтернет-платформ, соціальних мереж, відеохостингів тощо. Незважаючи на дискусійні підходи щодо допустимості такого контенту в суді, практика свідчить про посилення уваги до OSINT при формуванні доказової бази для кримінальних проваджень воєнного характеру [20].

При цьому методологічно важливо розмежовувати фіксацію цифрових даних на місці події (вилучення пристроїв, створення копій) та комплексний офлайн- та онлайн-аналіз, що проводиться в безпечних умовах лабораторій цифрової криміналістики. Процесуальні дії мають супроводжуватися детальною технічною фіксацією параметрів вилучення, аби забезпечити подальший ланцюг збереження даних.

Цілісність та автентичність цифрових доказів при їх зборі і фіксації в умовах воєнного стану є важливим криміналістичним завданням при роботі з цифровою інформацією. Цілісність означає, що дані збережено без несанкціонованих змін, а автентичність свідчить про те, що цифровий доказ дійсно походить від зазначеного джерела. В умовах воєнного стану ці проблеми загострюються із-за таких причин як фрагментарність зв’язку, відсутність стабільного доступу до хмарних сервісів, фізичні ушкодження пристроїв тощо. Посилені ризики втрати або знищення цифрових доказів спричиняють загрозу для доказової інформації у цілому.

З точки зору криміналістики встановлення автентичності цифрового доказу вимагає застосування метаданих, цифрових підписів, записів журналів доступу та інструментів, що дозволяють реконструювати повний технічний шлях утворення, зберігання й передачі даних. Практичний аспект у цьому процесі пов’язаний, у тому числі, із необхідністю дотримання стандартів міжнародних протоколів, зокрема протоколу Берклі (Berkeley Protocol), що визначають правила архівації та збереження цифрової інформації для юридичного використання.

ISSN: 3041-2110

Процесуально-криміналістична практика використання цифрових доказів під час досудового розслідування в умовах воєнного стану фокусується на проблемі можливих маніпуляцій із цифровими даними у відкритих і закритих мережах. Цифрові записи можна змінити, видалити або підробити, що унеможливлює їх належне використання без детальної технічної верифікації. Саме через ризики таких змін цифрові докази потребують суворого дотримання криміналістичного ланцюга збереження, адже будь-яка технічна недбалість може бути підставою для їх виключення з доказового масиву в суді.

Аналіз судової практики у рішеннях, пов’язаних із використанням цифрових доказів під час досудового розслідування в умовах воєнного стану свідчить про низку типових помилок, через які цифрові докази визнавалися недопустимими або такими, що не підлягають оцінюванню у кримінальному провадженні. Однією з поширених помилок є недостатнє документальне оформлення ланцюга збереження цифрових носіїв, що має вираз у відсутності чітких записів про час, місце, осіб, які вилучали пристрій, або неправильному маркуванні файлів. Це призводить до сумнівів щодо цілісності доказів та можливості їх технічної зміни, що суперечить вимогам допустимості.

Також суди звертають увагу на випадки, коли скріншоти, відео або файли не супроводжувалися підтвердженням джерела їх отримання. Без сертифікатів експертиз або без технічного протоколу вилучення такі матеріали можуть бути відхилені. Однак, у деяких випадках суди застосовують гнучкий підхід до визнання цифрових доказів. Так, рішенням районного суду Херсонської області від 18 грудня 2025 року було визнано допустимими електронні докази (фото, звукозаписи, відео), що містилися у відкритих та закритих мережах, з врахуванням їх репрезентативності для обставин злочину та належної фіксації у матеріалах справи [21]. Вважаємо, що такі підходи є важливим елементом сучасного доказування, що дозволяє збалансувати право

 ISSN: 3041-2110

на справедливий суд із потребами ефективного розслідування, зокрема складних злочинів, пов'язаних із агресією та безпекою держави.

Суперечливим залишається питання оцінки доказів OSINT без додаткової технічної верифікації, що у деяких рішеннях викликає заперечення суддів щодо достовірності таких даних, якщо вони не підтверджені експертними висновками. Це свідчить про необхідність удосконалення методик криміналістичного дослідження цифрових доказів та підготовки спеціалістів для їх коректної оцінки в суді.

Законодавче регулювання використання цифрових доказів під час досудового розслідування в умовах воєнного стану має передбачати наявність чітких умов здобуття цифрових доказів, що випливають із загальних положень КПК України про доказування, а також із спеціальних норм, що регламентують слідчі дії. Зокрема, обшук та вилучення електронних пристроїв, доступ до інформації в автоматизованих системах та інші дії, що можуть зачіпати право на таємницю листування, здійснюються на підставі ухвали слідчого судді, окрім випадків, чітко передбачених законом як невідкладні. Процедури тимчасового доступу до речей і документів, а також застосування негласних слідчих розшукових дій також вимагають дозволу суду. Це гарантує законність збору цифрових даних як доказів і запобігає свавільному втручанню в приватну інформацію, оскільки цифрові технології за своєю природою можуть містити значний обсяг персональних даних, доступ до яких без належних процесуальних підстав створює ризик порушення конституційних прав.

Судова практика Верховного Суду останніх років містить численні позиції, що ілюструють стандарти оцінки цифрових доказів за різних обставин. Процесуальні порушення на етапі вилучення електронних пристроїв можуть істотно вплинути на допустимість доказів. Якщо обшук або вилучення здійснено з порушенням обов'язкових умов (наприклад, без судового дозволу там, де це обов'язково), такі докази можуть бути визнані недопустимими.

ISSN: 3041-2110

Судова практика вказує на необхідність чіткої фіксації процедурних дій із цифровими носіями, включно з фіксацією їх стану, ланцюга зберігання та можливістю ідентифікації джерела доказів, що є запобіжником проти маніпуляцій та утручань у хід розслідування.

Цифрові матеріали з відкритих джерел, у тому числі скріншоти сторінок криптовалютних платформ, чатів месенджерів (Telegram, Viber тощо) та відео, наприклад з безпілотних літальних апаратів, за наявності підтвердження їх походження та автентичності, можуть бути допустимими доказами. Так, у справі № 569/1908/23 Верховний Суд підтвердив, що такі цифрові докази мають значну доказову силу за умови дотримання процедурних вимог їх здобуття й фіксації [19].

Такі правові позиції Верховного Суду формують прецедентну базу, яка дозволяє практикам досудового розслідування і судам краще орієнтуватися в межах допустимого використання цифрових доказів у кримінальному процесі, зокрема у складних умовах воєнного стану. Прецедентне значення наведених правових позицій полягає у формуванні трьох ключових стандартів допустимості цифрових доказів: 1) недискримінації електронної форми доказу; 2) обов'язкової перевірки автентичності та цілісності цифрових даних; 3) забезпечення процесуальної простежуваності їх походження та збереження, з урахуванням специфіки воєнного стану. Саме ці стандарти становлять основу подальшого розвитку судової практики у сфері використання цифрових доказів. Загалом можна констатувати, що оцінювання судом цифрових доказів здійснюється із урахуванням критеріїв допустимості та специфіки їх створення, збереження та можливої вразливості до змін.

Аналіз актуальної судової практики свідчить, що використання цифрових доказів у досудовому розслідуванні в умовах воєнного стану супроводжується низкою системних проблем правозастосування, які мають як процесуальний, так і криміналістичний характер (табл. 1). Насамперед йдеться про нерівномірність підходів судів різних інстанцій до оцінки допустимості

цифрових доказів, зумовлену відсутністю чітко унормованих критеріїв їх процесуального статусу та порядку фіксації. У практиці місцевих та апеляційних судів досі фіксуються випадки формального застосування загальних положень КПК України до цифрової інформації без урахування її технічної специфіки, що призводить до суперечливих рішень щодо однорідних за змістом доказів. Верховний Суд змушений реагувати вже на наслідки допущених під час досудового розслідування процесуальних порушень, а не на їх причини.

Таблиця 1

Проблеми правозастосування використання цифрових доказів під час досудового розслідування в умовах воєнного стану

Проблема	Її особливість в умовах воєнного стану	Можливі вирішення
Відсутність чіткого процесуального визначення цифрових доказів.	Суди по-різному тлумачать правову природу цифрових даних, застосовуючи загальні норми КПК без урахування технічної специфіки.	Нормативне закріплення поняття та видів цифрових доказів у КПК України; формування узагальненої позиції Верховного Суду.
Нерівномірність судової практики щодо допустимості цифрових доказів.	За аналогічних фактичних обставин суди ухвалюють різні рішення щодо допустимості одних і тих самих цифрових доказів.	Судові узагальнення та правові висновки Верховного Суду; розроблення орієнтовних стандартів оцінки.
Порушення порядку фіксації та вилучення цифрової інформації.	У бойових або деокупованих зонах часто неможливо дотриматися класичних процедур огляду та вилучення.	Запровадження спрощених, але процесуально фіксованих процедур з обов'язковим обґрунтуванням відступів.
Недостатня фіксація технічних параметрів цифрових доказів.	Відсутність даних про час створення файлу, метадані, програмні засоби призводить до сумнівів у достовірності.	Обов'язкова деталізація технічних характеристик у протоколах; залучення спеціалістів.
Складність забезпечення цілісності та автентичності цифрових даних.	Під час евакуації, переміщення або втрати обладнання зростає ризик модифікації даних.	Використання хеш-сум, журналів доступу, резервного копіювання; стандарти цифрової криміналістики.
Формальне посилання на воєнний стан як підставу для	Судова практика не визнає воєнний стан автоматичним	Обов'язок сторони обвинувачення доводити причинно-наслідковий

ISSN: 3041-2110

порушення процесуальних гарантій.	виправданням процесуальних порушень.	зв'язок між умовами війни та відступом від процедури.
Недостатній рівень спеціальної підготовки слідчих і прокурорів.	Зростання ролі цифрових доказів не супроводжується належною криміналістичною підготовкою.	Системне навчання з цифрової криміналістики; розроблення методичних рекомендацій.
Відсутність єдиних криміналістичних стандартів роботи з цифровими доказами.	Різні підрозділи застосовують різні підходи до збирання й аналізу цифрових даних.	Уніфікація відомчих інструкцій; адаптація міжнародних стандартів (ISO, ENFSI).

Воєнний стан істотно вплинув на трансформацію судових підходів до оцінки цифрових доказів. Суди змушені враховувати об'єктивні обмеження, пов'язані з бойовими діями, окупацією окремих територій, неможливістю дотримання передбачених законом процедур фіксації доказів. З іншого боку, сам по собі режим воєнного стану не визнається судами універсальним виправданням для відступу від базових процесуальних гарантій. У цьому контексті простежується тенденція до застосування підвищеного стандарту аргументації стороною обвинувачення щодо причин і меж процесуальних відхилень, допущених під час отримання цифрових доказів. Такий підхід загалом відповідає європейським стандартам справедливого судового розгляду, однак водночас загострює проблему передбачуваності судових рішень.

Висновки. Цифрові докази слід розглядати як інформацію, зафіксовану у цифровому форматі, яка потенційно може бути використана для встановлення істини в справі за умови дотримання процесуальних гарантій. Використання цифрових доказів під час досудового розслідування є одним із інструментів сучасного доказування, яке набуває значення в умовах воєнного стану.

Цифрові докази мають властивості, що ускладнюють їх правову оцінку, зокрема можливість несанкціонованого втручання, змінюваності та залежності від складних технічних засобів. Саме тому система допустимості

таких доказів ґрунтується на чітких процесуальних гарантіях, метою яких є забезпечення балансу між ефективністю розслідування та дотриманням прав людини.

Виявлені практикою труднощі актуалізують питання нормативного уточнення процесуального статусу цифрових доказів. Обґрунтованою видається необхідність закріплення в КПК України спеціальних положень, які б визначали поняття цифрового доказу, його різновиди, а також мінімальні вимоги до способів фіксації, збереження та перевірки автентичності цифрових даних. У зв'язку із цими нами пропонується доповнити ст. 99 КПК України новою частиною такого змісту: *«Цифрові докази, отримані в порядку, передбаченому цим Кодексом, є допустимими за умови забезпечення їх цілісності, автентичності та безперервності ланцюга збереження. Сторона кримінального провадження, яка подає цифровий доказ, зобов'язана підтвердити спосіб його отримання, фіксації та збереження із зазначенням технічних засобів, що забезпечують перевірку незмінності даних»*. Таке положення дозволить нормативно закріпити процесуальний стандарт допустимості цифрових доказів, а також забезпечить уніфікацію судової практики в умовах воєнного стану. Альтернативним підходом може стати поєднання загальних процесуальних стандартів із відсилочними нормами до криміналістичних методик і відомчих інструкцій, які легше адаптуються до змін технічного середовища.

Судова практика Верховного Суду окреслює стандарти, які ускладнюють формальні підходи до цифрових доказів і закладають основу для їх надійної оцінки в умовах воєнного стану. З урахуванням узагальнень судової практики доцільно сформулювати окрему криміналістичну рекомендацію для слідчих і прокурорів. Насамперед, це максимальна процесуальна прозорість під час роботи з цифровими носіями. Йдеться про детальну фіксацію технічних параметрів, умов доступу до інформації, використаних програмних засобів, а також залучення спеціалістів у випадках,

коли цілісність або автентичність цифрових даних може бути поставлена під сумнів.

Недооцінка криміналістичних аспектів роботи з цифровими доказами під час досудового розслідування в умовах воєнного стану найчастіше стає підставою для їх подальшого виключення з доказової бази. У цьому сенсі воєнний стан не скасовує професійного підходу, а, навпаки, підвищує його значення з огляду на зростання ролі цифрових джерел інформації у досудовому розслідуванні. Проблематика використання цифрових доказів у досудовому розслідуванні в умовах воєнного стану у подальшому буде потребуватиме комплексного осмислення, яке має поєднувати процесуальний аналіз, криміналістичні методи та узагальнення судової практики.

Список використаних джерел

1. Татулич І. Ю. Електронні докази як засіб доказування в цивільному судочинстві. *Часопис Київського університету права*. 2020. № 1. С. 215–219. DOI: https://doi.org/10.36695/2219-5521.1.2020.43

2. Кондрат'єва Л. А. Електронні докази в цивільному судочинстві в період воєнного стану. *Юридичний науковий електронний журнал*. 2022. № 3. С. 90–93. DOI: https://doi.org/10.32782/2524-0374/2022-3/18

3. Завгородня Ю. В., Грудницький В. М. Роль електронних доказів у цивільному судочинстві в умовах воєнного стану. *Прикарпатський юридичний вісник*. 2023. № 6. С. 29–32. DOI: https://doi.org/10.32782/pyuv.v6.2023.6

4. Братішко Н. Напрями використання цифрової криміналістики в умовах воєнного стану. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2023. № 2 (127). С. 282–288. DOI: https://doi.org/10.31733/2078-3566-2023-6-282-288

5. Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія. Харків : Право, 2022. 408 с.

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

7. Крижановський А. С. Критерії віднесення електронної інформації до видів доказів. *Аналітично-порівняльне правознавство*. 2025. № 2. С. 1027–1032. DOI: https://doi.org/10.24144/2788-6018.2025.02.152

8. Ангеленюк А.-М. Ю. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). *Науковий вісник Ужгородського університету: серія: Право*. 2023. Т. 2. Вип. 79. С. 214–218. DOI: https://doi.org/10.24144/2307-3322.2023.79.2.32

9. Manzhai O. V., Potylchak A. O., Manzhai I. A. Procedural aspects of working with electronic evidence: the Ukrainian context. *Law and Safety*. 2021. № 3 (82). P. 13–18. DOI: https://doi.org/10.32631/pb.2021.3.01

10. Prysiazhniuk I. Use of digital evidence in criminal process: some issues of right to privacy protection. *Visegrad Journal on Human Rights*. 2023. № 5. P. 81–88. DOI: https://doi.org/10.61345/1339-7915.2023.5.11

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

12. Сенченко Н. М., Костюченко Н. Д. Збирання доказів у кримінальному провадженні в умовах воєнного стану. *Академічні візії*. 2025. № 43. С. 1–6. DOI: https://doi.org/10.5281/zenodo.15719753

13. Капустіна М. В., Демидова Є. Є., Латиш К. В. Використання сучасних інформаційних технологій при розслідуванні воєнних злочинів. *Юридичний науковий електронний журнал*. 2023. № 4. С. 564–566. DOI: https://doi.org/10.32782/2524-0374/2023-4/134

14. Стратонов В. М. Актуальні напрями використання електронних інформаційних систем в умовах воєнного стану. *Науковий вісник ХДУ. Серія:*

юридичні науки. 2025. № 1. С. 36–41. DOI: https://doi.org/10.32999/ksu2307-8049/2025-1-6

15. Болвінов С. П. Практичні аспекти застосування інформаційних систем під час розслідування воєнних злочинів (на прикладі системи SORC). *Вісник кримінологічної асоціації України*. 2024. № 2 (32). С. 531–543. DOI: https://doi.org/10.32631/vca.2024.2.38

16. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651–VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 10.12.2025).

17. Постанова Об'єднаної палати Касаційного кримінального суду Верховного Суду від 29 березня 2021 р. у справі № 554/5090/16-к. URL: https://reyestr.court.gov.ua/Review/96074938 (дата звернення: 10.12.2025).

18. Постанова Об'єднаної палати Касаційного кримінального суду Верховного Суду від 25 вересня 2023 р. у справі № 208/2160/18. URL: https://reyestr.court.gov.ua/Review/113817314 (дата звернення: 10.12.2025).

19. Постанова Касаційного кримінального суду Верховного Суду від 12 червня 2024 р. у справі № 569/1908/23. URL: https://ips.ligazakon.net/document/view/C028046 (дата звернення: 10.12.2025).

20. OSINT як доказ у розслідуванні воєнних злочинів: представники ВС взяли участь у тематичному семінарі. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1883443/ (дата звернення: 10.12.2025).

21. Вирок Нововоронцовського районного суду Херсонської області від 18 грудня 2025 р. у справі № 954/240/25. URL: https://youcontrol.com.ua/catalog/court-document/132734947/ (дата звернення: 10.12.2025).

 ISSN: 3041-2110