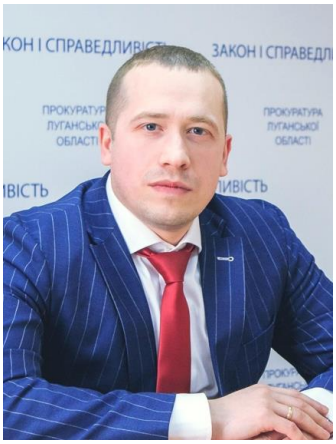
УДК 343.98 (477) *DOI: https://doi.org/10.32631/vca.2025.2.16*



Костянтин Валерійович КАРАМАН,
доктор філософії
(Ізмаїльський міськрайонний суд Одеської області, м. Ізмаїл)

СУЧАСНА ПАРАДИГМА КРИМІНАЛІСТИЧНОГО ЗНАЧЕННЯ ЦИФРОВИХ СЛІДІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

У статті проаналізовано природу цифрових слідів як елементів інформаційного середовища, що формується внаслідок злочинної діяльності у цифровому просторі. Визначено, що цифрові сліди мають потенціал виступати в ролі криміналістично значущих джерел інформації, здатних відображати механізм учинення кримінального правопорушення, особу злочинця, обстановку події та інші обставини, що мають значення для доказування. Обґрунтовано відмінність цифрових слідів від традиційних матеріальних носіїв слідової інформації, зокрема — їхня нестабільність, нематеріальність, уразливість до зовнішнього втручання та складність фіксації. Зазначено, що такі особливості потребують адаптації існуючих криміналістичних підходів і розробки нових методик фіксації, верифікації, збереження й оцінки цифрової інформації як доказу. Окреслено коло ключових проблем нормативно-правового регулювання роботи з цифровими слідами в кримінальному процесі, серед яких — відсутність усталеного поняття електронного доказу, нечіткість критеріїв допустимості та неналежне процесуальне оформлення дій із цифровими носіями. Увага також приділяється необхідності уніфікації термінології та процедур відповідно до міжнародних стандартів, зокрема положень Будапештської конвенції та рекомендацій Ради Європи.

Ключові слова: криміналістика, слід, цифровий слід, електронний доказ, доказування, збирання доказів, цифровий простір.

Постановка проблеми. Трансформаційні процеси, спричинені цифровізацією усіх сфер суспільного життя, радикально змінюють не лише форму та зміст соціальних і правових взаємодій, а й детермінують нові

моделі злочинної поведінки зокрема, та протиправної діяльності в цілому. Інформаційні технології дедалі частіше стають не просто фоном, а безпосереднім інструментом учинення кримінальних правопорушень, результатом чого є поява цифрових слідів, які дедалі більше набувають значення інформаційного ресурсу криміналістичного характеру. Ці сліди, на відміну від традиційних речових доказів, існують у нестабільному віртуальному середовищі, що потребує переосмислення методів їх виявлення, фіксації, дослідження і подальшої оцінки.

У сучасних умовах більшість протиправних дій супроводжується появою електронно-фіксованих наслідків, які можуть слугувати джерелами доказової інформації у кримінальному провадженні. Однак ефективність залучення таких слідів до процесу доказування значно ускладнюється через низку чинників — зокрема, через нечіткість процесуального статусу електронного доказу, недостатню нормативну деталізацію процедур його збирання, верифікації та збереження. Вітчизняне кримінальне процесуальне законодавство досі не містить усталеного понятійного апарату у цій сфері, а також не забезпечує належного рівня процесуальних гарантій при роботі з цифровими доказами.

Це породжує численні практичні труднощі у діяльності слідчих, прокурорів, суддів та адвокатів, включаючи випадки визнання електронних доказів недопустимими через порушення процедури їх збирання або автентифікації. Особливу загрозу становить вразливість електронної інформації до несанкціонованого доступу, видалення, фальсифікації, а також відсутність чіткого алгоритму криміналістичної оцінки її достовірності та релевантності.

Не менш важливим чинником, що впливає на формування сучасного підходу до цифрових слідів, є міжнародний вимір цієї проблематики. Як учасниця Будапештської конвенції, Україна взяла на себе зобов'язання адаптувати кримінально-процесуальні механізми до стандартів Ради Європи, які передбачають захист прав людини під час обробки електронної інформації, а також забезпечення її доказової сили у міждержавному правовому обміні. Крім того, прагнення інтегруватися до цифрового правового простору Європейського Союзу зумовлює потребу в концептуальному оновленні підходів до роботи з цифровими слідами у кримінальному провадженні, включаючи формування ефективної національної моделі їх криміналістичної оцінки.

За цих умов актуальним постає завдання не лише осмислення сутності та значення цифрових слідів як елементів криміналістичної характеристики злочинів, але й формування системних методичних підходів до їх практичного використання у механізмі доказування.

Мета статті — окреслити місце та оцінити криміналістичну цінність цифрових слідів у кримінальному провадженні.

Виклад основного матеріалу. У сучасному світі повсякденне життя людини невід'ємно пов'язане з цифровими технологіями та пристроями, які формують навколо неї складну і динамічну інформаційну екосистему. Ця

масштабна цифровізація створює нові виклики для кримінального провадження, адже більшість кримінальних правопорушень сьогодні супроводжуються появою цифрових слідів, а часом і повністю реалізуються у віртуальному середовищі. Відтак, цифрова криміналістика — як міждисциплінарна галузь знань і практики — відіграє ключову роль у забезпеченні ефективного розслідування таких діянь.

Цифрова криміналістика спрямована на виявлення, вилучення, аналіз та збереження інформації з цифрових носіїв у спосіб, що гарантує її автентичність, цілісність і допустимість як доказу в кримінальному провадженні. Проте здійснення цих завдань значно ускладнюється низкою факторів. По-перше, це — велика кількість пристроїв із різною архітектурою, конфігурацією та форматами зберігання даних. По-друге, цифрові дані часто є фрагментарними, неструктурованими, динамічними, схильними до швидкого знищення чи модифікації.

Криміналісти сьогодні змушені працювати в умовах складного мультидисциплінарного середовища, де перетинаються знання з права, кібербезпеки, інформатики, фінансової аналітики, кримінального процесу та штучного інтелекту. У контексті транснаціональної кіберзлочинності особливу складність становить необхідність взаємодії з правовими системами різних держав і дотримання вимог екстериторіального процесуального співробітництва. Ба більше, стрімкий розвиток обчислювальної техніки, хмарних технологій і телекомунікаційних мереж постійно змінює конфігурацію слідового цифрового простору, що потребує оперативної адаптації методичних підходів.

Значна частина цифрових доказів прихована в масивах великих даних (Big Data), що потребує використання спеціалізованих аналітичних інструментів і технік візуалізації. Така ситуація вимагає від слідчих, детективів, прокурорів, судових експертів та інших осіб, які забезпечують здійснення правосуддя, не лише технічної обізнаності, але й нових способів представлення та інтерпретації цифрових доказів з урахуванням їх правового статусу, доказового потенціалу й етичних обмежень.

Водночас темпи розвитку технологій нерідко випереджають можливості адаптації закону, правозастосовної практики та судово-експертних установ. Це створює потребу у формуванні стійких механізмів міжінституційної, наукової та міжнародної співпраці. Особливої актуальності набуває питання формування політик у сфері цифрової криміналістики, що включають розвиток освітніх програм, професійної підготовки кадрів, стандартизацію процесів, а також створення технологічних рішень у тісній взаємодії між слідчими органами й розробниками цифрових продуктів.

З огляду на це, подолання викликів цифрової трансформації у сфері протидії злочинності можливе лише за умови поєднання технологічних інновацій, міждисциплінарної експертизи та системного підходу до використання цифрових доказів у кримінальному провадженні.

Попри широке використання у сфері цифрової криміналістики,

інформаційної безпеки та протидії кіберзлочинності, поняття «цифровий слід» (digital trace / digital footprint) на сьогодні не має уніфікованого визначення в міжнародно-правових актах. Натомість, у нормативних і прикладних документах авторитетних міжнародних організацій (Ради Європи, Європейського Союзу, INTERPOL, ENISA, UNODC) воно трактується як інформаційний залишок, що виникає в результаті взаємодії особи або об'єкта з цифровими технологіями та має потенційну доказову цінність.

Загальновизнаним у правничій літературі є підхід, згідно з яким цифровий слід — це будь-який фрагмент цифрової інформації, що може бути зафіксований, верифікований та використаний для встановлення обставин події, ідентифікації особи або об'єкта. До цифрових слідів відносять:

- лог-файли операційних систем та сервісів;
- метадані електронних документів;
- технічну інформацію про з'єднання (IP-адреси, MAC-адреси);
- геолокаційні дані, сліди Bluetooth або Wi-Fi-з'єднань;
- історію браузера, повідомлення у месенджерах, цифрові підписи тощо.

У звітах Агентства ЄС з кібербезпеки цифрові сліди визначаються як залишкова або непряма інформація, що створюється під час взаємодії з електронними пристроями та може мати слідову й індикативну цінність для розслідування[1].

Подібний підхід спостерігається і в документах INTERPOL та Europol, де наголошується на інформативному потенціалі таких об'єктів, який реалізується лише за умови їх правильної ідентифікації, фіксації та аналізу[2].

У посібниках Ради Європи, цифрові сліди розглядаються як первинна форма цифрової інформації, що може набути статусу доказу після належної процесуальної обробки, включаючи перевірку достовірності, джерела походження та релевантності[3].

Окрему увагу цифровим слідам приділяє Управління ООН з наркотиків і злочинності (UNODC), що розглядає їх як елементи цифрового середовища, залишені в результаті онлайн-активності користувачів, які мають потенційну судову значущість у контексті протидії кіберзлочинам[4].

Щодо національного розуміння поняття «цифровий слід», то тут слід

---

[1] European Union Agency for Cybersecurity (ENISA). Roadmap on the cooperation between CSIRTs and law enforcement authorities. *ENISA.* 2019. URL: https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation (дата звернення: 14.07.2025).

[2] INTERPOL: Global Guidelines for Digital Forensics Laboratories, 2019. 78 с. – URL: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics (дата звернення: 16.07.2025).

[3] Guidelines on electronic evidence in civil and administrative proceedings: Guidelines and explanatory memorandum. Strasbourg: Council of Europe, 2019. 76 p. URL: https://book.coe.int/en/legal-instruments/7958-electronic-evidence-in-civil-and-administrative-proceedings-guidelines-and-explanatory-memorandum.html (дата звернення: 18.07.2025).

[4] United Nations Office on Drugs and Crime. (2019). *Module 4: Key issues: Digital evidence*. Education for Justice (E4J) University Module Series: Cybercrime. URL: https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/digital-evidence.html (дата звернення: 18.07.2025).

наголосити на плюралізмі термінологічного апарату. Як слушно вказує Є. Є. Демидова, «у науковій літературі на сьогодні використовують, крім поняття «цифрові сліди», також «електронні сліди», «електронні (цифрові) сліди», «віртуальні сліди», «комп'ютерні сліди»[1].

На думку А. В. Коваленка, застосування терміну «електронні (цифрові) сліди» є цілком обґрунтованим, оскільки поняття «електронний» і «цифровий» у контексті слідів і доказів мають однакове значення та є тотожними за своїм сенсо[2]. Не поглиблюючись у семантичне значення окремих термінів, ми будемо використовувати традиційний термін «цифровий слід».

Осмислення вагомості значення цифрових слідів, вважаємо за потрібне здійснити через систему їх ознак. Однією з таких є їх нематеріальна (віртуальна) природа та можливість багаторазового копіювання без втрати якості. Зокрема, цифрові зображення, відеозаписи, електронні документи можуть бути дубльовані у повному обсязі або частково змінені без жодного помітного сліду втручання, що створює як нові можливості, так і ризики в розслідуванні.

Модифікація цифрової інформації можлива завдяки широкому спектру програмного забезпечення, яке дозволяє редагувати візуальні й текстові файли. Подальшу загрозу становить розвиток технологій штучного інтелекту, який уможливлює створення високоякісних фальсифікованих матеріалів.

Окрім редагування, цифрові сліди можуть бути віддалено змінені або знищені, що часто унеможливлює їх своєчасне вилучення. У цьому контексті розрізняють два основні вектори цифрового впливу:

1. Злочинне втручання — використання шкідливого ПЗ (вірусів, троянських програм тощо) з метою зміни або знищення важливих файлів;

2. Приховування злочину — умисне редагування або видалення інформації, що становить інтерес для органів досудового розслідування.

3. Віддалений доступ до цифрових пристроїв або використання «хмарних» технологій створює можливість для керування, синхронізації та знищення інформації з будь-якої точки світу. Це значно ускладнює процес фіксації, вилучення та збереження цифрових слідів у правовому полі.

У зв'язку з цим зростає значення спеціальних знань і високої технічної кваліфікації осіб, які залучені до роботи з цифровими доказами. Недотримання технічних і процесуальних вимог при роботі з такими слідами може призвести до втрати доказової інформації або визнання її недопустимою в суді. Тому питання збереження автентичності цифрових джерел стає критичним для ефективного розслідування.

Отже, до характерних властивостей цифрових слідів належать:

---

[1] Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 4. № 85. С. 72.

[2] Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ ім. Е.О. Дідоренка.* 2022. № 4. С. 229.

1) нематеріальний (цифровий) формат існування;

2) виникнення внаслідок взаємодії з цифровими пристроями або інформаційними мережами;

3) локалізація у віртуальному середовищі (сервери, пристрої, хмари тощо);

4) можливість виявлення, фіксації та аналізу за допомогою спеціального ПЗ і обладнання;

5) відтворюваність без втрати якості, у тому числі з віддаленого доступу;

6) високий ризик модифікації або знищення, зокрема дистанційно. Ці особливості визначають унікальність цифрових слідів як об'єктів криміналістичного дослідження і потребують формування нових методичних підходів до їх обробки у межах кримінального провадження. У цьому контексті цифровий слід можна охарактеризувати як сукупність даних, що залишаються в електронному середовищі в результаті взаємодії особи з цифровими технологіями, пристроями або мережами, які можуть мати доказове значення в межах кримінального процесу.

Важливо зазначити, що цифровий слід відрізняється від цифрового доказу тим, що не є безпосередньо процесуальним джерелом доказів доти, доки не буде оброблений і верифікований відповідно до вимог кримінального процесуального законодавства. Цей факт актуалізує потребу у чіткій класифікації цифрових слідів, їх методичній і процедурній стандартизації, а також розмежуванні понять у контексті національного та міжнародного кримінального процесуального права.

Таким чином, цифрові сліди виступають як криміналістично значущі носії інформації, що можуть бути трансформовані у допустимі цифрові докази в межах кримінального провадження, за умови дотримання належних процедур їх виявлення, ідентифікації, фіксації та оцінки.

Отже, сучасне бачення ролі цифрових слідів у кримінальному провадженні формується як новітня криміналістична парадигма, згідно з якою цифрові сліди розглядаються не просто як технічні артефакти, а як самостійна категорія нематеріальних інформаційних відомостей, що виникають внаслідок взаємодії людини або інших суб'єктів з цифровим середовищем і потенційно здатні відображати обставини вчинення кримінального правопорушення.

Ця парадигма має такі ключові концептуальні ознаки:

1. Визнання цифрових слідів як окремий елемент криміналістичної характеристики (зокрема в групі слідів кримінальної протиправної діяльності). Цифрові сліди розглядаються як специфічне джерело інформації, що потребує криміналістичного аналізу нарівні з традиційними матеріальними й ідеальними слідами. Їхній доказовий потенціал формується лише за умови ідентифікації, надійної фіксації, верифікації та процесуальної оцінки відповідно до норм кримінального процесуального законодавства.

2. Переорієнтація криміналістики в бік цифрової складової. У сучасних

умовах розслідування злочинів неможливе без використання інструментів цифрової криміналістики, яка інтегрує знання з інформатики, кібербезпеки, аналізу даних, штучного інтелекту, а також міжнародного та європейського права [1]. Віртуальне середовище дедалі частіше стає місцем вчинення злочинів і, водночас, джерелом доказів [2].

3. Урахування специфічних властивостей цифрових слідів, а саме:

- нематеріальний характер та існування у цифровій формі;
- здатність до безлічі копіювань без втрати якості;
- вразливість до редагування, фальсифікації чи знищення, у тому числі з віддаленого доступу;
- розміщення в різноманітних цифрових середовищах — локальних (пристрої, носії) або віддалених (сервери, хмарні сервіси);
- необхідність спеціальних технічних знань і програмного забезпечення для виявлення, збереження та аналізу.

4. Міжнародно-правовий вимір та гармонізація правових стандартів. У зв'язку з міжнародними зобов'язаннями, зокрема участю України в Будапештській конвенції про кіберзлочинність, національна система повинна забезпечувати взаємне визнання цифрових доказів, а також готовність до транскордонного співробітництва[3].

5. Необхідність законодавчої деталізації та стандартизації. Ефективне використання цифрових слідів у кримінальному процесі неможливе без чіткого нормативного регулювання, включаючи усталену термінологію, стандартизовані алгоритми дій, методичне забезпечення та правові гарантії, які мінімізують ризики втрати доказової цінності цифрових слідів.

6. Інтеграція цифрових слідів у системну модель доказування. Цифрові сліди поступово стають невід'ємною складовою механізму встановлення предмету доказування у кримінальному провадженні. Вони дозволяють ідентифікувати події, осіб, обстановку та взаємозв'язки, значно розширюючи можливості доказування на етапах досудового розслідування та судового розгляду.

Висновки. Цифрові сліди дедалі більше впливають на змістовне наповнення криміналістики як науки та практики, формуючи нову парадигму доказування в умовах цифрового середовища. Їх правова і криміналістична цінність обумовлена здатністю відображати ключові елементи кримінального правопорушення, хоча й потребує спеціалізованих

---

[1] Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права.* 2022. № 1. С. 176–180; Шевчук В. М. Цифрова криміналістика: формування та роль у забезпеченні безпекового середовища України. *Нова архітектура безпекового середовища України*: зб. тез Всеукр. наук.-практ. конф. (м. Харків, 23 грудня, 2022 р.). Харків: Юрайт, 2022. С. 146–150.

[2] Динту В. А. Місце кіберпростору у системі обстановки злочину. Науковий вісник Херсонського державно го університету. Серія: Юридичні науки. 2016. № 2 (3). С. 72–75; Самойленко О. А. Природа кіберпростору як об'єкта криміналістичного дослідження. Криміналістика і судова експертиза. 2018. № 63 (1). С. 174–184; Вуйма А. Г. Збирання доказів в умовах цифрового простору. *Війна в Україні: зроблені висновки та незасвоєні уроки:* ІІ міжн. наук.-практ. конф. (м. Львів, 21 лютого 2025 р.). Львів : ЛьвДУВС, 2025. С. 114–115.

[3] Рада Європи. *Конвенція про кіберзлочинність (Будапештська конвенція)*. Страсбург: Рада Європи, 2001. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 18.07.2025).

підходів до виявлення, документування та оцінки.

Наявні виклики – як нормативні, так і технічні – потребують концептуального оновлення процесуального законодавства, гармонізації його з міжнародними стандартами та розроблення ефективних криміналістичних інструментів. Визначальним чинником є інтеграція цифрових слідів у цілісну систему криміналістичної характеристики злочинів, що дозволить підвищити ефективність досудового розслідування, забезпечити належну доказову базу та гарантувати дотримання прав учасників кримінального провадження. Таким чином, формування сучасної методології збирання, дослідження, використання й оцінки цифрових слідів є не лише теоретичним завданням, а й практичною необхідністю в умовах цифрової трансформації правової системи. Відтак сучасна парадигма криміналістичного значення цифрових слідів репрезентує інтегрований, міждисциплінарний, орієнтований на цифрову трансформацію підхід, що розглядає цифрові сліди як стратегічний доказовий ресурс, здатний за умови належної обробки перетворюватися на повноцінний доказ у кримінальному процесі. Вона ґрунтується на дотриманні як національних процесуальних норм, так і міжнародно-правових стандартів, забезпечуючи баланс між ефективністю кримінального провадження та дотриманням прав людини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вуйма А. Г. Збирання доказів в умовах цифрового простору. *Війна в Україні: зроблені висновки та незасвоєні уроки:* ІІ міжн. наук.-практ. конф. (м. Львів, 21 лютого 2025 р.). Львів: ЛьвДУВС, 2025. С. 114-115.

2. Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 4. № 85. С. 71-75.

3. Динту В. А. Місце кіберпростору у системі обстановки злочину. *Науковий вісник Херсонського державно го університету. Серія: Юридичні науки*. 2016. № 2 (3). С. 72–75.

4. Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального право-порушення. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка.* 2022. № 4. С. 226–236.

5. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. Київський часопис права. 2022. № 1. С. 176–180.

6. Рада Європи. *Конвенція про кіберзлочинність (Будапештська конвенція)*. Страсбург: Рада Європи, 2001. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 18.07.2025).

7. Самойленко О. А. Природа кіберпростору як об’єкта криміналістичного дослідження. *Криміналістика і судова експертиза.* 2018. № 63 (1). С. 174–184.

8. Шевчук В. М. Цифрова криміналістика: формування та роль у забезпеченні безпекового середовища України. *Нова архітектура*

безпекового середовища України: зб. тез Всеукр. наук.-практ. конф. (м. Харків, 23 грудня, 2022 р.). Харків: Юрайт, 2022. С. 146–150.

9. European Union Agency for Cybersecurity (ENISA). Roadmap on the cooperation between CSIRTs and law enforcement authorities. ENISA. 2019. URL: https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation (дата звернення: 14.07.2025).

10. Guidelines on electronic evidence in civil and administrative proceedings: Guidelines and explanatory memorandum. Strasbourg: Council of Europe, 2019. 76 p. URL: https://book.coe.int/en/legal-instruments/7958-electronic-evidence-in-civil-and-administrative-proceedings-guidelines-and-explanatory-memorandum.html (дата звернення: 18.07.2025).

11. INTERPOL: Global Guidelines for Digital Forensics Laboratories, 2019. 78 с. URL: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_Global GuidelinesDigitalForensics (дата звернення: 16.07.2025).

12. United Nations Office on Drugs and Crime. (2019). Module 4: Key issues: Digital evidence. Education for Justice (E4J) University Module Series: Cybercrime. URL: https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/digital-evidence.html (дата звернення: 18.07.2025).

Стаття надійшла до редакції 30.07.2025

Kostiantyn V. KARAMAN,
Doctor of Philosophy in Political Science
(*Judge of the Izmail District Court of Odessa Region, Izmail, Ukraine*)

MODERN PARADIGM OF THE FORENSIC SIGNIFICANCE OF DIGITAL TRACES IN CRIMINAL PROCEEDINGS

The article examines the nature of digital traces as elements of the information environment created by criminal activity in the digital space. It establishes that digital traces can serve as forensically significant sources of information capable of revealing the mechanism of the crime, the identity of the offender, the circumstances of the incident, and other relevant details vital for evidence. The distinction between digital traces and traditional material carriers of trace information is clarified, particularly their instability, intangibility, susceptibility to external interference, and the difficulty of fixation. It is highlighted that these features necessitate adapting current forensic methods and developing new techniques for the fixation, verification, preservation, and evaluation of digital information as evidence. Several critical issues related to regulatory frameworks for handling digital traces in criminal proceedings are outlined, including the absence of a clear definition of electronic evidence, vague admissibility criteria, and inadequate procedural documentation of actions involving digital media. The need to unify terminology and procedures in line with international standards, especially those outlined in the Budapest Convention and the recommendations of the Council of Europe, is also emphasized.

Key words: *forensics, trace, digital trace, electronic evidence, proving, evidence collection, digital space.*