УДК 343.9
DOI https://doi.org/10.32782/2524-0374/2022-4/90

ЦИФРОВА КРИМІНАЛІСТИКА: ПРОБЛЕМИ ТЕОРІЇ І ПРАКТИКИ

DIGITAL FORENSICS: PROBLEMS OF THEORY AND PRACTICE

Колодіна А.С., к. ю. н.,
доцент кафедри криміналістики
Національний університет «Одеська юридична академія«

Федорова Т.С., к. ю. н.,
доцент кафедри міжнародного та європейського права
Національний університет «Одеська юридична академія«

З кожним роком інноваційні технології все більше впроваджуються в різні сфери суспільного життя. Не винятком є і криміналістична експертиза, яку сучасні інформаційні технології вивели на новий етап розвитку. Зокрема, завдяки новітнім технологіям з'явилася нова галузь криміналістики – цифрова криміналістика.

У статті досліджується новітня галузь криміналістики – цифрова криміналістика, яка є прикладною наукою про розкриття злочинів, пов'язаних з комп'ютерною інформацією, про дослідження цифрових доказів, методи пошуку, отримання і закріплення таких доказів.

Цифрова криміналістична експертиза – це «одна із галузей криміналістичної експертизи, яка зосереджується на кримінально-процесуальному праві та доказах щодо комп'ютерів та пов'язаних із ними пристроїв», таких як мобільні пристрої (телефони, смартфони тощо), ігрові консолі та інші пристрої, які функціонують через Інтернет (охорона здоров'я і фітнес-пристрої та медичні прилади тощо). Цифрова криміналістична експертиза, зокрема, відноситься до процесу збору, отримання, зберігання, аналізу та подання електронних доказів (також відомих як цифрові докази) з метою отримання слідчої інформації та розслідування та переслідування різних видів злочинів, у тому числі кіберзлочинів.

Автори статті проаналізували складові частини цифрової криміналістики, оцінили тенденції розвитку цієї науки на сучасному етапі та спрогнозували подальший розвиток цифрової криміналістик в Україні і в іноземних країнах.

Цифрова криміналістична експертиза включає процеси ідентифікації, отримання, зберігання, аналізу та представлення цифрових доказів. Криміналістичні артефакти та криміналістичні методи (наприклад, збір статичних даних або даних у реальному часі) залежать від пристрою, його операційної системи та функцій безпеки. Запатентовані операційні системи (з якими дослідники можуть бути незнайомі) і функції безпеки (наприклад, шифрування) є перешкодами для цифрової криміналістичної експертизи. Наприклад, шифрування, яке блокує доступ третіх сторін до інформації та повідомлень користувачів, може перешкодити правоохоронним органам отримати доступ до даних, що містяться на цифрових пристроях, таких як смартфони.

В Національній поліції було створено спецпідрозділ по боротьбі з кіберзлочинністю. Але для того, щоб вітчизняні правоохоронні органи дійсно змогли використовувати весь спектр можливостей, які надають сучасні технології, необхідно якомога швидше завершити процес інтеграції вітчизняних правоохоронних структур у європейський простір.

Ключові слова: цифрова криміналістика, криміналістика, докази, кримінальний процес, кіберзлочинність.

Every year, innovative technologies are increasingly being introduced into various spheres of public life. No. exception in this sense is forensics, which the newest technologies have allowed to bring to a new stage of development. In particular, thanks to the latest technologies, a new field of forensics has emerged, which is digital forensics.

Therefore, digital forensics (forensics, computer forensics, cybercrime investigations) is the applied science of computer-related crime disclosure, the study of digital evidence, the methods of finding, obtaining and securing of such evidence.

Digital forensics is "one of the forensic fields that focuses on criminal procedure law and evidence regarding computers and related devices", such as mobile devices (phones, smartphones, etc.), game consoles, and other devices that function over the Internet (health and fitness devices and medical devices, etc.). Digital forensics, in particular, refers to the process of collecting, obtaining, storing, analyzing and presenting electronic evidence (also known as digital evidence) for the purpose of obtaining investigative information and investigating and prosecuting various types of crime, including cybercrime.

Digital forensics originated approximately in the 1980s.

The first stage in the development of digital forensics covers 1985–1995. This phase involved the use of program codes to view data on internal operating systems and computer hardware.

The second stage of the development of digital forensics is 1995–2005. It was marked by the emergence of cybercrime and the need to combat it.

The third stage of the development of digital forensics took place in 2005–2010. During this period, complex digital models of crime investigation emerged. One such model, which is widely used in the world, is the "Generic Computer Forensic Investigation Model" (GCFIM).

The current stage of the development of digital forensics begins around 2010 and continues to this day.

Digital forensics involves the processes of identifying, receiving, storing, analyzing and presenting of digital evidence. The digital evidence must be authenticated to ensure that it is admissible in court. Ultimately, forensic artifacts and forensic techniques (such as static or real-time data collection) depend on the device, its operating system, and its security features. Patented operating systems (which investigators may be unfamiliar with) and security features (such as encryption) are barriers to digital forensics. For example, encryption that blocks third-party access to user information and messages may prevent law enforcement agencies from accessing data contained on digital devices such as smartphones.

However, digital forensics in developed countries is developing at a rapid pace and is worth resisting the spread of cybercrime. Our country is no exception. In particular, a special unit for combating cybercrime was created within the national police a few years ago. However, in order for the domestic law enforcement agencies to really be able to use the full range of capabilities that modern technologies provide, it is necessary to complete the process of integrating of domestic law enforcement structures into the European space as soon as possible.

Key words: digital forensics, forensics, evidence, criminal process, cybercrime.

Постановка проблеми. Ще в 70-ті роки минулого століття було помічено, що «стрімкі, динамічні зміни в соціальній структурі суспільства породжуються лавиноподібним процесом інновацій, матеріалізованих наукових ідей, наукових відкриттів, технічних винаходів і розробок, з принципово новими технологічними процесами [1, с. 7].

З кожним роком інноваційні технології все більше впроваджуються в різні сфери суспільного життя. Не винятком в цьому сенсі є криміналістика, яку новітні технології дозволили вивести на новий щабель розвитку. Зокрема, завдяки новітнім технологіям виникла нова галузь криміналістики, якою є цифрова криміналістика.

Стан дослідження теми. Дослідженням цифрової криміналістики в Україні займаються небагато дослідників. Це пов'язано з тим, що цифрова криміналістика є відносно новою наукою, що зародилася лише у 80-ті роки XX століття. Серед авторів, які торкаються окремих проблем цифрової криміналістики є Бутузов В. М., Власова С. В., Іщенко Є. П., Нечаєва Н. Б. тощо. Однією із провідних іноземних дослідниць цифрової криміналістики є Marie-Helen Maras.

Мета статті. Метою статті є дослідження нової сфери криміналістики – цифрової криміналістики.

Викладення основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Отже, цифрова криміналістика (форензіка, комп'ютерна криміналістика, розслідування кіберзлочинів) – прикладна наука про розкриття злочинів, пов'язаних з комп'ютерною інформацією, про дослідження цифрових доказів, методи пошуку, отримання і закріплення таких доказів.

На думку С. В. Власової «цифрові технології дозволять перейти від слідчого типу кримінального процесу до змагального. Повинен бути створений новий правовий механізм застосування кримінального закону, якщо завгодно – новий порядок притягнення до кримінальної відповідальності. Інший, ніж той, що склався в умовах слідчого процесу, централізованої слідчо-обвинувальної влади і її монополії на формування підстав правозастосовних актів» [2].

Цифрова криміналістика є «однією з галузей криміналістики, яка зосереджена на кримінально-процесуальному праві і доказах стосовно комп'ютерів і пов'язаних з ними пристроїв» [3, с. 29], такими, як мобільні пристрої (телефони, смартфони тощо), ігрові приставки та інші пристрої, що функціонують через Інтернет (пристрої для здоров'я та фітнесу та медичні прилади тощо). Цифрова криміналістика, зокрема, має відношення до процесу збору, отримання, збереження, аналізу та подання електронних доказів (також відомих як цифрові докази) з метою отримання оперативно-розшукових відомостей і здійснення розслідування та кримінального переслідування по відношенню до різних видів злочинів, включаючи кіберзлочини.

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 років. 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).

Сучаний етап розвитку цифрової криміналістики починається приблизно в 2010 році та продовжується по цей час.

Цифрова криміналістика ґрунтується на загальних принципах криміналістики. Зокрема, одним із головних з них є принцип обміну Едмона Локара: коли об'єкти і поверхні вступають в контакт один з одним, відбувається перехресне перенесення матеріалів.

У контексті цифрової криміналістики люди, після використання інформаціонокомунікаційних технологій (ІКТ), залишають цифрові сліди. Зокрема, особа, яка використовує ІКТ, може залишити «цифрові відбитки». Дані, залишені користувачами ІКТ, можуть розкрити відомості про них, включаючи інформацію про вік, стать, расову та етнічну приналежність, громадянство, сексуальну орієнтацію, думки, уподобання, звички, хобі, історію хвороби і проблеми зі здоров'ям, психологічні розлади, статус, зайнятість, приналежність до будь-якої спільноти, особисті відносини, геолокацію, розпорядок дня та інші активності.

Такі цифрові відбитки можуть бути активними або пасивними. Активний цифровий відбиток створюється даними, наданими користувачем, такими як персональні дані, відео, зображення і коментарі, що розміщуються в додатках, на вебсайтах, електронних дошках оголошень, в соціальних мережах та інших онлайн-форумах.

Пасивний цифровий відбиток – це дані, які ненавмисно залишають люди, які користуються Інтернетом і цифровими технологіями (наприклад, історія переглядів в браузері). Дані, які є частиною активних і пасивних цифрових відбитків, можуть використовуватися як доказ скоєння злочину, в тому числі кіберзлочину (тобто в якості цифрових доказів). Такі дані можуть також використовуватися для доведення або спростування твердження про факт; підтвердження або спростування показань потерпілого, свідка і підозрюваного; визначення причетності або непричетності підозрюваного до скоєння злочину. Дані зберігаються в цифрових пристроях (наприклад, комп'ютерах, смартфонах, планшетах, телефонах, принтерах, «розумних» телевізорах (Smart TV) і будь-яких інших пристроях, які мають цифрову пам'ять), зовнішніх запам'ятовуючих пристроях (наприклад, зовнішніх жорстких дисках і USB-флеш накопичувачах), мережевих компонентах і пристроях (наприклад, маршрутизаторах), серверах і хмарному сховищі (де дані зберігаються «в кількох центрах даних в різних географічних точках).

Дані, що добуваються, можуть бути ідентифіковані як контент (тобто слова в письмових повідомленнях або вимовлені слова в аудіофайлі, наприклад, відео, текст електронних листів, текстові повідомлення, миттєві повідомлення та зміст соціальних мереж), і дані, що не відносяться до контенту, або мета-дані (тобто дані про зміст; наприклад, особистість і місце розташування користувачів і дані про операції, такі як інформація про відправників і одержувачів телекомунікаційних та електронних повідомлень).

Дані, що одержуються в режимі онлайн і добуваються із цифрових пристроїв, можуть містити велику кількість інформації про користувачів і події. Наприклад, ігрові приставки, які працюють як персональні комп'ютери, зберігають особисту інформацію про користувачів пристроїв (наприклад, імена та адреси електронної пошти), фінансову інформацію (наприклад, дані кредитної картки), інформацію про історію відвідувань Інтернету (наприклад, про відвідані вебсайти), зображення, відео та інші дані.

Ще одним цифровим пристроєм, який накопичує значний обсяг даних про його користувачів, є Amazon Echo (з голосовим помічником Alexa). Дані, що накопичуються цим пристроєм, можуть містити цінні відомості про користувачів, такі як інформація про їх інтереси, уподобання, запити, покупки і інші види активності, а також про їх місцезнаходження (щоб, наприклад, визначити, чи знаходяться вони вдома або поза будинком, шляхом перегляду міток часу і аудіозаписів взаємодії з мовним помічником Alexa). Дані, стягнуті з Amazon Echo, вже використовувалися в Сполучених Штатах Америки при розслідуванні справи про вбивство. Хоча звинувачення проти підозрюваного були в кінцевому підсумку зняті, це справа наочно продемонструвала, що дані, зібрані з використанням нових цифрових технологій, неминуче будуть представлені в суді як доказ.

Дані можуть добуватися і використовуватися в цілях отримання оперативно-розшукових відомостей або можуть представлятися в суді в якості цифрових доказів. В останньому випадку цифрові докази можуть служити прямими доказами шляхом «встановлення факту» або непрямими доказами шляхом «виведення висновку про істинність певного факту».

Перш ніж цифрові докази можуть бути представлені в суді в якості прямих або непрямих доказів, їх треба розпізнати (тобто необхідно показати, що докази відповідають передбачуваній меті).

Для наочної демонстрації практики аутентифікації можна навести такі приклади цифрових доказів: контент, генерований одним або кількома особами (наприклад, текст електронного листа або миттєве повідомлення і документи текстового редактора, такого як Microsoft Word); контент, генерований комп'ютером або цифровим пристроєм без участі користувача (наприклад, журнали реєстрації даних), і контент, генерований одночасно користувачем і пристроєм (наприклад, динамічні таблиці в таких програмах, як Microsoft Excel, які включають в себе дані, що вводяться користувачем, і розрахунки, що здійснюються програмою).

Контент, що генерується користувачем, може вважатися допустимим доказом, якщо він є достовірним і правдоподібним (тобто можна встановити його приналежність будь-якій особі). Контент, що генерується пристроєм, може вважатися допустимим доказом, якщо можна довести, що пристрій функціонував належним чином в момент генерування даних, і якщо можна показати, що в момент генерування даних діяли механізми забезпечення захисту для запобігання зміни даних. У випадках, коли контент генерується одночасно пристроєм і користувачем, необхідно встановити достовірність і правдоподібність кожного з них.

У порівнянні з традиційними доказами (наприклад, паперовими документами, зброєю, контрольованими речовинами і т. д.), цифрові докази створюють унікальні складності при аутентифікації через обсяг доступних даних, їх швидкості (тобто швидкості, з якою вони створюються і передаються), нестійкості (тобто вони можуть швидко зникнути при перезапису або видаленні) і уразливості (тобто їх легко можна обробити, змінити або пошкодити).

У той час як одні країни впровадили норми доказового права, що включають в себе вимоги щодо аутентифікації, які конкретно відносяться до цифрових доказів, інші країни для аутентифікації традиційних доказів і цифрових доказів використовують схожі вимоги.

У Франції, наприклад, як паперові, так і електронні документи повинні аутентифікуватися шляхом перевірки особистості творця документів і цілісності документів.

Перевірка цілісності документів означає не тільки перевірку їх точності, а й здатності зберігати точність (тобто несуперечливість) з плином часу. Більш того, для того щоб уніфікувати режими поводження з нецифровими і цифровими доказами, Сінгапур вніс поправки в норми процесуального права, прийнявши Закон про докази 2012 року, щоб забезпечити однакову практику аутентифікації для нецифрових і цифрових доказів.

У 2012 році Міжнародна організація зі стандартизації (ISO) і Міжнародна електротехнічна комісія (МЕК) опублікували міжнародні стандарти, що стосуються поводження з цифровими доказами (ISO / IEC 27037 Керівництво по ідентифікації, збирання, одержання і збереження свідчень, представлених в цифровій формі [4]). Пропонуються наступні чотири етапи поводження з цифровими доказами:

Ідентифікація. Цей етап включає в себе пошук і розпізнавання відповідних доказів, а також їх документування. На цьому етапі пріоритетні завдання збору доказів визначаються на основі цінності і мінливості доказів.

Збір. Цей етап передбачає збір всіх цифрових пристроїв, які можуть містити дані, що мають доказову цінність. Ці пристрої потім транспортуються в лабораторію судової експертизи або іншу установу для збору і аналізу цифрових доказів. Цей процес називається збором даних в статичному режимі. Однак бувають випадки, коли збір даних в статичному режимі є практично нездійсненним. У таких ситуаціях здійснюється збір даних в реальному часі.

Отримання. Цифрові докази необхідно отримувати без шкоди для цілісності даних. Таке отримання даних без їх зміни здійснюється шляхом створення копії вмісту цифрового пристрою (процес, відомий як створення неспотвореного образу) з використанням пристрою (блокувальника запису), який призначений для запобігання зміни даних в процесі копіювання. Для того щоб визначити, чи є дублікат точною копією оригіналу, значення хешфункції розраховується з використанням математичних обчислень; тут для отримання значення хешфункції використовується криптографічна хешфункція. Якщо значення хешфункції для оригіналу та копії збігаються, то вміст копії є точно таким же, що і в оригіналі.

Збереження. Цілісність цифрових пристроїв і цифрових доказів – «процес, за допомогою якого слідчі забезпечують охорону місця злочину (або події) і збереження доказів протягом всього періоду провадження у справі. У журнал реєстрації записують інформацію про те, хто здійснював збір доказів, де і яким чином вони були зібрані, які особи отримали ці докази, і коли вони їх отримали. Ретельне документування процесу цифрової судової експертизи на кожному етапі має важливе значення для забезпечення допустимості доказів у суді.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Таким чином, цифрова криміналістика включає в себе процеси ідентифікації, отримання, збереження, аналізу та подання цифрових доказів. Цифрові докази повинні бути автентифіковані, щоб забезпечити їх допустимість в суді. В кінцевому рахунку артефакти для судово-експертного аналізу та використовувані криміналістичні методи (наприклад, збір даних в статичному режимі або в режимі реального часу) залежать від пристрою, його операційної системи та його засобів захисту. Запатентовані операційні системи (з якими слідчі можуть бути незнайомі) і засоби захисту (наприклад, шифрування) служать перешкодами для проведення цифрової судової експертизи. Наприклад, шифрування, яке блокує доступ третіх осіб до інформації про користувачів і їх повідомленнями, може завадити правоохоронним органам отримати доступ до даних, що містяться в цифрових пристроях, таких як смартфони.

Втім, цифрова криміналістика в розвинутих країнах розвивається стрімкими темпами і гідно протистоїть поширенню кіберзлочинності. Не є винятком і наша країна. Зокрема, в складі національної поліції ще декілька років тому було створено спеціальний підрозділ з боротьби з кіберзлочинністю. Проте для того, щоб вітчизняні правоохоронні органи дійсно могли використовувати весь спектр можливостей, які надають сучасні технології, необхідно якомога швидше завершити процес інтеграції вітчизняних правоохоронних структур в європейський простір.

ЛІТЕРАТУРА

1. Лазар М. Г., Лейман И. И. НТР и нравственные факторы научной деятельности. Ленинград, «Наука», 1978. 156 с.
2. Власова С. В. К вопросу о приспосабливании уголовно-процессуального механизма к цифровой реальности. Библиотека криминалиста. Научный журнал. 2018. № 1. С. 9–18. URL: https://www.iuaj.net/node/2433
3. Maras M.-.H. *Computer forensics: cybercriminals, laws, and evidence*, Jones & Bartlett Learning; 2 edition (2014).
4. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html