УДК [351/75:324:342.9](477)
DOI https://doi.org/10.24144/2307-3322.2026.93.5.13

ПРО КРИМІНАЛІСТИЧНІ МЕТОДИ ВИЯВЛЕННЯ ТА ФІКСАЦІЇ ЦИФРОВИХ СЛІДІВ ВІД КІБЕРЗЛОЧИНІВ

Крижановський А.С.,
кандидат юридичних наук, доцент,
доцент кафедри міжнародного та кримінального права,
Навчально-науковий інститут права,
психології та інноваційної освіти,
Національний університет «Львівська політехніка»
ORCID: 0000-0002-2432-5285

Кравець В.С.,
здобувачка вищої освіти,
Навчально-науковий інститут права,
психології та інноваційної освіти
Національний університет «Львівська політехніка»
ORCID - 0009-0002-7952-6904
e-mail: viktoriia.kravets.pv.2022@lpnu.ua

Крижановський А.С., Кравець В.С. Про криміналістичні методи виявлення та фіксації цифрових слідів від кіберзлочинів.

У сучасному інформаційному суспільстві кіберзлочини набувають все більшої поширеності та різноманітності, що зумовлює необхідність удосконалення криміналістичних методів їх виявлення та розслідування. У статті досліджено криміналістичну характеристику кіберзлочинів та особливості роботи з цифровими слідами в умовах стрімкої цифровізації суспільства. Визначено поняття кіберзлочину відповідно до законодавства України та положень Будапештської конвенції про кіберзлочинність. Проаналізовано основні елементи криміналістичної характеристики кіберзлочинів, зокрема способи їх учинення, типові цифрові сліди та відмінність цифрових слідів від матеріальних. З'ясовано, що цифрові сліди мають нематеріальний характер і можуть зберігатися на різних носіях і легко змінюватися чи видалятися, що вимагає застосування спеціалізованих технічних засобів і процедур фіксації. Розглянуто сучасні методи виявлення та аналізу цифрових доказів: використання OSINT (розвідки з відкритих джерел), геш-функцій, метаданих і програмного забезпечення криміналістичного призначення («X-Ways Forensics», «Cellebrite UFED Touch 2» тощо). Також зосереджено увагу на дотриманні міжнародних стандартів, зокрема ДСТУ ISO/IEC 27037:2017, що регламентує процес ідентифікації, збирання та збереження цифрових доказів. Проаналізовано норми Кримінально процесуального кодексу України щодо фіксації електронних доказів і наведено позицію Європейського суду з прав людини у справі *Khan v. the United Kingdom*, відповідно до якої допустимість цифрових доказів залежить не лише від законності їх отримання, а й від забезпечення справедливості судового процесу. На останок розглянуто сучасні методи виявлення, фіксації та збереження цифрових доказів, включно з аналізом комп'ютерних та мережевих слідів, логів, електронної пошти, баз даних та інтернет-трафіку. Дослідження обґрунтовує важливість інтегрованого підходу, що поєднує юридичну, технічну та процесуальну складові, для ефективного розслідування кіберзлочинів, а також доводить важливість дотримання порядку роботи з цифровими слідами, для подальшого їх використання як доказів у кримінальному провадженні.

Ключові слова: кіберзлочини, цифрові сліди, криміналістична характеристика, цифрові докази, OSINT, геш-функція, кримінальне провадження, фіксація доказів.

Kryzhanovskyi A.S., Kravets V.S. On criminalistic methods for detecting and recording digital traces of cybercrimes.

In today's information society, cybercrimes are becoming increasingly widespread and diverse, necessitating the improvement of forensic methods for their detection and investigation. The article examines the forensic characteristics of cybercrimes and the peculiarities of working with digital traces in the context of rapid digitalization of society. The concept of cybercrime is defined in accordance with Ukrainian legislation and the provisions of the Budapest Convention on Cybercrime. The main elements of the forensic characteristics of cybercrimes are analyzed, in particular, the methods of their commission, typical digital traces, and the difference between digital and material traces. It has been established that digital traces are intangible, can be stored on various media, and can be easily altered or deleted, which requires the use of specialized technical means and recording procedures. Modern methods of detecting and analyzing digital evidence are considered: the use of OSINT, hash functions, metadata, and forensic software. It also focuses on compliance with international standards, in particular DSTU ISO/IEC 27037:2017, which regulates the process of identifying, collecting, and preserving digital evidence. The norms of the Criminal Procedure Code of Ukraine regarding the recording of electronic evidence are analyzed, and the position of the European Court of Human Rights in the case of Khan v. the United Kingdom is presented, according to which the admissibility of digital evidence depends not only on the legality of its acquisition, but also on ensuring the fairness of the judicial process. Finally, modern methods of detecting, recording, and preserving digital evidence are considered, including the analysis of computer and network traces, logs, e-mail, databases, and Internet traffic. The study substantiates the importance of an integrated approach that combines legal, technical, and procedural components for the effective investigation of cybercrimes, and also proves the importance of complying with the procedure for working with digital traces for their further use as evidence in criminal proceedings.

Key words: cybercrime, digital traces, forensic characteristics, digital evidence, OSINT, hash function, criminal proceedings, evidence preservation.

Постановка проблеми. Стрімкий розвиток інформаційно-комунікаційних технологій призвів до появи нових форм злочинної діяльності, які здійснюються у цифровому середовищі. Кібернетичні злочини відзначаються високим рівнем латентності, анонімності та транснаціонального характеру, що ускладнює їх виявлення, розслідування та доведення доказової бази у суді. Традиційні криміналістичні підходи не завжди ефективні у цифровому просторі, адже електронні сліди є нематеріальними, легко змінюваними або видаляються протягом короткого часу. Це зумовлює необхідність розроблення й упровадження сучасних методів виявлення, фіксації та збереження цифрових доказів, які забезпечать їх достовірність і допустимість у кримінальному провадженні.

Метою статті є дослідження сутності криміналістичної характеристики кіберзлочинів, визначення особливостей цифрових слідів та аналіз сучасних методів їх виявлення, фіксації й збереження. Потребує обґрунтування щодо впровадження міжнародних стандартів у фіксації цифрових слідів під час їх криміналістичної експертизи та формування на цій основі рекомендацій, спрямованих на підвищення ефективності діяльності правоохоронних підрозділів у сфері боротьби з кібернетичною злочинністю.

Стан опрацювання проблематики. Проблематика криміналістичного дослідження кіберзлочинів перебуває у полі зору багатьох науковців, зокрема О. Довженко, О.В. Кузьменко, Є.Є. Демидової, В.О. Нороха, К.В. Караман, І.А. Колеснікова, Ю. Жданова, С. Спасітєлєва, С. Шевченко тощо. У їхніх працях досліджуються проблеми, пов'язані з характеристикою понять цифрових слідів, методи їх виявлення та вплив на формування доказової бази. Водночас залишається фрагментарно дослідженою уніфікація криміналістичних процедур роботи з цифровими доказами, практичне застосування міжнародних стандартів, таких як ДСТУ ISO/IEC 27037:2017, а також застосування європейського досвіду щодо забезпечення автентичності електронних доказів у національну криміналістичну практику.

Виклад основного матеріалу. Кіберзлочини сьогодні становлять одну з поширених та динамічних категорій кримінальних правопорушень, оскільки розвиток інформаційних технологій розширює можливості вчинення злочинів та ускладнює їх ідентифікацію. Цифровізація суспільства та розширення інформаційного простору є однією з умов розвитку суспільства, держави як у сфері публічного управління, так і в захисті громадян від посягань на їх права, свободи шляхом використання новітніх технологій у боротьбі зі злочинністю. Варто зазначити, що злочинці також

намагаються використовувати нові засоби і способи вчинення з метою досягнення протиправних результатів.

Варто детальніше розкрити роль цифровізації у поширенні кіберзлочинності, тому що саме вона стає інструментом вчинення злочинів зі сторони асоціальних осіб, дії яких спрямовані на заволодіння даними, які зберігаються в електронному вигляді. Чим більше персональної, фінансової та корпоративної інформації стає доступною у режимі онлайн, тим привабливішою вона є для зловмисників. На жаль, Інтернет надає можливість віддалених атак та анонімних дій, що ускладнюють виявлення і притягнення до відповідальності кіберзлочинців. Швидкий розвиток технологій та складність сучасних інформаційних систем дозволяють злочинцям використовувати інструменти шифрування, VPN та анонімайзери для приховування слідів. Зазначимо, що багато організацій і користувачів інформації не впроваджують достатніх заходів кібербезпеки, що створює вразливості для несанкціонованого до них доступу. Крім того, поширення цифрових платформ і сервісів у фінансах, державних послугах, освіті та медицині збільшує загальну ймовірність кібератак, а їх вчинення суттєво ускладнює криміналістичне дослідження кіберзлочинів через труднощі у доступі до доказів. Цифрові сліди часто розподілені між різними пристроями, серверами та хмарними сховищами, що ускладнює їх виявлення та фіксацію. Використання сучасних технологій шифрування та захисту даних створює додаткові бар'єри для експертів і слідчих. Крім того, віддалені атаки та анонімні дії злочинців зменшують можливість безпосередньо пов'язати конкретну особу з протиправними діями. Внаслідок цього криміналістичне дослідження кіберзлочинів потребує застосування спеціалізованих методів збору, збереження та аналізу цифрових доказів, які гарантують їхню допустимість розгляду у суді та забезпечують достовірність висновків експерта.

Характеристика сутності поняття кіберзлочину є однією з умов його правозастосування у сфері криміналістичної експертизи. Так, у рішеннях Конгресу ООН до ***кіберзлочину*** відносять будь-яке правопорушення, що здійснюється за допомогою комп'ютерної системи чи мережі, а також відбувається в їх межах та спрямоване проти них. Іншими словами, на думку Довженко О. кіберзлочинами вважаються будь-які протиправні діяння, що вчиняються в електронному середовищі. До основних ознак кіберзлочинів належать: використання інформаційно-комунікаційних технологій, високий ступінь анонімності та віддаленість у часі і просторі між місцем скоєння злочину і його наслідками [1, с. 81]. Відповідно до п. 8 ч. 1. ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» ***кіберзлочин (комп'ютерний злочин)*** – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

Підтримуючи в цілому дане визначення кіберзлочину зазначимо, що законодавство України так само як Будапештська Конвенція проти кіберзлочинності (2001 р.) містить перелік правопорушень, які можна віднести до категорії кіберзлочинів. До них належать: несанкціонований доступ до комп'ютерної інформації (ст. 361-362 КК України); комп'ютерне шахрайство (ст. 190, 361 КК України); незаконне зберігання, виготовлення та розповсюдження шкідливого програмного забезпечення (ст.361-361-1 КК України); порушення авторських і суміжних прав у цифровому середовищі (ст. 176-177 КК України); поширення забороненої інформації (ст. 301, 156 КК України) [3]. Крім того, Будапештська конвенція про кіберзлочинність відносить до кіберзлочинів: злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; комп'ютерне шахрайство; злочини, пов'язані з дитячою порнографією та незаконне використання криптографічних та мережевих технологій [4]. Шляхом врахування форм та класифікації правопорушень у криміналістичній практиці стає можливим формування методів їх виявлення, фіксації та документування, що є основою для належної доказової бази під час кримінального провадження.

Наявність криміналістичної характеристики та класифікації кіберзлочинів служить практичним інструментом, для кращого розуміння та розслідування кіберзлочинів. На думку О.В. Кузьменко, криміналістична характеристика є систематизованим описом об'єкта чи явища криміналістики з метою дослідження, розкриття та розслідування злочинів. Вона поєднує юридичні, технічні та процесуальні аспекти і використовується для встановлення конкретних ознак злочину, способів його вчинення та доказів [5, с. 162-163]. Ці складові криміналістичної характеристики є тотожними по відношенню до кіберзлочинів, саме тому, що вона включає: типи та способи вчинення злочину у цифровому середовищі, специфіку цифрових слідів та інформаційних сис-

тем, методи їх збору, збереження і аналіз, оцінку доказової сили та допустимості отриманих матеріалів у кримінальному провадженню. Отже, криміналістична характеристика кіберзлочинів передбачає визначення специфіки цифрових слідів та способів їх виявлення. Саме вона дозволяє систематизувати знання про типові способи вчинення таких злочинів, їх основні ознаки, особливості поведінки правопорушників, характер слідів, що залишаються у цифровому середовищі та механізми їх утворення.

Характеристика кіберзлочинів потребує розгляду цифрових слідів, які являються об'єктом криміналістичного дослідження при їх розслідуванні та виявленні. Цифрові сліди в криміналістичній практиці розглядаються як будь-які сліди діяльності або взаємодії особи з цифровими засобами, що можуть бути використані як доказ у кримінальному провадженні. У науковій літературі існують різні підходи до їх визначення. Демидова Є. Є. зазначає, що терміни «електронні» та «цифрові» сліди є рівнозначними, проте дуалістична природа терміну може ускладнювати його розуміння. Використання поняття «віртуальні сліди», означає, що це цифрові образи або електронні сигнали, що зберігаються у пам'яті електронних пристроїв і мають кримінально-релевантне значення. Водночас цифрові сліди містять сукупність інформації про діяльність користувача у віртуальному просторі [6, с. 73]. Таким чином, цифрові сліди – це будь-які відомості, інформація або дані, що виникають або залишаються в електронних інформаційних системах, внаслідок використання цифрових засобів і технологій та можуть виступати джерелом доказів у судовому провадженні. Вони є ключовим елементом криміналістичної характеристики кіберзлочинів, оскільки саме вони дозволяють встановити фактичні обставини вчинення правопорушення, ідентифікувати правопорушника, визначити спосіб вчинення правопорушення та обсяг заподіяної шкоди.

Основним критерієм класифікації цифрових слідів, як слушно вважає Демидова Є.Є. є їх поділ за джерелом чи носієм їх збереження, сюди відносять: 1) внутрішні носії (дані в пам'яті пристрою: внутрішні диски, флеш-пам'ять мобільних та інші); 2) зовнішні носії (CD/DVD, USB, зовнішні HDD, флеш-карти); 3) сервера і хмара (лог-файли веб-сервісів, синхронізовані файли) [6, с. 74]. Зазначимо, що при цьому має місце відмінність цифрових слідів від традиційних, а саме матеріальних слідів. Цифрові сліди не лишаються на фізичних поверхнях, тобто їх можна побачити та виявити лише через пристрої та програмне забезпечення. Дані можуть зберігатися на багатьох пристроях і серверах одночасно, і дублювання файлів не змінює їх суті та є необмеженим. Тобто на відміну від матеріальних слідів, їх легко копіювати, змінювати та видаляти дистанційно, а також підробляти. Саме ця відмінність між ними ускладнює методи виявлення цих слідів, а також дослідження та збереження, що вимагає запровадження спеціалізованих інструментів, цифрового обладнання та спеціально навчених спеціалістів, тому що звичайні методи криміналістики тут неефективні.

Складовою нашого дослідження є методи виявлення та фіксації цифрових слідів. Вони є ключовим елементом криміналістичної характеристики кіберзлочинів, адже від правильності їх застосування залежить достовірність і допустимість отриманих доказів у кримінальному провадженні. Кримінально процесуальний кодекс України (далі КПК України) на жаль не містить норм, які регулювали процедуру роботи з цифровими доказами, як окремим видом доказування, тому це значно ускладнює діяльність правоохоронців та інших суб'єктів, які працюють з цими доказами. У такому випадку з'являється необхідність звертатися до міжнародних стандартів та практики. Це стосується положень ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» [7]. Зазначений стандарт містить методичні рекомендації щодо пошуку, розпізнавання, документування та збереження цифрових об'єктів, що можуть бути використані як докази у кримінальному провадженні. Дотримання положень ДСТУ ISO/IEC 27037:2017 забезпечує допустимість цифрових доказів у кримінальному процесі, оскільки підтверджує належну фіксацію, збереження та захист інформації. Крім того, використання цього стандарту сприяє уніфікації процедур між різними слідчими органами та експертними установами, що, у свою чергу, підвищує результативність та якість проведення розслідувань.

Особливе місце серед сучасних методів виявлення посідає OSINT, або розвідка з відкритих джерел. OSINT (Open Source Intelligence) – є сучасним методом збору та аналізу інформації з відкритих джерел, що активно використовується у сфері кібербезпеки та розслідування кіберзлочинів. У криміналістичному аспекті OSINT застосовується для виявлення та аналізу цифрових слідів, зокрема інформації із соціальних мереж, відкритих веб-ресурсів, форумів, реєстрів та пу-

блічних баз даних. Використання OSINT сприяє ідентифікації осіб, встановленню зв'язків між учасниками протиправної діяльності та з'ясуванню способів учинення кіберзлочинів. Отримана з відкритих джерел інформація за умови належної процесуальної фіксації та дотримання вимог кримінального процесуального законодавства може набувати статусу цифрового доказу у кримінальному провадженні [8, с. 13-16]. Його застосування у криміналістиці дозволяє виявляти потенційно важливі цифрові сліди, що відображають злочинну діяльність або її наслідки. Отримані дані можуть бути використана як доказ у суді, за умови дотримання правил підтвердження автентичності та незмінності даних (наприклад, через обчислення геш-значень та збереження метаданих). Результати OSINT доцільно розглядати як документи у розумінні ст. 99 КПК України, які підлягають процесуальній фіксації у протоколі із доданням скриншотів, фото- чи відеоматеріалів та інших носіїв інформації (у тому числі комп'ютерних даних) [9, с. 146].

Серед способів виявлення та збереження цифрових слідів, важливе місце належить хеш-функції. У науковій публікації «Прикладні та методичні аспекти застосування хеш-функцій в інформаційній безпеці» наголошується, що хеш-функції є фундаментальним елементом сучасних механізмів забезпечення цілісності та безпеки даних у цифрових системах. Хеш-функція перетворює довільний вхідний масив даних у фіксований бітовий масив (хеш-код), який не тільки стискає інформацію, а й дозволяє ефективно контролювати її цілісність та достовірність. Використання алгоритмів хешування властиве для вирішення таких задач, як: ефективне зберігання та пошук даних у масивах і базах даних, захист паролів при автентифікації, формування електронного цифрового підпису та контроль важливих цифрових файлів. Автори також розглядають алгоритмічні аспекти хешування, включаючи їх практичне застосування за допомогою криптографічних служб і програмних інструментів, що є важливими для підготовки фахівців із інформаційної безпеки. Отриманий огляд підкреслює необхідність систематичного вивчення хеш-функцій у сфері кібербезпеки як засобу забезпечення надійного функціонування сучасних інформаційно-комунікаційних систем [10, с. 89-91]. Зазначимо, що застосування хеш-функцій є одним із ключових способів підтвердження цілісності цифрових об'єктів. В Україні цей метод використовують у межах криміналістичних експертиз, проте для всіх цифрових доказів варто запровадити стандартизовану практику розрахунку хеш-функцій та фіксації метаданих на всіх етапах слідчих дій.

До спеціалізованих засобів виявлення та аналізу цифрових слідів кримінальних правопорушень відносять: 1) експертне програмне забезпечення для криміналістичного дослідження комп'ютерних носіїв інформації, наприклад «X-Ways Forensics», «EnCase Forensic», «Belkasoft Evidence Center», «Forensic Toolkit»; 2) мобільні комплекси, що дозволяють добувати, декодувати та аналізувати цифрову інформацію, отриману з мобільних пристроїв, зокрема «MSAB XRY Field», «MOBILedit Forensic Express Pro», «Cellebrite UFED Touch 2»; 3) програмне забезпечення з відновлення комп'ютерних даних «UFS Explorer», «RStudio» тощо [11, с. 474]. Зазначені програмні засоби не є універсальними інструментами пошуку інформації, а становлять спеціалізоване програмне забезпечення, розроблене фахівцями у сфері цифрової криміналістики та кібербезпеки з урахуванням вимог кримінального процесу. Їх призначення полягає не лише у швидкому виявленні цифрових слідів, а насамперед у забезпеченні збереження цілісності, автентичності та відтворюваності цифрових даних. Таке програмне забезпечення дозволяє здійснювати аналіз комп'ютерних і мобільних носіїв, відновлення видалених файлів, дослідження метаданих і логів, а також автоматичну фіксацію хеш-значень, що є необхідною умовою допустимості цифрових доказів у кримінальному провадженні.

Належне виявлення та збереження цифрових слідів є ключовим для їх доказової сили. Всі операції мають супроводжуватися обчисленням хеш-функцій і веденням ланцюга збереження доказів, що гарантує їх цілісність та допустимість у суді. Цифрові сліди мають транзитний і швидкоплинний характер: дані можуть автоматично перезаписуватися, кешуватися, видалятися або розподілятися між серверами різних юрисдикцій. Це створює ризик втрати доказів, якщо їх не зафіксовано своєчасно. Для мінімізації таких ризиків застосовуються оперативні алгоритми реагування, стандартизовані процедури звернення до провайдерів послуг та технічні засоби для моментального вилучення й фіксації даних.

Забезпечення достовірності цифрових доказів вимагає суворого дотримання наступних процедур: використання сертифікованого програмного забезпечення, хронологічне документування всіх дій експерта, уникнення модифікації оригінальних даних та контроль за ланцюгом зберігання доказів. Важливою складовою є також оцінка надійності джерел інформації та встановлення

причетності конкретних осіб до кіберзлочину через аналіз метаданих, IP-адрес, логінів та інших цифрових слідів. Таким чином, криміналістичне дослідження кіберзлочинів поєднує юридичну, технічну та процесуальну складові, що дозволяє не лише виявити та задокументувати злочин, а й забезпечити ефективність його розслідування та доказової сили у суді. Оптимізація методів виявлення та фіксації цифрових слідів підвищує результативність роботи правоохоронних органів, а також сприяє захисту прав і свобод громадян у цифровому середовищі. Важливим є аналіз фіксації цифрових слідів, як доказів для подальшого їх використання у кримінальному провадженні.

Відповідно до положень КПК України, фіксація доказів є однією з ключових стадій процесу доказування. Згідно зі статтею 99 КПК України, доказами у кримінальному провадженні є фактичні дані, отримані у передбаченому законом порядку, на підставі яких встановлюються наявність чи відсутність обставин, що мають значення для кримінального провадження [12]. До таких доказів належать речові та електронні (цифрові) докази, отримані з інформаційних систем, носіїв чи мереж. Згідно зі статтею 100 КПК України, порядок зберігання речових доказів, документів та електронних носіїв інформації визначається з урахуванням їхніх властивостей та з метою забезпечення цілісності й автентичності інформації [12]. При цьому орган досудового розслідування зобов'язаний вжити заходів для недопущення пошкодження, зміни або знищення електронних даних, що можуть мати доказове значення.

Однією з головних проблем, що виникають під час фіксації цифрових доказів, є забезпечення їхньої автентичності та допустимості. Оскільки цифрова інформація може бути легко змінена або знищена, надзвичайно важливо дотримуватися процесуальних вимог до збору, копіювання, зберігання та передавання таких доказів. Відповідно до практики Європейського суду з прав людини (ЄСПЛ), зокрема, у справі Khan v. the United Kingdom, допустимість цифрових доказів визначається не лише їх технічними характеристиками, а й дотриманням прав людини під час їх отримання. У контексті цифрових слідів справа Khan v. the United Kingdom демонструє, що навіть за наявності процедурних порушень при зборі електронних даних, вирішальним критерієм є не формальна законність, а вплив цих порушень на загальну справедливість процесу. Такий підхід є особливо актуальним для сучасного цифрового середовища, де збирання електронних доказів часто супроводжується ризиком втручання у приватне життя особи. ЄСПЛ наголошує, що держава повинна забезпечити чіткі та передбачувані правові механізми для збору, зберігання та використання цифрових доказів, аби уникнути свавільного втручання у сферу приватності [13]. Справа Khan v. the United Kingdom може бути застосована у національній практиці для обґрунтування необхідності оцінювати допустимість цифрових слідів не лише за формальними критеріями законності, а й з огляду на загальну справедливість провадження. Отже, навіть якщо цифрові дані отримані з певними процедурними недоліками, вони можуть бути використані у суді, якщо не порушують права сторін на змагальність, рівність і справедливий розгляд справи.

Караман К. В. окреслив та вділив певний алгоритм виявлення цифрових слідів, який узгоджується з вимогами криміналістичної тактики та положеннями міжнародних стандартів, зокрема ДСТУ ISO/IEC 27037:2017. Процес роботи з цифровими доказами він розділив на декілька послідовних етапів, щоб зберегти їх цілісність та забезпечити достовірність та допустимість для подальшого їх використання у судовому провадженні. Ці етапи поділені наступним чином: 1) виявлення потенційних цифрових об'єктів; 2) фіксація виявленої інформації; 3) підтвердження цілісності та достовірності цифрової інформації; 4) збереження та передача даних; 5) процесуальне оформлення отриманих матеріалів [9, с. 146-147].

Зазначимо, що усі виявлені цифрові об'єкти підлягають обов'язковому документуванню з характеристикою джерела їх походження та обставин виявлення. Якщо слідчий або детектив не має достатнього рівня технічної підготовки, доцільним є залучення спеціаліста. Його участь забезпечує кваліфіковану технічну підтримку під час роботи з цифровою інформацією. Другим етапом є фіксація виявленої інформації, що полягає у складанні процесуального протоколу, в якому детально відображаються всі дії, пов'язані з виявленням, вилученням і збереженням цифрових слідів. Доцільним є застосування додаткових способів фіксації – долучення електронних носіїв із копіями виявлених даних. Це забезпечує можливість повного відтворення проведених дій і перевірки їх достовірності. Для перевірку цілісності та автентичності цифрової інформації проводиться обчислення та фіксація хеш-функцій (геш-значень), збереження метаданих та інших технічних характеристик, що підтверджують відсутність змін або пошкоджень у файлах. Втрата або модифікація цифрового об'єкта може поставити під сумнів його доказову цінність, тому дотри-

мання вимог цілісності є критично важливим. Завершальним етапом є процесуальне оформлення отриманих матеріалів. Цифрові сліди включаються до системи доказування шляхом визнання їх документами відповідно до ст. 99 КПК України [12].

Ефективне використання цифрових слідів у кримінальному провадженні можливе лише за умов чіткого дотримання послідовних процедур – від їх виявлення та фіксації до забезпечення автентичності та належного процесуального оформлення. Дотримання національних процесуальних норм разом із міжнародно-правовими стандартами дозволяє цифровим доказам набути повноцінного статусу, забезпечуючи їх допустимість у суді та поєднуючи ефективність кримінального переслідування з дотриманням загальних засад кримінального провадження.

З метою підвищення ефективності правоохоронної діяльності у сфері розслідування кіберзлочинів доцільно оптимізувати процес криміналістичної експертизи цифрових доказів. Насамперед варто забезпечити уніфікацію процедур їх виявлення, фіксації та дослідження відповідно до міжнародних стандартів, зокрема до ДСТУ ISO/IEC 27037:2017. Адже, запровадження єдиних норм і стандартів роботи з цифровими слідами в Україні сприятиме уніфікації діяльності слідчих, експертів і спеціалістів, мінімізації процесуальних і технічних помилок, а також усуненню неоднозначного тлумачення порядку роботи з цифровими доказами. Це, в свою чергу підвищить ефективність досудового розслідування та забезпечить допустимість цифрових слідів у кримінальному провадженні.

Необхідним також є розширення спеціалізованих підрозділів цифрової криміналістики, оснащених сертифікованим програмним забезпеченням. Використання цих засобів забезпечує точність аналізу, збереження цілісності інформації та оперативність отримання результатів експертизи та цифрових доказів. Суттєве значення має підготовка кадрів – слідчих, експертів, прокурорів – у сфері цифрової криміналістики та кібербезпеки. Проведення регулярних навчань і підвищення кваліфікації сприятиме зменшенню кількості помилок під час збору та дослідження цифрових доказів. Також актуальним є удосконалення положень КПК України з метою чіткого регулювання порядку роботи з електронними доказами, як окремим видом доказів. Реалізація зазначених рекомендацій має на меті підвищення ефективності криміналістичної експертизи цифрових доказів, сприятиме захисту прав громадян у кіберпросторі та створенню цілісної системи цифрової криміналістики, здатної швидко відповідати на виклики сучасного інформаційного суспільства.

Висновки. Проведене дослідження показало, що цифрові сліди є не допоміжним, а центральним елементом доказування у справах про кіберзлочини. Саме вони дозволяють відтворити механізм вчинення правопорушення, встановити зв'язок між діями в цифровому середовищі та конкретною особою, а також підтвердити обсяг і характер завданої шкоди. Водночас їх нестабільний і нематеріальний характер зумовлює підвищені вимоги до порядку роботи з такими даними. Дослідження показало, що ключовим чинником ефективності розслідування кіберзлочинів є не лише наявність технічних засобів, а насамперед чітко визначений і уніфікований алгоритм дій під час виявлення, фіксації та збереження цифрових слідів. Дотримання такого алгоритму, заснованого на міжнародних стандартах і процесуальних гарантіях, зменшує ризик помилок, втрати доказів і сумнівів щодо їх допустимості. Отже, важливим є необхідність переходу від часткового використання окремих технічних інструментів до системного підходу в роботі з цифровими доказами. Саме стандартизація процедур і належна підготовка фахівців створюють передумови для формування сталої та ефективної практики розслідування кіберзлочинів у сучасному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Довженко О. Поняття кіберзлочину з криміналістичної позиції. *Трибуна молодого вченого. Юридичний вісник*. № 3. 2018 С. 79-83. URL: http://yurvisnyk.in.ua/v3_2018/14.pdf.
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 30.11.2025).
3. Кримінальний кодекс України : Закон від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 30.11.2025).
4. Конвенція про кіберзлочинність Рада Європи: Міжнародний документ від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 30.11.2025).

5. Кузьменко О.В. Особливості криміналістичної характеристики кіберзлочинів. *Актуальні проблеми вітчизняної юриспруденції* № 4. 2022. С. 162-166. URL: http://apnl.dnu.in.ua/4_2022/4_2022.pdf#page=162.
6. Демидова Є.Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського Національного Університету*, Серія ПРАВО. Випуск 85: частина 4. 2024. С. 71-75. DOI https://doi.org/10.24144/2307-3322.2024.85.4.10.
7. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. На заміну ДСТУ ISO/IEC 27037:2016; чинний від 2019-01-01. Вид. офіц. Київ: УкрНДНЦ, 2018.
8. Нороха, В.О. Метод структурування та збору даних за допомогою технології OSINT: кваліфікаційна робота бакалавра за спеціальністю 125 «Кібербезпека». Чернігівський національний університет «Чернігівська політехніка», Чернігів. 2023. 57 с. URL: http://ir.stu.cn.ua/handle/123456789/29390.
9. Караман К. В. Виявлення цифрових слідів: особливості й алгоритм. *Вісник ХНУВС*. № 3. 2025. С. 141-150. DOI: https://doi.org/10.32631/v.2025.3.12.
10. Жданова Ю., Спасітєлєва С., Шевченко С. Прикладні та методичні аспекти застосування хеш-функцій в інформаційній безпеці. *Кібербезпека: освіта, наука, техніка, 4*(8), 2025. С. 85–96. DOI: https://doi.org/10.28925/2663-4023.2020.8.8596.
11. Колеснікова І.А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал*. 2023. С. 472–475. DOI https://doi.org/10.32782/2524-0374/2023-10/114.
12. Кримінальний процесуальний кодекс України: Закон, Кодекс від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 30.11.2025).
13. Khan v. the United Kingdom: Judgment of 12 May 2000, *HUDOC*. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58841%22]} (дата звернення: 30.11.2025).

Дата першого надходження рукопису до видання: 4.02.2026
Дата прийняття до друку рукопису після рецензування: 20.02.2026
Дата публікації: 5.03.2026