УДК 343.9 **DOI https://doi.org/10.32782/2522-9656/2024-16-6**

Черемнова Антоніна Іванівна,
кандидат юридичних наук, доцент, вчений секретар
Одеського науково-дослідного інституту
судових експертиз Міністерства юстиції України
ORCID ID: 0000-0002-0221-6337

ЦИФРОВА КРИМІНАЛІСТИКА ЯК СКЛАДОВА КРИМІНАЛІСТИЧНОЇ ТЕХНІКИ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

DIGITAL FORENSICS AS A COMPONENT OF FORENSIC TECHNOLOGY: CURRENT STATE AND PROSPECTS FOR DEVELOPMENT

Анотація. Стаття присвячена розгляду питання цифрової криміналістики як складової криміналістичної техніки. На основі аналізу наукової літератури та наявних криміналістичних досліджень сформульовано авторське визначення цифрової криміналістики, під яким пропонується розуміти розділ криміналістичної техніки, який вивчає особливості утворення цифрових слідів та слідової картини у віртуальному середовищі, а також систему технічних засобів і прикладних алгоритмів їх виявлення, вилучення, дослідження та представлення для безпосереднього дослідження судом під час судового розгляду кримінального провадження. Водночас виокремлено декілька напрямів цифрової криміналістики як складової криміналістичної техніки: по-перше, збирання та фіксація цифрової інформації з різноманітних носіїв. У контексті цього відзначено, що збирання інформації здійснюється зі стаціонарних пристроїв: комп’ютерної техніки (без відключення від локальної мережі – безпосередньо на місці, де розташований пристрій, оскільки в такому випадку зберігається доступ до певних баз даних, сховищ, який у випадку перенесення пристрою втрачається, після чого вилучається безпосередньо і сама комп’ютерна техніка як носій інформації, що в подальшому підлягає ретельному дослідженню та проведенню певних експертиз); а також з переносних носіїв: флеш-носіїв, телефонних пристроїв, SD-карток, жорстких дисків тощо; по-друге, дослідження цифрової інформації. У вказаному напрямі виокремлено: а) дослідження цифрової інформації, наявної на комп’ютерних пристроях; б) дослідження цифрової інформації, що міститься на носіях цифрової інформації (при цьому досліджується саме цифрова інформація, а не безпосередньо носій та його технічні характеристики тощо); в) дослідження цифрової інформації, яка міститься у хмарних сховищах (нематеріальних носіях інформації). У цьому аспекті як окремий підвид запропоновано визначити соціальні мережі, що є окремим джерелом зберігання, отримання та поширення цифрової інформації, аргументуючи вказану позицію тим, що протягом останніх років, під час яких Україна страждає через повномасштабне російське вторгнення, дедалі більшого поширення набули «нетипові» для України злочини, такі як, наприклад, державна зрада.

Констатовано, що цифрова інформація, отримана за результатами розслідування злочинної діяльності, може мати різний характер: по-перше, інформація про особу (особиста інформація про особу, яка здійснила протиправне діяння, стала жертвою злочину та/або була його свідком чи сприяла у його вчиненні); по-друге, інформація, яка свідчить про вчинення протиправного діяння. У розрізі розгляду заявленої категорії виокремлено: а) інформацію, що свідчить про спосіб вчинення протиправного діяння; б) інформацію про обставини, які

підлягають встановленню під час розслідування кримінального провадження; в) інформацію про злочинні посягання, які плануються в майбутньому.

Запропоновано внесення законодавчих змін, насамперед до ч. 2 ст. 84 Кримінального процесуального кодексу України, а саме пропонується викласти її в такій редакції: «2. Процесуальними джерелами доказів є показання, речові та цифрові (електронні) докази, документи, висновки експертів».

Ключові слова: криміналістика; цифрова криміналістика; криміналістична техніка; цифрові докази.

Abstract. The article is devoted to consideration of the issue of digital forensics as a component of forensic technology. Based on the analysis of scientific literature and existing forensic studies, the author's definition of digital forensics is formulated, under which it is proposed to understand the section of forensic techniques that studies the peculiarities of the formation of digital traces and trace patterns in the virtual environment, as well as the system of technical means and applied algorithms for their detection, extraction, research and submission for direct examination by the court during the trial of criminal proceedings. At the same time, several directions of digital forensics are singled out as a component of forensic techniques: first, collection and recording of digital information from various media. In this context, it is noted that the collection of information is carried out from: first, stationary devices: computer equipment (without disconnection from the local network – directly at the place where the device was located, since in this case access to certain databases, storages, which, in the case of transferring the device, they are lost, after which the computer equipment itself is directly removed as an information carrier, which is subsequently subject to thorough research and certain examinations); secondly, from portable media: flash drives, telephone devices, SD cards, hard drives, etc.; secondly, the study of digital information. In the specified direction, the following are highlighted: a) research of digital information available on computer devices; b) research of digital information contained on digital information carriers (at the same time, it is the digital information that is researched, and not directly the carrier and its technical characteristics, etc.); c) research of digital information contained in cloud storages (intangible media). In this aspect, as a separate subspecies, it is proposed to define social networks, which are a separate source of storage, acquisition and distribution of digital information, arguing this position by the fact that during recent years, during which Ukraine is suffering due to a full-scale Russian invasion, “atypical” networks have become more and more widespread for Ukraine, crimes such as, for example, treason.

It was established that digital information obtained as a result of the investigation of criminal activity can be of different nature: first, information about a person (personal information about a person who committed an illegal act, who became a victim of a crime, and/or was a witness to it or contributed to it his actions); secondly, information that indicates the commission of an illegal act. In the context of consideration of the declared category, the following are distinguished: a) information that indicates the method of committing an illegal act; b) information about the circumstances to be established during the investigation of criminal proceedings; c) information about criminal offenses that are planned in the future.

It is proposed to introduce legislative changes, in particular, first of all to Part 2 of Art. 84 of the Criminal Procedure Code of Ukraine and set it out in the following version: “2. Procedural sources of evidence are testimony, material and digital (electronic) evidence, documents, experts' conclusions”.

Key words: criminalistics; digital forensics; forensic technique; digital evidence.

Постановка проблеми. Глобалізація, що триває, стрімка цифровізація та неухильне збільшення цифрової інформації значним чином вплинули на характер суспільних відносин. Водночас указані процеси мають як позитивну

спрямованість, так і негативну, зокрема, розвиток цифрових технологій, легкість в доступі до отримання й обробки інформації мусили б мати на меті створення умов для безперешкодного розвитку людини, прикладаючи для цього мінімум зусиль з боку споживача, проте на фоні таких змін трансформуються і прояви злочинної поведінки. Так, кількість протиправних діянь, вчинюваних у кіберпросторі, дедалі збільшується, як і ускладняються способи та методи їх вчинення. Водночас варто констатувати, що вказані процеси супроводжуються тим, що злочинні посягання, вчинювані з використанням кіберпростору, все частіше набувають статусу латентних. Так само збільшення кількості злочинів окресленої категорії пояснюється насамперед тим, що наразі в Інтернеті міститься доволі велика кількість особистої інформації громадян, суб’єктів господарювання, що зберігається в певних базах даних, хмарних сховищах тощо. Зазначене вимагає зміни усталених парадигм у розслідуванні злочинної діяльності, зокрема доповнення та переосмислення вже наявних способів, методів і методик розслідування протиправної діяльності з коригуванням відповідно до реалій сьогодення.

Наведене зумовлює й переосмислення структури окремих галузей наукового знання й упровадження нових елементів, які потребують системного наукового дослідження з метою подальшої побудови несуперечливої концепції та ефективних алгоритмів роботи правоохоронних органів.

Мета статті полягає в розгляді цифрової криміналістики як складової криміналістичної техніки, аналізі її сучасного стану розвитку й виокремленні подальших перспектив розвитку цього феномену.

Виклад основного матеріалу. Розпочинаючи аналіз, вважаємо за потрібне розглянути ретроспективу розвитку та виникнення «цифрової криміналістики». Зокрема, як слушно визначили А. Колодіна та Т. Федорова, «цифрова криміналістика виникла орієнтовно у 80-ті роки XX століття. Перший етап розвитку цифрової криміналістики охоплює 1985–1995 роки. Цей етап включав використання програмних кодів для перегляду даних у внутрішніх операційних системах та апаратних засобах комп’ютерів. Другий етап розвитку цифрової криміналістики припадає на 1995–2005 роки. Він ознаменувався появою кіберзлочинності і необхідністю боротьби з нею. Третій етап розвитку цифрової криміналістики відбувся у 2005–2010 роки. У цей період виникають складні цифрові моделі розслідування злочинів. Однією з таких моделей, яка широко використовується у світі, стала «загальна модель комп’ютерних криміналістичних розслідувань» (Generic Computer Forensic Investigation Model – GCFIM). Сучасний етап розвитку цифрової криміналістики починається приблизно в 2010 році та продовжується по цей час» [2, с. 379]. Узагальнюючи зазначене, можна зробити проміжний висновок, що особливістю саме цифрової криміналістики виступає те, що в цьому випадку сліди, які залишаються в процесі вчинення та після завершення злочинного

умислу, є цифровими (електронними), що суттєво відрізняє їх від матеріальних та ідеальних слідів, які є традиційними об’єктами криміналістичного пізнання, зокрема, за їх формою, особливостями формування й існування в об’єктивній реальності, а також технологією вилучення, фіксації та подальшого зберігання.

Вагомий внесок у розуміння явища цифрової криміналістики у своєму дослідженні зробили Р. Степанюк та С. Перлін, де зазначається, що «технічні питання, які є основними в цифровій криміналістиці, вочевидь, мали б сформувати окрему галузь криміналістичної техніки, чого досі зроблено не було, за винятком окремого виду судової експертизи комп’ютерної техніки та програмних продуктів і вдосконалення методик проведення деяких інших експертиз, які використовують методи цифрової криміналістики (фототехнічної, експертизи відео-, звукозапису та ін.)» [5, с. 287]. Продовжуючи, науковці відзначають, що «у судових науках (forensic sciences) сформовано окрему галузь – цифрову криміналістику (digital forensics), яка являє собою систему наукових методів дослідження цифрових доказів з метою сприяння виявленню та розслідуванню кримінальних правопорушень. Водночас у вітчизняній системі криміналістики відповідні засоби та методи належного місця досі не знайшли. Тому в Україні існує нагальна потреба у становленні окремого розділу криміналістичної техніки, присвяченого криміналістичному дослідженню цифрових доказів, зміст якого включатиме наукові положення цифрової криміналістики як галузі судових наук, адаптованих до реалій вітчизняної правоохоронної практики та криміналістичної теорії» [5, с. 290].

У навчальній літературі відзначається, що «під поняттям «криміналістична техніка», з одного боку, розуміється розділ науки криміналістики, а з іншого – сукупність технічних засобів, які використовуються в кримінальному судочинстві» [3].

Водночас І. Когутич зазначає, що «підгалузями цифрової криміналістики є: 1) криміналістичне вчення про комп’ютерну інформацію; 2) теоретичні положення й рекомендації щодо криміналістичного дослідження комп’ютерних засобів, інформаційних систем та інформаційно-телекомунікаційних мереж; 3) теоретичні положення й рекомендації стосовно шляхів і можливостей криміналістичного застосування комп’ютерної інформації, засобів її обробки та захисту» [1, с. 81–82]. Існує також думка, що «цифрова криміналістика визначається як процес збереження, ідентифікації, вилучення та документування комп’ютерних доказів, які можуть бути використані судом. Це наука про пошук доказів у цифрових носіях, таких як комп’ютер, мобільний телефон, сервер або мережа» [9].

Отже, зважаючи на вищенаведене, можна констатувати, що *цифрова криміналістика – це розділ криміналістичної техніки, який вивчає особливості утворення цифрових слідів та слідової картини у віртуальному середовищі, а також*

систему технічних засобів і прикладних алгоритмів їх виявлення, вилучення, дослідження та представлення для безпосереднього дослідження судом під час судового розгляду кримінального провадження.

У цьому випадку під час досудового розслідування йдеться про цифрові докази, які на сьогодні законодавцем так і не внесені до переліку джерел доказів, зокрема, у чинному Кримінальному процесуальному кодексі України зазначено, що «джерелами доказів є показання, речові докази, документи, висновки експертів» [4]. Зі свого боку, Д. Цехан під цифровими доказами пропонує розуміти «фактичні дані, що представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія та після обробки ЕОМ стають доступними для сприйняття людиною. При цьому обов’язковою ознакою цифрового доказу є конвергентність, під якою розуміється здатність одиничного доказу входити у сукупність інших доказів і набувати у зв’язку з цим доказового значення» [6, с. 257].

Водночас ми в попередніх своїх дослідженнях дійшли висновку, розглядаючи цифрову інформацію як об’єкт експертного дослідження, що «під цифровою інформацією в контексті розслідування кримінальних проваджень слід розуміти дані, представлені в електронній (цифровій) формі, що містять відомості, які мають значення для справи, містять сліди вчиненого кримінального правопорушення, були знаряддям чи засобом його вчинення, які зберігаються на матеріальних носіях інформації: комп’ютерних, мобільних пристроях, цифрових камерах, роутерах тощо – або нематеріальних ресурсах, як-от мережа Інтернет, локальні мережі установ та організацій тощо, при цьому на зазначених носіях інформації можуть міститися: файли (з текстовою інформацією, аудіо чи відео); різноманітне програмне забезпечення, що використовується як «знаряддя» вчинення злочину чи для приховання слідів його вчинення; файли, що містять сліди підробки чи фальсифікації; бази даних, вільний доступ до яких заборонено чинним законодавством у сфері охорони державної таємниці, захисту персональних даних тощо; скановані копії, фотокопії документів, обмежених для обігу тощо» [8, с. 60].

Беручи до уваги зазначене вище, вважаємо, що можна виокремити декілька напрямів цифрової криміналістики як складової криміналістичної техніки:

– по-перше, збирання та фіксація цифрової інформації з різноманітних носіїв. У контексті цього варто відзначити, що збирання інформації здійснюється зі стаціонарних пристроїв: комп’ютерної техніки (без відключення від локальної сітки – безпосередньо на місці, де розташований пристрій, оскільки в такому випадку зберігається доступ до певних баз даних, сховищ, який у випадку перенесення пристрою втрачається, після чого вилучається безпосередньо і сама комп’ютерна техніка як носій інформації, що в подальшому підлягає ретельному дослідженню та проведенню певних експертиз); а також з переносних носіїв: флеш-носіїв, телефонних пристроїв, SD-карток, жорстких дисків тощо;

– по-друге, дослідження цифрової інформації. У вказаному напрямі, вважаємо, можна виокремити:

а) дослідження цифрової інформації, наявної на комп’ютерних пристроях;

б) дослідження цифрової інформації, що міститься на носіях цифрової інформації (при цьому досліджується саме цифрова інформація, а не безпосередньо носій та його технічні характеристики тощо);

в) дослідження цифрової інформації, яка міститься у хмарних сховищах (нематеріальних носіях інформації). У цьому аспекті як окремий підвид пропонуємо визначити *соціальні мережі*, що є окремим джерелом зберігання, отримання й поширення цифрової інформації, зокрема, через те, що соціальні мережі певним чином стали знаряддям та обстановкою вчинення великої кількості протиправних діянь, особливо прояв цього можна спостерігати з початку активних військових дій на території України та повномасштабного російського вторгнення, унаслідок чого дедалі більшого поширення набули «нетипові» для України злочини, як-от, наприклад, державна зрада. Так, до прикладу, у літературі висловлюється думка, що «аналіз наявних підходів дозволяє виокремити три основні напрями використання соціальних мереж під час розслідування кримінальних правопорушень, які можуть повністю бути екстрапольовані й на розслідування державної зради: по-перше, отримання відповідної системи установчих даних на особу, яка притягується до кримінальної відповідальності на початковому етапі розслідування кримінального провадження чи попереднього документування злочинної діяльності; по-друге, виявлення та вилучення різних типів слідів із метою подальшого формування доказів у межах кримінальних проваджень; по-третє, використання таких даних для встановлення місцезнаходження осіб, які причетні до вчинення кримінального правопорушення» [7, с. 482].

Отже, узагальнюючи, варто зазначити, що цифрова інформація, отримана за результатами розслідування злочинної діяльності, може мати різний характер:

– по-перше, інформація про особу (особиста інформація про особу, яка здійснила протиправне діяння, стала жертвою злочину та/або була його свідком чи сприяла у його вчиненні);

– по-друге, інформація, яка свідчить про вчинення протиправного діяння. У розрізі розгляду заявленої категорії можна виокремити:

– інформацію, що свідчить про спосіб вчинення протиправного діяння;

– інформацію про обставини, які підлягають встановленню під час розслідування кримінального провадження;

– інформацію про злочинні посягання, які плануються в майбутньому. У рамках цього різновиду слушним є використання розвідувальної аналітики як однієї з моделей оперативного обслуговування кіберпростору. Так, у науковій літературі підкреслюється, що вказане надає можливість «по-перше, своєчасного виявлення як окремих осіб, так і спільнот, які потенційно можуть

вчиняти будь-які правопорушення… з метою оперативного контролю за ними; по-друге, вчинення заходів ранньої профілактики щодо таких осіб; по-третє, своєчасного припинення їх злочинної діяльності. У контексті цього потрібно наголосити, що оперативний контроль за такими спільнотами та соціальними медіа має важливе значення для виявлення всіх учасників злочинної діяльності як на етапі її попереднього документування, так і безпосередньо в процесі розслідування конкретних кримінальних правопорушень, а також встановлення інфраструктурних елементів такої діяльності, зокрема джерел фінансової підтримки таких груп» [7, с. 483].

Так, у контексті вищезазначеного, на наш погляд, значним недоліком чинного кримінального процесуального законодавства є те, що в ньому відсутня нормативна регламентація цифрових (електронних) доказів, на відміну від Цивільного процесуального кодексу України та Господарського процесуального кодексу України, які передбачають електронні докази допустимими, тому для ефективного та «легального» використання здобутків цифрової криміналістики, а в подальшому – допустимості отриманої доказової інформації під час досудового розслідування кримінальних правопорушень нагальним і затребуваним є внесення законодавчих змін, насамперед до ч. 2 ст. 84 Кримінального процесуального кодексу України: пропонується викласти її в такій редакції: *«2. Процесуальними джерелами доказів є показання, речові та цифрові (електронні) докази, документи, висновки експертів».*

Перелік використаних джерел:

1. Когутич І. І. Застосування цифрових технологій – новий напрям криміналістики. *Наукові читання пам’яті Ганса Гросса* : збірник тез міжнародної науково-практичної конференції (м. Чернівці, 9 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці : Технодрук, 2021. С. 79–84.

2. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Юридичний науковий електронний журнал*. 2022. № 4. С. 378–380. URL: http://lsej.org.ua/4_2022/90.pdf.

3. Криміналістична техніка. Криміналістика : мультимедійний навчальний підручник. URL: https://arm.naiau.kiev.ua/books/criminalistics/info/lec4.html.

4. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

5. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2022. Вип. 3 (99). С. 283–294. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/5f268f43-1af7-4fa7-bae0-5e2d05ac71bb/content.

6. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2013. № 5. С. 256–260.

7. Цехан Д. М., Мурашко А. С. Використання соціальних медіа для вирішення ідентифікаційних завдань під час виявлення та розслідування злочинів, пов’язаних із державною зрадою. *Юридичний науковий електронний журнал*. 2024. № 2. С. 481–483. URL: http://www.lsej.org.ua/2_2024/121.pdf.

8. Черемнова А. І., Бєлік Л. С. Цифрова інформація як об’єкт експертного дослідження в умовах діджиталізації: проблеми та перспективи розвитку. *Криміналістика і судова експертиза.* 2023. Вип. 68. С. 57–65.

9. Що таке цифрова криміналістика? Історія, процес, типи, виклики. *GURU99*: вебсайт. URL: https://www.guru99.com/uk/digital-forensics.html.

References:

1. Kohutych, I. I. (2021). Zastosuvannia tsyfrovykh tekhnolohii – novyi napriam kryminalistyky [The use of digital technologies is a new direction of forensics]. *Naukovi chytannia pamiati Hansa Hrossa*: zbirnyk tez mizhnarodnoi naukovo-praktychnoi konferentsii (m. Chernivtsi, 9 hrudnia 2021 r.). Chernivetskyi natsionalnyi universytet imeni Yuriia Fedkovycha. Chernivtsi: Tekhnodruk. P. 79–84.

2. Kolodina, A. S., Fedorova, T. S. (2022). Tsyfrova kryminalistyka: problemy teorii i praktyky [Digital forensics: problems of theory and practice]. *Yurydychnyi naukovyi elektronnyi zhurnal*. № 4. P. 378–380. Retrieved from: http://lsej.org.ua/4_2022/90.pdf (accessed: 22.11.2024).

3. Kryminalistychna tekhnika. Kryminalistyka: multymediinyi navchalnyi pidruchnyk [Forensic technique. Criminalistics: multimedia textbook]. Retrieved from: https://arm.naiau.kiev.ua/books/criminalistics/info/lec4.html (accessed: 22.11.2024).

4. Kryminalnyi protsesualnyi kodeks Ukrainy: Zakon Ukrainy vid 13.04.2012 № 4651-VI [Criminal Procedure Code of Ukraine: Law of Ukraine dated 04/13/2012 No. 4651-VI]. Retrieved from: https://zakon.rada.gov.ua/laws/show/4651-17#Text (accessed: 22.11.2024).

5. Stepaniuk, R. L., Perlin, S. I. (2022). Tsyfrova kryminalistyka y udoskonalennia systemy kryminalistychnoi tekhniky v Ukraini [Digital forensics and improvement of the forensic technology system in Ukraine]. *Visnyk LDUVS im. E. O. Didorenka*. Issue 3 (99). P. 283–294. Retrieved from: https://dspace.univd.edu.ua/server/api/core/bitstreams/5f268f43-1af7-4fa7-bae0-5e2d05ac71bb/content (accessed: 22.11.2024).

6. Tsekhan, D. M. (2013). Tsyfrovi dokazy: poniattia, osoblyvosti ta mistse u systemi dokazuvannia [Digital evidence: concepts, features and place in the evidence system]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu*. Ser.: Yurysprudentsiia. № 5. P. 256–260.

7. Tsekhan, D. M., Murashko, A. S. (2024). Vykorystannia sotsialnykh media dlia vyrishennia identyfikatsiinykh zavdan pid chas vyiavlennia ta rozsliduvannia zlochyniv, poviazanykh iz derzhavnoiu zradoiu [The use of social media to solve identification tasks during the detection and investigation of crimes related to high treason]. *Yurydychnyi naukovyi elektronnyi zhurnal*. № 2. P. 481–483. Retrieved from: http://www.lsej.org.ua/2_2024/121.pdf (accessed: 22.11.2024).

8. Cheremnova, A. I., Bielik, L. S. (2023). Tsyfrova informatsiia yak obiekt ekspertnoho doslidzhennia v umovakh didzhytalizatsii: problemy ta perspektyvy rozvytku [Digital information as an object of expert research in the conditions of digitization: problems and development prospects]. *Kryminalistyka i sudova ekspertyza*. Issue 68. P. 57–65.

9. Shcho take tsyfrova kryminalistyka? Istoriia, protses, typy, vyklyky [What is digital forensics? History, process, types, challenges]. GURU99: vebsait. Retrieved from: https://www.guru99.com/uk/digital-forensics.html (accessed: 22.11.2024).