DOI: https//doi.org/10.32353/acfs.13.2026.04
УДК 343.98 (477)

Костянтин Караман,
доктор філософії, докторант Національного наукового центру
«Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса»
м. Харків, Україна;
ORCID: https://orcid.org/0000-0003-2965-9661,
e-mail: karamankostantin@gmail.com

Костянтин Караман

Тактичні особливості збирання цифрових слідів

У статті досліджено тактичні особливості збирання цифрових слідів у кримінальному провадженні з урахуванням специфіки їх утворення, функціонування та використання у доказуванні. Обгрунтовано, що цифрові сліди є самостійним різновидом криміналістично значущої інформації, яка формується у процесі взаємодії людини, технічних засобів і цифрового середовища, характеризується динамічністю, розподіленістю, залежністю від технічних умов і можливістю дистанційного впливу. Визначено механізм їх утворення, який охоплює етапи ініціювання інформаційного процесу, технічної фіксації, розподілу, трансформації та збереження даних. Розкрито особливості тактико-криміналістичного забезпечення виявлення, вилучення та фіксації цифрових слідів, зокрема необхідність ідентифікації як матеріальних носіїв, так і логічних середовищ існування інформації, застосування спеціалізованих технічних засобів, забезпечення цілісності даних і дотримання процесуальної форми.

Ключові слова: досудове розслідування, криміналістичне забезпечення, тактично-криміналістичне забезпечення, цифровий слід, огляд комп'ютерних даних, тактичний прийом.

Постановка наукової проблеми. Вивченням матеріалів правозастосовної практики установлено, що існує низка проблем, пов'язаних із недостатньою адаптацією криміналістичних рекомендацій до особливостей цифрового середовища. Зокрема, відсутність уніфікованих тактичних алгоритмів роботи з цифровими слідами, складність забезпечення їх автентичності та цілісності, ризики втрати або модифікації даних, а також труднощі у встановленні їх джерела і достовірності істотно ускладнюють процес доказування. Додаткові виклики пов'язані з використанням сучасних технологій шифрування, анонімізації, розподіленого зберігання інформації та транскордонного характеру цифрових даних.

Не менш важливою є проблема дотримання процесуальної форми під час роботи з цифровими слідами. Неправильне застосування технічних засобів, порушення порядку вилучення чи фіксації інформації, відсутність належного документування дій із цифровими носіями можуть призвести до визнання таких доказів недопустимими. У цьому контексті особливого значення набуває поєднання техніко-криміналістичних можливостей із тактичними прийомами проведення слідчих (розшукових) дій.

Крім того, у сучасних умовах цифрові сліди дедалі частіше формуються поза межами безпосереднього контролю правоохоронних органів – у соціальних мережах, месенджерах, відкритих джерелах інформації, що актуалізує питання використання OSINT-технологій, кіберрозвідки та спеціалізованого програмного забезпечення. Водночас відсутність чітких стандартів їх застосування та процесуальної легалізації результатів такої діяльності створює додаткові ризики для доказування.

Таким чином, наявність зазначених проблем свідчить про необхідність комплексного наукового дослідження тактичних особливостей збирання та дослідження цифрових слідів, розроблення відповідних

ФІНАНСУВАННЯ

Це дослідження не отримувало жодних спеціальних грантів від фінансуючих організацій у державному, комерційному чи некомерційному секторах.

ЗАСТЕРЕЖЕННЯ

Фінансуюча сторона не брала участі в розробці дизайну дослідження, зборі та аналізі даних, прийнятті рішення про публікацію або підготовці рукопису.

УЧАСНИКИ

Автор брав участь виключно в інтелектуальній дискусії, що лежить в основі цієї статті, дослідженні прецедентного права, написанні та редагуванні, і несе відповідальність за зміст та інтерпретацію.

ДЕКЛАРАЦІЯ ПРО КОНФЛІКТ ІНТЕРЕСІВ

Автор заявляє, що у нього немає конфлікту інтересів.

криміналістичних рекомендацій і алгоритмів дій, що забезпечуватимуть ефективне використання цифрової інформації як доказу у кримінальному провадженні.

Аналіз основних досліджень і публікацій. Проблематика виявлення, фіксації та дослідження цифрових слідів у кримінальному провадженні останніми роками привертає значну увагу науковців і практиків, що зумовлено стрімкою цифровізацією суспільних відносин та ускладненням механізмів учинення кримінальних правопорушень. Аналіз сучасних досліджень свідчить про формування комплексного підходу до розуміння цифрових слідів як самостійного об'єкта криміналістичного дослідження.

Так, у роботах Д. Б. Сергєєвої обгрунтовується значення цифрових слідів у структурі доказування службових правопорушень, зокрема акцентується увага на роботі з метаданими, журналами доступу, історіями змін і резервними копіями, а також підкреслюється необхідність дотримання безперервного ланцюга збереження доказів. Це дозволяє розглядати цифрові сліди як динамічний інформаційний масив, що потребує спеціальних підходів до документування [1].

А. С. Крижановський і В. С. Кравець розглядають криміналістичні методи виявлення та фіксації цифрових слідів, акцентуючи увагу на необхідності дотримання вимог криміналістичної тактики та процесуального законодавства[2].

Суттєвий внесок у розвиток тактики роботи з цифровими доказами зроблено Л. П. Гринько, яка досліджує особливості огляду комп'ютерних засобів під час розслідування злочинів, пов'язаних із використанням мережі Інтернет. Авторка звертає увагу на значення метаданих, інформаційних слідів і необхідність комплексного підходу до організації тактики огляду. Аналогічні підходи розвиваємо і ми у своїх попередніх дослідженнях [3].

Окремий напрям досліджень пов'язаний із використанням цифрових слідів у діяльності сторони захисту. Зокрема, М. М. Щирук аналізує криміналістичні механізми адвокатського захисту, наголошуючи на значенні тактики роботи з цифровими даними та електронними документами для забезпечення якості доказів [4]. Це свідчить про поступове розширення сфери застосування цифрових слідів за межі діяльності сторони обвинувачення.

Разом із тим у науковій літературі значна увага приділяється і процесуальним аспектам проведення слідчих дій. Зокрема, у працях Б. В. Черняховського та А. В. Коваленка досліджуються питання організації огляду комп'ютерних даних, особливості їх вилучення та фіксації, а також проблеми формування доказової бази з використанням електронної інформації [5]. У цих роботах підкреслюється необхідність поєднання процесуальних вимог із криміналістичними рекомендаціями.

Kostiantyn Karaman,

TACTICAL FEATURES OF COLLECTING DIGITAL TRACES

The article examines the tactical features of collecting digital traces in criminal proceedings, taking into account their formation, operation, and use as evidence. It is substantiated that digital traces constitute an independent type of forensically significant information formed during interaction between a person, technical means, and the digital environment, characterized by dynamism, distribution, dependence on technical conditions, and the possibility of remote influence. The mechanism of their formation is determined, which includes the stages of initiating the information process, technical fixation, distribution, transformation, and storage of data. The features of tactical and forensic support for the detection, extraction, and fixation of digital traces are revealed, in particular, the need to identify both the material carriers and the logical environments of information existence, the use of specialized technical means, and the assurance of data integrity and compliance with procedural form.

Keywords: pre-trial investigation, forensic support, tactical-forensic support, digital trail, computer data review, tactical technique.

[1] Сергєєва Д. Б. Виявлення і документування способів учинення службових правопорушень: методика, тактика, цифрові сліди та ланцюг збереження доказів [Identifying and Documenting Methods of Committing Workplace Misconduct: Methods, Tactics, Digital Traces, and the Chain of Evidence]. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2025. Т. 4. № 91. С. 438-451. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.60

[2] Гринько Л. П. Тактичні особливості огляду комп'ютерних засобів під час розслідування шахрайств, учинених із використанням мережі «Інтернет» [Tactical Considerations for Examining Computer Equipment During Investigations of Internet Fraud]. *Вісник Пенітенціарної асоціації України.* 2025. № 3. С. 152-159. DOI: https://doi.org/10.34015/2523-4552.2025.3.17

[3] Караман К. В. Виявлення цифрових слідів: особливості й алгоритм [Detection of Digital Traces: Characteristics and Algorithm]. *Вісник Харківського національного університету внутрішніх справ*. 2025. Т. 110. № 3. С. 141-150.

[4] Щирук М. М. Змагальність і «якість» доказів у справах про розтрату та привласнення: криміналістичні механізми адвокатського захисту [Adversarial Proceedings and the "Quality" of Evidence in Cases of Embezzlement and Misappropriation: Forensic Mechanisms of Legal Defense]. *Аналітично-порівняльне правознавство.* 2026. Т. 3. № 1. С. 468-476. DOI: https://doi.org/10.24144/2788-6018.2026.01.3.68

[5] Черняховський Б. В. Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [Specifics of Conducting a Forensic Examination During the Investigation of Unauthorized Interference with Computers, Automated

Konstantin Karaman,

TAKTISCHE BESONDERHEITEN DER SICHERUNG DIGITALER SPUREN

In diesem Artikel werden die taktischen Besonderheiten der Sicherung digitaler Spuren im Strafverfahren unter Berücksichtigung der Besonderheiten ihrer Entstehung, Funktionsweise und Verwendung in der Beweisführung untersucht. Es wird begründet, dass digitale Spuren eine eigenständige Art von kriminalistisch relevanter Information darstellen, die im Prozess der Interaktion zwischen Mensch, technischen Mitteln und digitaler Umgebung entsteht und sich durch Dynamik, Verteiltheit, Abhängigkeit von technischen Bedingungen und die Möglichkeit der Fernbeeinflussung auszeichnet. Es wird der Mechanismus ihrer Entstehung bestimmt, der die Phasen der Einleitung des Informationsprozesses, der technischen Erfassung, der Verteilung, der Transformation und der Speicherung von Daten umfasst. Es werden die Besonderheiten der taktisch-kriminalistischen Absicherung der Aufdeckung, Sicherstellung und Erfassung digitaler Spuren aufgezeigt, insbesondere die Notwendigkeit der Identifizierung sowohl materieller Datenträger als auch logischer Informationsumgebungen, der Einsatz spezialisierter technischer Mittel, die Gewährleistung der Datenintegrität und die Einhaltung der Verfahrensvorschriften.

Schlüsselwörter: Voruntersuchung, kriminaltechnische Unterstützung, taktisch-kriminaltechnische Unterstützung, digitale Spur, Überprüfung von Computerdaten, taktischer Ansatz.

Окремі автори звертають увагу на поширеність цифрових слідів [6] або ж досліджують їх у контексті окремих видів злочинів [7]. Попри значний обсяг наукових напрацювань, слід констатувати, що проблематика тактико-криміналістичного забезпечення виявлення, вилучення та фіксації цифрових слідів залишається недостатньо систематизованою. Зокрема, потребують подальшого дослідження питання ситуаційної зумовленості тактики слідчих дій, розроблення уніфікованих алгоритмів роботи з цифровими слідами, а також інтеграції технічних і тактичних елементів у єдину криміналістичну модель. Це зумовлює актуальність подальших наукових розвідок у зазначеному напрямі.

Мета статті – розкрити тактичні особливості збирання цифрових слідів під час розслідування.

Викладення основного матеріалу дослідження. Цифрові сліди виникають у процесі взаємодії людини, технічного пристрою та інформаційного середовища. У цьому сенсі їхня поява є результатом функціонування електронних систем, які фіксують, обробляють і зберігають інформацію [8].

Механізм утворення цифрових слідів доцільно розглядати через такі взаємопов'язані етапи:

1. Ініціювання інформаційного процесу, яке може бути зумовлене діями користувача (створення файлу, надсилання повідомлення, пошуковий запит), автоматизованими процесами (оновлення системи, синхронізація даних) або зовнішнім впливом (кібератака, віддалений доступ). Саме на цьому етапі формується первинна інформація.

2. Технічна фіксація інформації в цифровому середовищі. Будь-яка дія трансформується у цифровий код і записується в пам'яті пристрою, мережевих системах або хмарній інфраструктурі. При цьому фіксуються не лише основні дані, а й супутня інформація – метадані (час, IP-адреса, параметри доступу), що мають самостійне доказове значення.

3. Розподіл і дублювання цифрових слідів. Через мережеву природу сучасних технологій інформація може одночасно зберігатися: на локальному носії; на серверах; у хмарних сховищах; у резервних копіях. Це зумовлює їх багатоканальний характер і підвищує стійкість, але водночас ускладнює контроль за їх цілісністю.

4. Цифрові сліди піддаються динамічним змінам. Вони можуть: 1) модифікуватися внаслідок подальших дій користувача; 2) автоматично оновлюватися системою; 3) змінюватися або знищуватися внаслідок злочинного втручання чи антифорензики. Це означає, що цифровий слід не є статичним, а має часову мінливість.

5. Формується залишкова (латентна) слідова інформація. Навіть після видалення даних у системі можуть залишатися їх фрагменти, кеш, журнали подій або резервні копії, що створює додатковий рівень цифрових слідів.

Таким чином, механізм утворення цифрових слідів можна визначити як процес виникнення, фіксації, трансформації та збереження інформації в електронних системах у результаті взаємодії суб'єктів із цифровим середовищем, що супроводжується формуванням як основних даних, так і похідної (метаданих та системної) інформації.

Systems, Computer Networks, or Telecommunications Networks]. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 2. С. 58-68;

[6] Нікішев О. В. Цифрові (електронні) докази у кримінальному провадженні в умовах надзвичайних правових режимів [Digital (electronic) evidence in criminal proceedings under states of emergency]. *Право.ua*. 2025. № 1. С. 365-371. https://doi.org/10.71404/law.ua.2025.1.54; Вуйма А. Цифровий вимір сучасної злочинності: кіберпростір як типова обстановка вчинення кримінальних правопорушень [The Digital Dimension of Modern Crime: Cyberspace as a Common Setting for Criminal Offenses]. *Архів кримінології та судових наук*. 2025. Т. 12, № 2. С. 64–70. DOI: https://doi.org/10.32353/acfs.12.2025.05.

[7] Романюк В. В., Фоміна Т. Г. Порядок збирання електронних (цифрових) доказів у кримінальних провадженнях про колабораційну діяльність [Procedures for Collecting Electronic (Digital) Evidence in Criminal Proceedings Concerning Collaboration]. *Вісник Кримінологічної асоціації України*. 2024. Т. 32. № 2. С. 344-353. DOI: https://doi.org/10.32631/vca.2024.2.25%20

[8] Каланча І. Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України [Organizational Aspects of Handling Electronic Evidence in Criminal Proceedings in Ukraine]. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Т. 4, № 90. С. 263. DOI: https://doi.org/10.24144/2307-3322.2025.90.4.36

Цей механізм принципово відрізняється від утворення матеріальних слідів, оскільки характеризується: нематеріальною природою, багатоканальністю існування, динамічністю, залежністю від технічного середовища, можливістю дистанційного впливу.

Визначений механізм утворення цифрових слідів, що характеризується їх нематеріальною природою, динамічністю, розподіленістю та залежністю від технічного середовища функціонування, об'єктивно зумовлює специфіку тактико-криміналістичного забезпечення їх виявлення, вилучення та фіксації. Саме ці властивості визначають необхідність формування особливих підходів, відмінних від традиційної роботи з матеріальними слідами, та потребують інтеграції технічних і тактичних елементів у єдину систему криміналістичних рекомендацій.

Насамперед, особливості виявлення цифрових слідів зумовлені їх латентним характером і відсутністю безпосереднього візуального сприйняття. Виявлення таких слідів фактично передбачає встановлення не лише матеріальних носіїв інформації (комп'ютерна техніка, мобільні пристрої, сервери), але й визначення логічних середовищ їх існування – облікових записів, хмарних сервісів, мережевих ресурсів, інформаційних систем. У цьому контексті важливого значення набувають аналітичні дії, спрямовані на ідентифікацію потенційних джерел цифрової інформації, встановлення каналів її формування та збереження, а також прогнозування можливості її втрати або модифікації. Тактична специфіка цього етапу полягає у необхідності швидкого прийняття рішень щодо ізоляції цифрового середовища з метою недопущення дистанційного впливу на дані.

Особливості вилучення цифрових слідів безпосередньо пов'язані з їхньою технічною природою. На відміну від традиційних об'єктів, вилученню підлягає не стільки сам носій, скільки інформація, що на ньому міститься. Це зумовлює необхідність застосування спеціалізованих технічних засобів і дотримання принципу незмінності даних. Тактичним пріоритетом є забезпечення цілісності інформації шляхом використання методів криміналістичного копіювання (створення побітових копій), блокування запису на носій, фіксації поточного стану системи. Водночас важливо враховувати ситуаційні чинники: увімкнений або вимкнений стан пристрою, наявність шифрування, підключення до мережі, ризик автоматичного видалення даних. У зв'язку з цим вибір способу вилучення має ситуаційно обумовлений характер і потребує високого рівня спеціальної підготовки.

Не менш специфічними є тактичні аспекти фіксації цифрових слідів. Фіксація в цьому випадку передбачає не лише документування процесу вилучення, а й забезпечення відтворюваності цифрової інформації у подальшому. Це досягається шляхом детального протоколювання всіх дій із цифровими носіями, зазначення технічних характеристик пристроїв, програмного забезпечення, умов доступу до даних, а також використання контрольних механізмів перевірки цілісності (зокрема хеш-значень). Особливістю є також необхідність фіксації не лише змісту інформації, але й її структурних і технічних параметрів, які можуть мати самостійне доказове значення.

Окремої уваги потребує забезпечення безперервного ланцюга збереження цифрових доказів (chain of custody), що в умовах їхньої мобільності та можливості копіювання набуває особливого значення. Тактичне забезпечення цього процесу передбачає чітку регламентацію передачі носіїв і копій інформації, ідентифікацію осіб, відповідальних за кожен етап роботи з доказами, а також застосування технічних засобів контролю їх цілісності.

Важливим елементом тактико-криміналістичного забезпечення є також урахування протидії розслідуванню у формі антифорензичних дій. Можливість дистанційного видалення або модифікації даних, використання шкідливого програмного забезпечення, засобів шифрування та анонімізації зумовлює необхідність застосування превентивних тактичних заходів, зокрема негайної ізоляції пристроїв від мережі, використання спеціалізованих інструментів доступу до зашифрованих даних, а також залучення відповідних фахівців.

Таким чином, тактико-криміналістичне забезпечення виявлення, вилучення та фіксації цифрових слідів характеризується комплексністю,

Kostiantyn Karaman,

CARACTÉRISTIQUES TACTIQUES DE LA COLLECTE DE TRACES NUMÉRIQUES

L'article examine les aspects tactiques de la collecte de traces numériques dans le cadre de procédures pénales, en tenant compte des spécificités de leur formation, de leur fonctionnement et de leur utilisation comme preuve. Il démontre que les traces numériques constituent une catégorie d'information criminalistique à part entière, formée lors de l'interaction entre une personne, des moyens techniques et l'environnement numérique. Ces traces se caractérisent par leur dynamisme, leur distribution, leur dépendance aux conditions techniques et la possibilité d'une influence à distance. Le mécanisme de leur formation est déterminé, comprenant les étapes d'initiation du processus informationnel, de fixation technique, de distribution, de transformation et de stockage des données. Les spécificités du soutien tactique et criminalistique à la détection, à l'extraction et à la fixation des traces numériques sont mises en évidence, notamment la nécessité d'identifier les supports matériels et les environnements logiques d'existence de l'information, d'utiliser des moyens techniques spécialisés, de garantir l'intégrité des données et le respect des formes procédurales.

Mots-clés : enquête préliminaire, soutien criminalistique, soutien criminalistique tactique, trace numérique, examen des données informatiques, technique tactique.

Kostyantyn Karaman,

TAKTYCZNE ASPEKTY GROMADZENIA ŚLADÓW CYFROWYCH

W artykule przeanalizowano taktyczne aspekty gromadzenia śladów cyfrowych w postępowaniu karnym, z uwzględnieniem specyfiki ich powstawania, funkcjonowania oraz wykorzystania w postępowaniu dowodowym. Wykazano, że ślady cyfrowe stanowią samodzielny rodzaj informacji istotnej z punktu widzenia kryminalistyki, która powstaje w procesie interakcji człowieka, środków technicznych i środowiska cyfrowego, charakteryzuje się dynamiką, rozproszeniem, zależnością od warunków technicznych oraz możliwością oddziaływania na odległość. Określono mechanizm ich powstawania, który obejmuje etapy inicjowania procesu informacyjnego, technicznej fiksacji, dystrybucji, transformacji i przechowywania danych. Ujawniono specyfikę taktyczno-kryminalistycznego wsparcia wykrywania, zabezpieczania i rejestrowania śladów cyfrowych, w szczególności konieczność identyfikacji zarówno nośników fizycznych, jak i środowisk logicznych, w których istnieje informacja, stosowania specjalistycznych środków technicznych, zapewnienia integralności danych oraz przestrzegania formy proceduralnej.

Słowa kluczowe: postępowanie przygotowawcze, wsparcie kryminalistyczne, wsparcie taktyczno-kryminalistyczne, ślad cyfrowy, przegląd danych komputerowych, zabieg taktyczny.

високим рівнем технологічної зумовленості та необхідністю поєднання процесуальних, технічних і тактичних елементів. Його ефективність залежить від здатності суб'єктів кримінального провадження адекватно реагувати на динамічний характер цифрового середовища, своєчасно виявляти та зберігати доказову інформацію, а також забезпечувати її належність, допустимість і достовірність у подальшому доказуванні.

Розвиваючи викладені положення, слід підкреслити, що тактико-криміналістичне забезпечення роботи з цифровими слідами має виразну ситуаційну зумовленість і значною мірою залежить від можливості попереднього планування слідчої (розшукової) дії. Зокрема, у випадках, коли передбачається проведення огляду комп'ютерних даних, що перебувають у володінні юридичних чи фізичних осіб і зберігаються на стаціонарних носіях у приміщеннях офісів, підприємств або установ, виникають реальні передумови для належної організації техніко-тактичного забезпечення такої дії.

У подібних умовах вагомого значення набуває завчасна підготовка матеріально-технічної бази, що дозволяє мінімізувати ризики втрати або пошкодження цифрової інформації. Йдеться, передусім, про забезпечення безперебійного живлення електронних пристроїв, що особливо актуально у випадках роботи з увімкненими системами, де відключення електроживлення може призвести до втрати оперативних даних, сесійних ключів або незбереженої інформації. Використання джерел безперебійного живлення у таких ситуаціях виступає не лише технічним, а й тактичним засобом збереження доказової інформації.

Не менш важливою складовою є попереднє оснащення необхідною кількістю носіїв інформації, призначених для копіювання цифрових даних. З огляду на значні обсяги сучасної інформації, що може зберігатися на серверному обладнанні чи робочих станціях, слідчий та залучені спеціалісти повинні мати достатній резерв накопичувачів відповідного обсягу та технічних характеристик. Це дозволяє здійснювати повне або вибіркове копіювання даних без переривання процесу та без необхідності залишати місце події для отримання додаткових ресурсів, що могло б створити ризики втручання у інформаційне середовище.

Крім того, завчасне планування дає змогу визначити оптимальну тактику вилучення інформації – чи йдеться про створення повних (побітових) копій носіїв, чи про вибіркове копіювання окремих масивів даних. У цьому контексті враховуються такі обставини, як обсяг інформації, технічні характеристики обладнання, наявність мережевого доступу, ризики дистанційного втручання, а також процесуальні обмеження щодо строків проведення слідчої дії.

Водночас слід наголосити, що така можливість попередньої підготовки притаманна не всім ситуаціям. У випадках невідкладних дій або роботи у польових умовах (наприклад, під час обшуків чи оглядів у зоні бойових дій) рівень технічного забезпечення може бути обмеженим. Саме тому у сприятливих умовах, зокрема під час роботи в офісних або виробничих приміщеннях, необхідно максимально реалізовувати потенціал превентивного тактичного планування, що дозволяє підвищити якість фіксації та збереження цифрових слідів.

Отже, можливість забезпечення безперебійного живлення, наявність достатньої кількості носіїв для копіювання та загальна підготовленість до роботи з великими обсягами цифрових даних виступають важливими елементами тактико-криміналістичного забезпечення, які безпосередньо впливають на повноту, достовірність і допустимість отриманої доказової інформації.

Розширюючи положення щодо тактико-криміналістичного забезпечення виявлення, вилучення та фіксації цифрових слідів, слід звернути увагу на конкретні практичні рекомендації, що випливають із аналізу сучасної слідчої практики та наукових джерел.

Насамперед ефективність огляду комп'ютерних даних значною мірою залежить від якісної підготовчої стадії, яка має включати попередню розвідку інформаційного середовища. Уповноважена особа повинна заздалегідь визначити коло можливих носіїв, типи файлів і очікувану інформацію, а також сформувати склад учасників процесуальної дії із залученням спеціалістів у сфері комп'ютерних або інформаційних тех-

нологій. Це свідчить про те, що тактика роботи з цифровими слідами починається ще до фактичного контакту з носієм інформації.

Важливою тактичною рекомендацією є також обов'язкове залучення спеціалістів, які забезпечують не лише технічну підтримку, а й безпечність роботи з даними, ідентифікацію об'єктів та правильне копіювання інформації. У сучасних умовах без такого супроводу проведення огляду цифрових даних є суттєво ускладненим.

Зберігання електронних носіїв у межах кримінального провадження потребує дотримання чітко визначених технічних умов, спрямованих на гарантування цілісності та автентичності даних. Йдеться не лише про належне фізичне утримання носіїв, а й про створення та збереження криміналістичних образів (побітових копій), резервне копіювання, а також дотримання правил транспортування. З урахуванням підвищеної чутливості цифрової інформації до зовнішніх впливів особливого значення набуває підтримання контрольованого середовища, що передбачає регулювання температури та вологості, екранування від електромагнітних перешкод, а також захист від механічних пошкоджень і статичної електрики[9].

Окремо слід акцентувати увагу на техніко-криміналістичному забезпеченні збирання та дослідження цифрових слідів, яке має безпосереднє тактичне значення. До технічних засобів, які можуть застосовуватися належать:

– портативні комп'ютери з автономним живленням;
– змінні акумулятори;
– накопичувачі значної ємності;
– блокувачі жорстких дисків;
– інсталяційні носії програмного забезпечення;
– спеціалізовані інструменти для роботи з даними [10].

Разом із цим, слід зауважити, що забезпечення ресурсів (живлення, носії, обладнання) є не просто технічним, а тактичним елементом, що впливає на результативність слідчої (розшукової) дії.

Суттєвою тактичною вимогою є також використання ізольованих середовищ під час дослідження даних, що дозволяє уникнути зараження системи шкідливим програмним забезпеченням. Це демонструє необхідність врахування ризиків кіберзагроз як складової тактики.

Окремого значення набуває робота з метаданими, які повинні обов'язково фіксуватися в протоколі, оскільки вони дозволяють встановити час створення, редагування, користувача й інші параметри файлів. Таким чином, фіксація цифрових слідів виходить за межі змісту інформації і охоплює її технічний контекст.

Важливою тактичною рекомендацією є також контроль за поведінкою осіб на місці проведення слідчої (розшукової) дії. Зокрема, з метою недопущення дистанційного знищення або модифікації інформації доцільно обмежити використання мобільних пристроїв усіма присутніми. Це безпосередньо пов'язано з механізмом утворення цифрових слідів і можливістю віддаленого впливу на них.

Не менш важливою є рекомендація щодо застосування гешування для підтвердження цілісності даних, що забезпечує перевірку незмінності інформації до і після копіювання. Це важливий інструмент забезпечення допустимості цифрових доказів.

Окремо слід виділити тактичні аспекти роботи з віддаленими ресурсами та хмарними сервісами. У таких випадках доцільно:

– встановлювати IP-адреси ресурсів;
– визначати маршрути передачі даних;
– фіксувати технічні параметри доступу .

Це дозволяє не лише отримати інформацію, а й довести зв'язок між особою та цифровим середовищем.

Слід зважати на правові обмеження доступу до інформації, зокрема необхідності отримання судового дозволу для доступу до даних операторів і провайдерів. Крім того, ефективне тактико-криміналістичне забезпечення неможливе без організованої взаємодії між різними суб'єктами: слідчим, оперативними підрозділами, експертами та спеціалістами з кібербезпеки. Саме груповий характер роботи дозволяє комплексно вирішувати завдання виявлення та дослідження цифрових слідів.

Тактична організація огляду комп'ютерної техніки повинна обов'язково враховувати вплив людського чинника. Учасників процесуальної дії необхідно належним чином поінформувати про їхні права, обов'язки та правові наслідки будь-яких спроб знищення чи зміни інформації. Водночас із тактичних позицій важливо забезпечити контроль за їхньою поведінкою під час проведення огляду, зокрема шляхом обмеження доступу до мережі Інтернет і електронних пристроїв, які можуть бути використані для віддаленого втручання в інформаційні системи [11].

---

[9] Каланча І. Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України [Organizational Aspects of Handling Electronic Evidence in Criminal Proceedings in Ukraine]. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Т. 4, № 90. С. 263. DOI: https://doi.org/10.24144/2307-3322.2025.90.4.36.

[10] Гринько Л. П. Тактичні особливості огляду комп'ютерних засобів під час розслідування шахрайств, учинених із використанням мережі «Інтернет» [Tactical Considerations for Examining Computer Equipment During Investigations of Internet Fraud]. *Вісник Пенітенціарної асоціації України*. 2025. № 3. С. 152–159. DOI: https://doi.org/10.34015/2523-4552.2025.3.17.

[11] Гринько Л. П. Тактичні особливості огляду комп'ютерних засобів під час розслідування шахрайств, учинених із використанням мережі «Інтернет» [Tactical Considerations for Examining Computer Equipment During Investigations of Internet Fraud]. *Вісник*

Висновки. Цифрові сліди є специфічним різновидом криміналістично значущої інформації, механізм утворення якої істотно відрізняється від традиційних матеріальних слідів і зумовлений особливостями функціонування інформаційно-телекомунікаційних систем. Встановлено, що цифрові сліди формуються у процесі взаємодії людини, технічних засобів та цифрового середовища, характеризуються динамічністю, багатоканальністю існування, залежністю від технічних умов і можливістю дистанційного впливу, що об'єктивно ускладнює їх виявлення, вилучення та фіксацію.

Обґрунтовано, що зазначені властивості цифрових слідів детермінують необхідність формування спеціалізованих підходів до тактико-криміналістичного забезпечення їх збирання, які мають інтегрувати процесуальні, технічні та тактичні елементи. Встановлено, що ефективність виявлення цифрових слідів залежить від здатності ідентифікувати не лише матеріальні носії інформації, а й логічні середовища їх існування, зокрема мережеві ресурси, облікові записи та хмарні сервіси.

Доведено, що вилучення цифрових слідів має здійснюватися з урахуванням принципу незмінності інформації та передбачає використання спеціалізованих технічних засобів, зокрема методів криміналістичного копіювання, а також врахування ситуаційних чинників, пов'язаних із технічним станом пристроїв, рівнем їх захисту та ризиками дистанційного втручання. При цьому особливого значення набуває забезпечення цілісності даних і недопущення їх модифікації.

Визначено, що фіксація цифрових слідів виходить за межі традиційного документування і передбачає комплексне відображення як змісту інформації, так і її технічних параметрів, включаючи метадані та характеристики програмного середовища. Встановлено, що застосування контрольних механізмів, зокрема гешування, є необхідною умовою забезпечення достовірності та допустимості цифрових доказів.

Обґрунтовано, що тактико-криміналістичне забезпечення роботи з цифровими слідами має виразну ситуаційну зумовленість і залежить від можливості попереднього планування слідчих (розшукових) дій. Доведено, що у випадках, коли існують умови для завчасної підготовки, забезпечується більш високий рівень організації процесу вилучення і фіксації цифрової інформації, зокрема шляхом належного технічного оснащення, забезпечення безперебійного живлення та наявності необхідних носіїв для копіювання даних.

Встановлено, що ефективність збирання цифрових слідів значною мірою залежить від належної організації взаємодії між слідчими, оперативними підрозділами, експертами та спеціалістами у сфері інформаційних технологій, що дозволяє комплексно вирішувати завдання їх виявлення, дослідження та використання у доказуванні.

Таким чином, доведено, що удосконалення тактико-криміналістичного забезпечення збирання цифрових слідів має здійснюватися шляхом розроблення уніфікованих тактичних алгоритмів, адаптованих до умов цифрового середовища, а також впровадження сучасних технічних засобів і стандартів роботи з електронними доказами, що забезпечить підвищення ефективності кримінального провадження в умовах цифровізації суспільства.

References

Cherniakhovskyi, B. V. (2020). Osoblyvosti provedennia slidchoho ohliadu pid chas rozsliduvannia nesanktsionovanoho vtruchannia v robotu kompiuteriv, avtomatyzovanykh system, kompiuternykh merezh chy merezh elektrozviazku [Specifics of Conducting a Forensic Examination During the Investigation of Unauthorized Interference with Computers, Automated Systems, Computer Networks, or Telecommunications Networks]. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav*. № 2. S. 58-68 [in Ukrainian].

Hrynko, L. P. (2025). Taktychni osoblyvosti ohliadu kompiuternykh zasobiv pid chas rozsliduvannia shakhraistv, uchynenykh iz vykorystanniam merezhi «Internet» [Tactical Considerations for Examining Computer Equipment During Investigations of Internet Fraud]. *Visnyk Penitentsiarnoi asotsiatsii Ukrainy*. № 3. S. 152–159. DOI: https://doi.org/10.34015/2523-4552.2025.3.17. [in Ukrainian].

Kalancha, I. H. (2025). Orhanizatsiini aspekty roboty z dokazamy, shcho maiut elektronnu formu v kryminalnomu protsesi Ukrainy [Organizational Aspects of Handling Electronic Evidence in Criminal Proceedings in Ukraine]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*. Seriia: Pravo. T. 4, № 90. S. 263. DOI: https://doi.org/10.24144/2307-3322.2025.90.4.36 [in Ukrainian].

Kalancha, I. H. (2025). Orhanizatsiini aspekty roboty z dokazamy, shcho maiut elektronnu formu v kryminalnomu protsesi Ukrainy [Organizational Aspects of Handling Electronic Evidence in Criminal Proceedings in Ukraine]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*. Seriia: Pravo. 2025. T. 4, № 90. S. 263. DOI: https://doi.org/10.24144/2307-3322.2025.90.4.36. [in Ukrainian].

Karaman, K. V. (2025). Vyiavlennia tsyfrovykh slidiv: osoblyvosti y alhorytm [Detection of Digital Traces: Characteristics and Algorithm]. *Visnyk Kharkivskoho natsionalnoho universytetu vnutrishnikh sprav*. T. 110. № 3. S. 141-150. [in Ukrainian].

Пенітенціарної асоціації України. 2025. № 3. С. 157. DOI: https://doi.org/10.34015/2523-4552.2025.3.17.

Nikishev, O. V. (2025). Tsyfrovi (elektronni) dokazy u kryminalnomu provadzhenni v umovakh nadzvychainykh pravovykh rezhymiv [Digital (electronic) evidence in criminal proceedings under states of emergency]. *Pravo.ua*. № 1. S. 365-371. https://doi.org/10.71404/law.ua.2025.1.54 [in Ukrainian].

Romaniuk, V. V., Fomina, T. H. (2024). Poriadok zbyrannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh pro kolaboratsiinu diialnist [Procedures for Collecting Electronic (Digital) Evidence in Criminal Proceedings Concerning Collaboration]. *Visnyk Kryminolohichnoi asotsiatsii Ukrainy*. T. 32. № 2. S. 344-353. [in Ukrainian].

Serhieieva, D. B. (2025). Vyiavlennia i dokumentuvannia sposobiv uchynennia sluzhbovykh pravoporushen: metodyka, taktyka, tsyfrovi slidy ta lantsiuh zberezhennia dokaziv [Identifying and Documenting Methods of Committing Workplace Misconduct: Methods, Tactics, Digital Traces, and the Chain of Evidence]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*. Seriia: Pravo. T. 4. № 91. S. 438-451. [in Ukrainian].

Shchyruk, M. M. (2026). Zmahalnist i «iakist» dokaziv u spravakh pro roztratu ta pryvlasnennia: kryminalistychni mekhanizmy advokatskoho zakhystu [Adversarial Proceedings and the "Quality" of Evidence in Cases of Embezzlement and Misappropriation: Forensic Mechanisms of Legal Defense]. *Analitychno-porivnialne pravoznavstvo*. T. 3. № 1. S. 468-476. [in Ukrainian].

Vuima, A. (2025). Tsyfrovyi vymir suchasnoi zlochynnosti: kiberprostir yak typova obstanovka vchynennia kryminalnykh pravoporushen [The Digital Dimension of Modern Crime: Cyberspace as a Common Setting for Criminal Offenses]. *Arkhiv kryminolohii ta sudovykh nauk*. T. 12, № 2. S. 64–70. DOI: https://doi.org/10.32353/acfs.12.2025.05. [in Ukrainian].

Надійшла до редколегії: 16.03.2026 / Рецензовано 27.04.2026 / Прийнято до друку 29.04.2026 / Доступно онлайн 30.05.2026

Приклад цитування:

Караман, К. (2026). Залучення спеціаліста під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку. *Архів кримінології та судових наук*. 1 (13). 68-75. DOI: https://doi.org/10.32353/acfs.13.2026.04