УДК 343.9
DOI https://doi.org/10.32782/chern.v6.2023.27

Є. Ю. Колосовський
кандидат юридичних наук,
завідувач кафедри кримінального судочинства та аналітичної діяльності
Державного податкового університету
orcid.org/0009-0007-5720-6367

Ю. В. Якубівська
студентка IV курсу
Навчально-наукового інституту економічної безпеки та митної справи
Державного податкового університету
orcid.org/0009-0009-6263-4272

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ЦИФРОВОЇ КРИМІНАЛІСТИКИ: ПРОБЛЕМИ ТЕОРІЇ І ПРАКТИКИ

У статті досліджено значення цифрової криміналістики в умовах стрімкого технологічного розвитку та зростання цифрових злочинів, звернено увагу на вивчення, розкриття та запобігання цифровим злочинам, підкреслюючи потребу постійного оновлення знань криміналістів. Обговорено теоретичні та практичні виклики, включаючи визначення предметної області та обробку швидкозростаючої кількості цифрових даних.

Зазначено, що розвиток цифрових технологій створює нові можливості для злочинців та виклики для цифрових криміналістичних експертів. Визначено напрями майбутнього розвитку галузі, такі як розробка нових методів дослідження, впровадження стандартів та підготовка кваліфікованих кадрів. Виокремлено тезу щодо нестачі фахівців у цій сфері.

Публікація ґрунтується на дослідженнях вітчизняних та іноземних учених, ретельно вивчаючи особливості галузі та шляхів вирішення викликів. Проаналізовано цифрові докази, їх унікальні властивості та важливість правильної обробки для допустимості в суді. Приділено увагу міжнародним стандартам та розвитку цифрової криміналістики в Україні, зокрема створенню спеціального підрозділу для боротьби з кіберзлочинністю.

Сформульовані перспективи подальших досліджень, включаючи роботу над вдосконаленням методів дослідження, створення єдиної системи стандартів та вирішення проблеми нестачі кваліфікованих фахівців у галузі цифрової криміналістики. Рекомендації, наведені в заключній частині статті, можуть служити основою для подальшого розвитку цифрової криміналістики в Україні, включаючи підвищення кваліфікації фахівців та активізацію інтеграції в європейський правовий простір. Розробка та впровадження передових технологій обробки цифрових доказів, враховуючи їхню динамічність, також є ключовим аспектом подальших досліджень.

Ключові слова: цифрова криміналістика, цифрові докази, цифрові сліди, технологічний прогрес, методи дослідження.

Kolosovskyi Ye. Yu., Yakubivska Yu. V. **PECULIARITIES OF DIGITAL FORENSICS APPLICATION: PROBLEMS OF THEORY AND PRACTICE**

The article examines the importance of digital forensics in the context of rapid technological development and the growth of digital crimes. It focuses on the study, detection and prevention of digital crimes, emphasizing the need to constantly update the knowledge of forensic scientists. Theoretical and practical challenges are discussed, including defining the subject area and processing the rapidly growing amount of digital data.

The article points out that the development of digital technologies creates new opportunities for criminals and challenges for digital forensic experts. The author identifies areas of future development of the industry, such as the development of new research methods, the introduction of standards and the training of qualified personnel. The shortage of specialists in this field is noted.

The article is based on the research of domestic and foreign scholars, carefully studying the peculiarities of the industry and ways to solve the challenges. The author analyzes digital evidence, its unique properties and the importance of proper processing for its admissibility in court. Attention is paid to international standards and the development of digital forensics in Ukraine, including the creation of a special unit to combat cybercrime.

The article formulates prospects for further research, including work on improving research methods, creating a unified system of standards and addressing the shortage of qualified specialists in the field of digital forensics. The recommendations provided in the conclusion of the article can serve as a basis for further development of digital forensics in Ukraine, including professional development of specialists and intensification of integration into the European legal space. The development and implementation of advanced techniques for processing digital evidence, given its rapidly changing nature, is also a key aspect of further research.

Key words: digital forensics, digital evidence, technological progress, research methods.

Постановка проблеми. У період стрімкого технологічного розвитку, цифрове середовище трансформується не лише в платформу для інновацій та прогресу, але й у сферу, що включає численні ризики, асоційовані зі зловживаннями та порушеннями закону. Відповідно, цифрова криміналістика, як галузь, призначена для дослідження, розкриття та запобігання злочинам у цифровому

просторі, набуває значної актуальності. Цифрова криміналістика, будучи відносно новим напрямом, переживає стрімкий розвиток. Цей процес безпосередньо корелює зі зростанням ролі цифрових технологій у повсякденному житті. Унаслідок чого збільшення обсягу цифрових доказів у кримінальних справах висуває перед криміналістами, як науковцями, так і практиками, нові вимоги щодо знань та навичок. Паралельно з розвитком технологій виникають нові виклики та проблеми, які ставлять під сумнів існуючі теоретичні та практичні підходи в галузі цифрової криміналістики. Аналіз особливостей застосування цифрової криміналістики та висвітлення ключових проблем, що виникають у теоретичному та практичному аспектах даної дисципліни, є важливим завданням сучасних досліджень. Розробка нових методологій, інструментів та підходів до роботи з цифровими доказами становить ключову складову розвитку цифрової криміналістики, яка повинна адаптуватися до динамічно змінюваного цифрового середовища. Саме розгляд особливостей застосування цифрової криміналістики, висвітлення ключових проблемних аспектів, що виникають як у теоретиків, так і у практиків у даній галузі, є завданням, яке ми вбачаємо за доцільне розв'язати в цій публікації.

Аналіз останніх досліджень і публікацій. Питанням цифрової криміналістики у своїх працях приділяли увагу такі вчені та науковці, як: Г. К. Авдєєва, Н. М. Ахтирська, В. А. Журавель, А. Ю. Каламайко, А. В. Коваленко, О. Г. Козицька, А. С. Колодіна, І. О. Крицька, В. В. Мурадов, М. В. Нечипорук, Ю. Ю. Орлов, А. В. Ратнова, О. В. Ряшко, О. М. Сафонова, Г. А. Селютіна, В. М. Селютін, А. Ю. Стах, А. В. Столітній, С. В. Стороженко, Д. М. Цехан, С. С. Чернявський, В. Ю. Шепітько, М. В. Шепітько, Р. М. Шехавцов, Т. П. Яцик та інші. Також не можна не вказати на той факт, що однією з провідних іноземних дослідниць цифрової криміналістики є американська вчена Marie-Helen Maras [1, с. 9-18].

Мета статті полягає в узагальненні особливостей застосування цифрової криміналістики, розглядаючи проблеми, які виникають як у теоретичному, так і практичному аспектах цієї дисципліни. Важливо висвітлити актуальні питання, пов'язані з використанням цифрових технологій у сфері боротьби з кримінальною діяльністю, а також висунути пропозиції щодо подолання визначених труднощів у практиці та удосконалення теоретичних аспектів цифрової криміналістики.

Виклад основного матеріалу. Сучасний стан цифрової криміналістики характеризується зростанням кількості кіберзлочинів та розвитком нових цифрових технологій. У наукових публікаціях розглядаються окремі аспекти щодо питань збору та аналізу цифрових доказів інтелекту, а також особливостей міжнародного співробітництва в даній сфері. Водночас, невирішеними залишаються питання розробки єдиної системи стандартів, виокремлення проблем конфіденційності та забезпечення оперативності й ефективності розслідування кіберзлочинів.

Характеризуючи особливості цифрової криміналістики, слід зазначити, що вона включає методи збору, зберігання, аналізу та представлення цифрових даних для використання в судових процесах. Це може включати розслідування комп'ютерних систем, мереж, мобільних пристроїв та інших пристроїв, які мають здатність зберігати або передавати інформацію в цифровому форматі. Щодо визначення поняття «цифрова криміналістика», то єдності поглядів у науковому тлумаченні поки не досягнуто. Так А. С. Колодіна, Т. С. Федорова під цим поняттям розуміють «галузь криміналістики, яка займається дослідженням цифрових доказів у кримінальних провадженнях» [2, с. 176-180].

В. Ю. Шепітько та М. В. Шепітько зазначають, що цифрова криміналістика може розглядатись як стратегічний напрям у розвитку криміналістичної науки та правозастосовної практики [3, с. 12-27].

На думку К. Є. Борисова та В. А. Світличного, цифрова криміналістика –це новітня галузь криміналістики, яка займається збиранням, зберіганням та аналізом цифрових доказів. Вони можуть бути отримані з різних джерел, таких як комп'ютери, мобільні телефони, камери відеоспостереження та інші цифрові пристрої. Цифрова криміналістика є важливою галуззю, оскільки вона допомагає правоохоронним органам розслідувати злочини, які відбуваються в цифровому середовищі. Цифрова криміналістика – це важливий інструмент для боротьби зі злочинами, які відбуваються за допомогою цифрових технологій [4, с. 83-84].

Важливою теоретичною проблемою цифрової криміналістики є визначення її предметної області. На думку А. С. Колодіної та Т. С. Федорова, цифрова криміналістика часто розглядається як галузь криміналістики, що займається дослідженням цифрових доказів [2, с. 176-180]. Однак цифрові докази можуть бути різноманітними, включаючи інформацію з комп'ютерів, мобільних телефонів, соціальних мереж, інтернету та інших джерел. Це ускладнює визначення того, що саме є предметом дослідження цифрової криміналістики. Причому, зауважимо, що до найважливіших теоретичних проблем цифрової криміналістики слід віднести: ідентифікація цифрових доказів, яка ускладнюється їхньою модифікацією та знищенням; цілісність цифрових доказів, яка може порушуватися або змінюватися під час дослідже-

ня, призводячи до помилкових висновків; автентичність цифрових доказів, яка стає проблемою через можливість підроблення чи фальсифікації; оцінка доказової сили цифрових доказів, яка ускладнена їхньою неоднозначністю та складністю для розуміння.

Своєю чергою, однією з ключових практичних проблем цифрової криміналістики є швидке зростання кількості цифрових даних. Це ускладнює їх ефективне дослідження, оскільки фактично створюється ситуація, відповідно до якої стає доволі важко знайти потрібну інформацію серед величезної кількості даних.

Особливу увагу в цифровій криміналістиці приділяють виявленню та аналізу слідів цифрової активності, які можуть бути використані для встановлення фактів або для виявлення злочинної поведінки. Також важливою є здатність правильно інтерпретувати знайдені дані, враховуючи можливість маніпуляції ними або зміни. Цифрова криміналістика постійно розвивається відповідно до нових технологічних трендів та методів злочинної діяльності в цифровому просторі. Вона вимагає від спеціалістів глибоких знань в ІТ, а також розуміння правових аспектів збору та використання цифрових доказів.

Крім того, із розвитком цифрових технологій використання цифрових доказів стає все більш поширеними в кримінальних провадженнях. Цифрова криміналістика використовує широкий спектр інструментів і технологій для дослідження цифрових доказів. Не менш важливим є те, що цифрова криміналістика відіграє важливу роль у боротьбі з кіберзлочинністю.

Цікавим етапом у розвитку криміналістичної науки є формування та становлення цифрової криміналістики. Початкові дослідження в цьому напрямку відбулися у США та Великій Британії, де в 1970-х роках були створені перші підрозділи комп'ютерної криміналістики. Вже в 1980-ті роки у Великій Британії з'явився перший підручник з цифрової криміналістики. З поширенням інтернету та зростанням кількості кіберзлочинів у 1990-х роках ця галузь стрімко розвивалась, і були встановлені перші стандарти та методики. У XXI столітті цифрова криміналістика стала ключовою складовою криміналістики, оскільки цифрові докази стали невід'ємною частиною багатьох кримінальних проваджень. Сучасна цифрова криміналістика швидко розвивається, і тепер вчені та практики в цій сфері повинні постійно оновлювати свої знання та навички, відстежуючи останні тенденції і технології.

Важливими напрямами розвитку цифрової криміналістики в найближчому майбутньому стануть: розробка нових методів і методик дослідження цифрових доказів; впровадження стандартів цифрової криміналістики; підготовка кваліфікованих кадрів у галузі цифрової криміналістики; інтеграція цифрової криміналістики з іншими галузями; розвиток міжнародного співробітництва в галузі цифрової криміналістики.

Також можемо зауважити, що значною проблемою є і постійний розвиток нових технологій, які створюють нові можливості для злочинців і нові виклики для криміналістичних експертів. Як приклад, зростання використання хмарних обчислень ускладнює доступ до цифрових доказів.

Не можна не вказати і на той факт, що недостатня кількість кваліфікованих кадрів у галузі цифрової криміналістики також є актуальною проблемою. На нашу думку, криміналістичні експерти повинні мати змістовні знання в галузі комп'ютерної техніки, програмування, криптографії та інших інноваційних галузей. Однак ці навички не завжди є доступними для співробітників правоохоронних органів держави. Враховуючи вищевикладене, слід погодитись із думкою вчених, які вважають, що рішення практичних проблем цифрової криміналістики є важливим кроком для забезпечення ефективності боротьби з кіберзлочинністю. Для цього необхідним є виконання таких дій: розвиток навчальних програм із цифрової криміналістики; посилення співпраці між правоохоронними органами та науковими установами щодо розробки нових методів дослідження цифрових доказів; створення стандартів для зберігання та обміну цифровими доказами відносно забезпечення їхньої цілісності та автентичності.

Щодо питання характеристики цифрових доказів, то слід зазначити, що це є дані, які можуть бути використані як докази в кримінальному провадженні. Вони можуть бути отримані та використані для інформації в рамках досудового розслідування або представлені в суді [5].

Цифрові докази поділяються на прямі, що встановлюють факти, та непрямі, які роблять висновки. Перед використанням їх у суді, важливо розпізнати їхню відповідність передбачуваній меті, а їх унікальність порівняно з традиційними доказами створює складнощі в аутентифікації через обсяг, швидкість та вразливість.

Відповідної уваги заслуговують, на нашу думку, і цифрові сліди. Цифрові сліди – це дані, які люди залишають після використання інформаційно-комунікаційних технологій (ІКТ). Вони можуть містити інформацію про вік, стать, расу, національність, орієнтацію, думки, захоплення, звички, хобі, історію хвороби, психологічні розлади, статус, зайнятість, приналежність до спільноти, особисті відносини, геолокацію, розпорядок дня та інші активності особи [6].

Цифрові сліди слід класифікувати на активні та пасивні. Активні цифрові сліди створюються користувачем, наприклад, коли він залишає

коментарі в соціальних мережах, завантажує фотографії або відео, робить покупки в інтернеті. Пасивні цифрові сліди залишаються людиною ненавмисно, наприклад, коли вона переглядає відповідні веб сторінки, використовує пошукову систему або користується мобільним телефоном.

Цифрові сліди можуть використовуватися як докази скоєння злочину, у тому числі кіберзлочину. Вони можуть допомогти встановити особу злочинця, місце і час скоєння злочину, а також інші обставини справи. Наприклад, аналіз цифрових слідів може допомогти встановити, хто саме користувався певним пристроєм, коли і в якому місці були зроблені певні фотографії або відео, а також які сайти були відвідані [7, с. 464]. Цифрові сліди можуть бути також використані для відстеження руху злочинця, виявлення злочинних схем і навіть для відновлення інформації, яка була видалена або зашифрована. Цифрові сліди зберігаються на різних пристроях, включаючи комп'ютери, ноутбуки, смартфони, планшети, телевізори, принтери, розумні телевізори, зовнішні накопичувачі, мережеві компоненти, сервери та хмарні сховища тощо.

Дані з цифрових пристроїв поділяються на контент (текст, зображення, відео, звук) та метадані (інформація про контент, така як дата створення, розмір файлу та автор) [8]. Ці дані містять значну кількість інформації про користувачів і події в їхньому житті. Наприклад, ігрові приставки зберігають інформацію про те, у які ігри гравець саме грає, коли він грає та скільки часу проводить за грою. Ця інформація може використовуватися для різних цілей, таких як розслідування злочинів, маркетинг і таргетинг реклами [9].

У різних країнах існують різні вимоги до аутентифікації цифрових доказів, але незалежно від цього, важливо, щоб вони були аутентичними, що можна забезпечити за допомогою криптографічних методів, ланцюжка походження та експертних висновків. Аутентифікація цифрових доказів є важливою для їхнього використання в суді [10].

Міжнародна організація зі стандартизації (ISO) і Міжнародна електротехнічна комісія (МЕК) опублікували стандарти щодо поводження з цифровими доказами. Вони пропонують чотири етапи поводження з цифровими доказами: ідентифікація, збір, отримання та збереження:

– на етапі ідентифікації необхідно знайти та розпізнати цифрові докази, а також документувати їх;

– на етапі збору необхідно зібрати всі цифрові пристрої, які можуть містити дані, що мають доказову цінність;

– на етапі отримання необхідно отримати цифрові докази без шкоди для їх цілісності. Це здійснюється шляхом створення копії вмісту цифрового пристрою;

– на етапі збереження необхідно забезпечити цілісність цифрових доказів протягом усього періоду провадження в справі [11].

Цифрові докази можуть бути використані для встановлення різних обставин у кримінальному провадженні, наприклад, для встановлення особи злочинця, місця й часу скоєння злочину, а також інших обставин справи. Ретельне документування процесу збору та дослідження цифрових доказів на всіх етапах має важливе значення для забезпечення їх допустимості саме в суді [12].

Висновки. Отже, цифрова криміналістика являє собою інноваційну та багатоаспектну галузь криміналістики, яка включає процеси ідентифікації, отримання, збереження, аналізу та подання цифрових доказів. Цифрові докази можуть бути використані для визначення різних обставин у кримінальному провадженні, наприклад, для встановлення особи фігурантів, місця й часу скоєння злочину й т. ін. Можемо стверджувати, що криміналістична експертиза в галузі цифрових технологій у розвинених країнах світу постійно вдосконалюється й успішно протидіє поширенню кіберзлочинності. Україна в цьому питанні також не відстає від світових тенденцій. Підтвердженням є той факт, що в складі Національної поліції уже декілька років функціонує спеціальний підрозділ по боротьбі з кіберзлочинністю. Утім, для того щоб правоохоронні органи могли повною мірою використовувати можливості сучасних технологій, необхідно якнайшвидше завершити процес інтеграції вітчизняних правоохоронних структур у європейський простір.

Як уже було зазначено, цифрові докази відіграють ключову роль у розслідуванні злочинів. Адекватне збирання та зберігання цифрових доказів є критично важливим для їх подальшого використання в судовому процесі. У цьому контексті, вітчизняні правоохоронні органи стикаються з викликом інтеграції в європейський простір, що відкриє доступ до повного спектру можливостей, які надають сучасні технології.

Перспективи майбутніх досліджень у сфері цифрової криміналістики охоплюють розвиток новітніх технологій, що забезпечують виявлення та аналіз цифрових слідів. Це передбачає створення удосконалених інструментів для ідентифікації, збору та обробки цифрових даних, які можуть бути використані як докази в кримінальних справах. Особлива увага має бути приділена розробці методів кібербезпеки, які зможуть запобігати та виявляти кіберзлочини на ранніх стадіях. Наукові дослідження в цій області повинні бути спрямовані на формування ефективних стратегій протидії різноманітним формам кіберзлочинності, включаючи шахрайство, крадіжку даних, незаконне проникнення в комп'ютерні системи та інші види цифрових злочинів. Це вимагає не лише вдоско-

налення технологічних рішень, але й підвищення рівня кваліфікації фахівців, які займаються розслідуваннями у сфері цифрових злочинів. Крім того, актуальним є питання розробки міжнародних стандартів у цій галузі, що дозволило б забезпечити уніфікований підхід до збору, аналізу та використання цифрових доказів. Міжнародна співпраця між правоохоронними органами різних країн є ключовою для ефективного обміну інформацією та досвідом у боротьбі з транснаціональною кіберзлочинністю. Таким чином, цифрова криміналістика вимагає постійного розвитку та адаптації до швидкозмінного кіберпростору, що включає інновації в технологічному секторі, розвиток професійних навичок фахівців та зміцнення міжнародного співробітництва.

Література

1. Maras, M.-.H. Computer forensics: cybercriminals, laws, and evidence, Jones & Bartlett Learning; 2 edition. 2014.

2. Колодіна, А. С., Федорова, Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*. 2022. С. 176–180.

3. Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України.* 2021. № 8. С. 12-27. DOI: 10.33498/louu-2021-08-012.

4. Борисова К. Є., Світличний В. А. Застосування цифрової криміналістики. *Сучасні тенденції розвитку криміналістики та кримінального процесу в умовах воєнного стану* : зб. матеріалів доп. учасн. Міжнар. наук.-практ. конф. Харків, 2022. С. 83–84.

5. Особливості застосування безпілотних літальних апаратів органами та підрозділами поліції: метод. рек. / А. А. Саковський, С. М. Науменко, С. І. Кравченко, І. М. Єфіменко та ін. Київ: Нац. акад. внутр. справ. 2022. 72 с.

6. Селютін С. Т., Стах А. Ю. Електронні системи взаємодії держави та бізнесу в публічному управлінні. *Держава та регіони*. 2023. URL : http://pa.stateandregions.zp.ua/archive/2_2023/25.pdf.

7. Ринкова економіка : сучасна теорія і практика управління. Т. 19, Вип. 2 (45) : збірка наукових праць. Одеса : Одес. нац. ун-т ім. І. І. Мечникова, 2020. 464 с.

8. Murzo Ye., Halchenko V. Electronic evidence as a means of proof during the pillage investigation. *Scientific Journal of the National Academy of Internal Affair.* 2023. № 28(3), С. 48–57. URL : https://elar.naiau.kiev.ua/server/api/core/bitstreams/ 2ec51de9-c93c-4bc6-bc7b-7b52c836573b/content.

9. Міжнародне технічне регулювання: навч. посіб. / О. М. Сафонова, Г. А. Селютіна, М. В. Нечипорук, В. М. Селютін Харків : ХДУХТ, 2017. URL : https://docplayer.net/61335214-Mizhnarodne-tehnichne-regulyuvannya.html

10. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? *Новини України та Світу. Головні і останні новини – НВ*. [Електронний ресурс] URL : https://nv.ua/ukr/opinion/viyna-v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochini-rfv-ukrajini-novini-ukrajini-50248411.html.

11. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. [Електронний ресурс] URL : https://www.iso.org/standard/44381.html/

12. Цифрова криміналістика: проблеми теорії і практики. *Головна сторінка DSpace*. [Електронний ресурс] URL : https://ir.kneu.edu.ua/handle/2010/37911/.