УДК 343.9
DOI https://doi.org/10.32782/ln.2023.21.49

Прокопенко Н.М.
викладач кафедри кримінального права
факультету № 6
Харківський національний університет внутрішніх справ
ORCID ID: 0000-0003-4985-937X

МЕТОДИ ТА КРИМІНАЛІСТИЧНОГО АНАЛІЗУ ЦИФРОВИХ ДОКАЗІВ: ВИКЛИКИ ТА ІННОВАЦІЇ

Вступ. Сучасне суспільство все більше залежить від цифрових технологій, що впливає на різні сфери життя, включаючи кримінальні розслідування. Цифрові докази, такі як електронні листи, повідомлення в соціальних мережах, файли на комп'ютерах та мобільних пристроях, відіграють ключову роль у розкритті злочинів. Вони можуть містити важливу інформацію про злочинні дії, маршрути переміщень, контакти та інші докази, що можуть бути вирішальними у судових процесах.

Проте, аналіз цифрових доказів пов'язаний з численними викликами. Постійний розвиток технологій, зростання обсягу даних та нові методи шифрування ускладнюють процес виявлення та аналізу таких доказів. Крім того, швидка еволюція кіберзлочинності вимагає від криміналістів постійного вдосконалення своїх навичок та використання нових інструментів і методів.

У цьому контексті виникає необхідність вивчення та оцінки сучасних методів та інструментів криміналістичного аналізу цифрових доказів, а також інновацій, які можуть полегшити процес розслідування. Ця стаття присвячена огляду основних методів збору, аналізу та зберігання цифрових доказів, розгляду найбільш ефективних інструментів, а також аналізу викликів та інновацій у цій галузі.

Дослідження методів та інструментів криміналістичного аналізу цифрових доказів є критично важливим для підвищення ефективності розслідувань та забезпечення справедливості у судових процесах. Інновації в цій сфері можуть значно підвищити точність та надійність аналізу, що сприятиме ефективній боротьбі зі злочинністю в цифрову епоху.

Постановка проблеми. Зростання використання цифрових технологій у повсякденному житті та бізнесі призвело до збільшення обсягів цифрових даних, які можуть бути потенційними доказами у кримінальних розслідуваннях. Ці дані охоплюють широкий спектр інформації, від файлів на комп'ютерах і мобільних телефонах до даних у хмарних сервісах і мережевих ресурсах. Виявлення, збір, аналіз та зберігання цих доказів стикається з низкою складних проблем, які потребують вирішення.

Основні проблеми криміналістичного аналізу цифрових доказів можна класифікувати наступним чином:

Швидкий розвиток технологій.

Постійне оновлення апаратних і програмних засобів: Нові моделі пристроїв та оновлення програмного забезпечення вимагають від експертів постійного навчання та адаптації до нових умов.

Складність сучасних систем: Зростання складності та функціональності цифрових систем ускладнює процес збору та аналізу доказів.

Обсяг та різноманітність даних.

Велика кількість даних: Розслідування часто потребує аналізу великих обсягів даних, що може бути ресурсомістким та тривалим процесом.

Різноманітність джерел даних: Дані можуть надходити з різних джерел, таких як комп'ютери, мобільні пристрої, мережеві сервери, хмарні сервіси тощо.

Збереження цілісності доказів.

Цілісність даних: Під час збору та аналізу необхідно забезпечити незмінність даних, щоб вони залишалися прийнятними у суді.

Криптографічні методи захисту: Використання методів шифрування та інших захисних технологій може ускладнити доступ до даних.

Правові та етичні аспекти.

Юридичні вимоги: Необхідність дотримання юридичних норм та процедур при зборі та аналізі цифрових доказів.

Етичні питання: Дотримання конфіденційності та прав осіб під час розслідування.

Інноваційні виклики:

Впровадження нових технологій: Необхідність використання новітніх технологій, таких як машинне навчання та штучний інтелект, для підвищення ефективності аналізу.

Адаптація до нових методів кіберзлочинців: Кіберзлочинці постійно розробляють нові методи та техніки, що вимагає від криміналістів постійного вдосконалення своїх підходів.

Враховуючи ці проблеми, виникає необхідність у детальному дослідженні та розробці сучасних методів і інструментів криміналістичного аналізу цифрових доказів, які дозволять ефективно вирішувати вказані виклики. Це дослідження має на меті надати огляд сучасних підходів у цій сфері, виявити основні проблеми та запропонувати інноваційні рішення для підвищення ефективності та надійності криміналістичного аналізу цифрових доказів.

Аналіз останніх досліджень. У галузі криміналістичного аналізу цифрових доказів спостерігається значний прогрес завдяки розвитку нових методів та інструментів, що дозволяють ефективніше виявляти, збирати та аналізувати цифрові дані. Серед дослідників, які розглядають окремі питання цифрової криміналістики, можна виділити таких авторів, як А.С. Колодіна та Т.С. Федорова, вони представили свою авторську інтерпретацію поняття та змісту цифрової криміналістики як складової судових наук. І. І. Когутич визначив як новий напрям розвитку криміналістики можливості застосування цифрових технологій. М.О. Думчиков, В.Ю. Шепітько, М.В. Шепітько, Р.Л. Степанюк, С.І. Перлін, С.М. Тютченко, Н.А. Братішко, В.М. Бутузов, С.В. Іщенко тощо.

Метою статті є вивчення та аналіз сучасних методів та інструментів цифрового криміналістичного аналізу, їх викликів та інновацій, зокрема щодо їх застосування в сучасних умовах кримінальних розслідувань.

Наукова новизна. Наукова новизна цього дослідження полягає в систематизації сучасних методів інструментів цифрового криміналістичного аналізу, виявленні актуальних викликів цієї галузі та огляді інноваційних підходів до їх вирішення. Також дослідження спрямоване на оновлення розуміння процесів збору, аналізу та використання цифрових доказів в сучасних кримінальних розслідуваннях.

Виклад основного матеріалу. Збір доказової інформації є важливим аспектом у доведенні злочину. Це здійснюється шляхом проведення відкритих і таємних слідчих дій, які описані в розділах 20 та 21 Кримінального процесуального кодексу України. Процеси збору, аналізу та оцінки доказів виконуються в рамках кримінального провадження [1].

Розглянемо методи криміналістичного аналізу цифрових доказів:

Фізичне вилучення даних: Цей метод включає фізичний збір інформації безпосередньо з цифрових носіїв, таких як жорсткі диски, флеш-накопичувачі, мобільні телефони тощо. Це може включати копіювання всієї інформації з носія для подальшого аналізу, відновлення видалених файлів чи екстракцію конкретних типів даних, наприклад, текстових повідомлень або зображень [1].

Логічний аналіз: Використання спеціалізованого програмного забезпечення для

обробки і аналізу вже збережених даних. Цей підхід дозволяє аналізувати структуру даних, шукати ключові слова або фрази, фільтрувати і інформацію згідно з певними критеріями. Програмне забезпечення для логічного аналізу може допомагати виявляти закономірності та тенденції в масивах даних, що не завжди очевидні при ручному аналізі [1].

Аналіз цифрових доказів: Цей метод використовується для аналізу зв'язків між об'єктами і даними з метою виявлення поведінки або взаємозв'язків між різними суб'єктами. Він базується на аналізі великих мережевих даних і може включати в себе виявлення зв'язків через комунікаційні мережі, перегляд історій веб-браузера чи аналіз електронних листів [1].

Ці методи демонструють різні підходи до збору, обробки та аналізу цифрових доказів і використовуються криміналістами для розкриття злочинів і підтримки судових процесів.

Згідно зі статтею 89 Кримінального процесуального кодексу, доказами вважаються фактичні дані, отримані законним шляхом та використовуються для встановлення фактів, важливих для кримінального розслідування. Процес доказування включає в себе збір, перевірку та оцінку цих доказів [1].

У своїй науковій праці Колодіна А.С. та Федорова Т.С. вважають, що цифрові дані можуть використовуватися для отримання оперативно-розшукової інформації або представлятися в суді як електронні докази. У судовому контексті ці електронні докази можуть бути використані як прямі підтвердження фактів або як непрямі докази. Дані, що збираються в режимі онлайн з цифрових пристроїв, можуть включати різноманітну інформацію про користувачів і їх активності. Наприклад, ігрові консолі, що функціонують як персональні комп'ютери, можуть зберігати особисті дані, такі як імена та адреси електронної пошти, фінансову інформацію, історію відвідувань в Інтернеті, а також мультимедійні дані. Також автори вважають, що збір даних означає процес збирання цифрових пристроїв, які можуть містити важливу інформацію. Потім їх доставляють до лабораторії судових експертиз або іншої відповідної установи для подальшого аналізу та обробки цифрових доказів. Цей процес відомий як збір даних у статичному режимі, але існують ситуації, коли вимагається збір даних у реальному часі через обставини, коли статичний збір неможливий [2].

Розглянемо інструменти криміналістичного аналізу цифрових доказів.

Криміналістичний аналіз цифрових доказів вимагає використання спеціалізованих інструментів і програмного забезпечення для ефективного збору, аналізу та представлення даних. Основні інструменти, що використовуються в цій галузі, включають:

1. Програмне забезпечення для аналізу дисків.

Програмне забезпечення для аналізу дисків дозволяє криміналістам відновлювати та аналізувати дані з цифрових носіїв, таких як жорсткі диски та флеш-накопичувачі. Деякі з найпопулярніших інструментів.

EnCase Forensic: Відоме своїми потужними можливостями для збору даних, аналізу файлових систем, відновлення видалених файлів та створення детальних звітів. EnCase використовується правоохоронними органами по всьому світу.

О.І. Гриців вважає, що серед технічних рішень особливої уваги заслуговує EnCase Forensic v7 (остання версія v7.06), багатофункціональний програмний комплекс, що широко використовується в багатьох країнах. EnCase Forensic, протягом свого існування, став стандартом у сфері отримання та аналізу цифрових даних. Завдяки своїм потужним фільтрам і скриптам, цей інструмент дозволяє ефективно розслідувати інциденти та надавати достовірні докази для подальшого передавання справ до суду.[3]

2. Інструменти для аналізу мобільних пристроїв.

Мобільні пристрої, такі як смартфони та планшети, часто містять цінну інформацію

для розслідувань. Спеціалізовані інструменти допомагають зібрати та проаналізувати ці дані:

Cellebrite UFED: Використовується для збору та аналізу даних з мобільних пристроїв. UFED підтримує широкий спектр мобільних платформ та дозволяє відновлювати видалені повідомлення, контакти, журнали дзвінків та інші дані.

У методичних рекомендаціях Тіхонов С.В., Кобець М.В. створили алгоритм використання апаратно-програмного комплексу «Cellebrite UFED» для виявлення, запобігання та розслідування кримінальних правопорушень.[4]

Інструменти для аналізу мережі.

Ці інструменти використовуються для аналізу мережевих з'єднань та перехоплення мережевого трафіку, що може бути корисним для виявлення злочинних дій в Інтернеті:

Wireshark: Відомий інструмент для аналізу мережевого трафіку, що дозволяє перехоплювати та аналізувати пакети даних. Wireshark підтримує різні мережеві протоколи та допомагає виявляти підозрілу активність.

Дронюк І.М., Федевич О. Ю. в своїй праці аналізують Wireshark як один з найпопулярніших аналізаторів мережевих протоколів у світі. Цей інструмент дозволяє користувачам детально переглядати, що відбувається в їх мережі. Програму розробила команда The Wireshark Team, і вона постійно оновлюється з 21 червня 2012 року [5].

Інструменти для аналізу зображень і відео.

Зображення та відео можуть містити важливі докази, які потребують спеціалізованого аналізу:

Amped FIVE: Програмне забезпечення для аналізу та підвищення якості зображень і відео. Amped FIVE дозволяє криміналістам поліпшувати якість відео, здійснювати корекцію зображень та аналізувати метадані.

Інструменти для криптографічного аналізу.

Розшифрування зашифрованих файлів та дискових образів є важливим завданням у цифровій криміналістиці:

Passware Kit Forensic: Інструмент для розшифрування різних типів зашифрованих файлів, включаючи документи, архіви та дискові образи. Passware Kit Forensic підтримує широкий спектр криптографічних алгоритмів.

Застосування цих інструментів та методів дозволяє криміналістам ефективно аналізувати цифрові докази та сприяти успішному розслідуванню злочинів у цифрову епоху.

Виклики та інновації криміналістичного аналізу цифрових доказів

Виклики

Швидкий розвиток технологій

Оновлення програмного забезпечення та обладнання: Постійний розвиток нових технологій та регулярне оновлення програмного забезпечення і обладнання створює складнощі для криміналістів, які повинні постійно вдосконалювати свої навички та інструменти.

Шифрування даних: Сучасні методи шифрування даних значно ускладнюють доступ до інформації, що може бути важливою для розслідування.

Великий обсяг даних.

Аналіз великих даних: Розслідування часто включають аналіз величезних обсягів даних, що вимагає значних ресурсів та часу для ефективної обробки.

Розподілені джерела даних: Дані можуть зберігатися на різних пристроях і в різних місцях, що ускладнює їх збір та аналіз.

Правові та етичні питання.

Конфіденційність та приватність: Балансування між потребою у доступі до даних для розслідування та захистом приватності користувачів є складним завданням.

Юридичні обмеження: Різні країни мають свої законодавчі вимоги щодо збору та використання цифрових доказів, що може створювати додаткові перешкоди у міжнародних розслідуваннях.

Інновації.

Машинне навчання та штучний інтелект.

Автоматизація аналізу даних: Використання алгоритмів машинного навчання для автоматизації процесу аналізу великих обсягів даних, що дозволяє швидше і точніше виявляти інформацію.

Прогнозування та виявлення патернів: Алгоритми штучного інтелекту можуть виявляти складні патерни та прогнозувати можливі сценарії, що сприяє ефективнішому розслідуванню.

Хмарні технології.

Зберігання та обробка даних: Використання хмарних сервісів для зберігання та обробки великих обсягів даних дозволяє підвищити ефективність та масштабованість криміналістичних досліджень.

Спільний доступ до ресурсів: Хмарні платформи забезпечують можливість спільного доступу до інструментів та ресурсів, що полегшує співпрацю між різними командами та організаціями.

Інтегровані платформи аналізу.

Комплексні рішення: Інтегровані платформи, що об'єднують різні інструменти та методи аналізу, дозволяють підвищити ефективність криміналістичних досліджень, забезпечуючи більш узгоджений підхід до обробки та аналізу даних.

Співпраця та обмін інформацією: Такі платформи полегшують співпрацю між різними організаціями та фахівцями, сприяючи більш швидкому та ефективному обміну інформацією.

Висновок. Криміналістичний аналіз цифрових доказів стикається з численними викликами, пов'язаними з розвитком технологій, великими обсягами даних та правовими питаннями. Проте, інновації в галузі машинного навчання, хмарних технологій, Інтернету речей та інтегрованих платформ аналізу надають нові можливості для ефективного розслідування та збору доказів.

Розвиток цих технологій та методів дозволить криміналістам краще справлятися з сучасними викликами та підвищити ефективність криміналістичних розслідувань.

Анотація

Актуальність статті полягає в тому, що аналіз цифрових доказів пов'язаний з численними викликами. Постійний розвиток технологій, зростання обсягу даних та нові методи шифрування ускладнюють процес виявлення та аналізу таких доказів. Крім того, швидка еволюція кіберзлочинності вимагає від криміналістів постійного вдосконалення своїх навичок та використання нових інструментів і методів. У цьому контексті виникає необхідність вивчення та оцінки сучасних методів та інструментів криміналістичного аналізу цифрових доказів, а також інновацій, які можуть полегшити процес розслідування. Ця стаття присвячена огляду основних методів збору, аналізу та зберігання цифрових доказів, розгляду найбільш ефективних інструментів, а також аналізу викликів та інновацій у цій галузі. Метою статті є вивчення та аналіз сучасних методів та інструментів цифрового криміналістичного аналізу, їх викликів та інновацій, зокрема щодо їх застосування в сучасних умовах кримінальних розслідувань. У статті розглядаються методи та інструменти криміналістичного аналізу цифрових доказів, а також виклики та інновації в цій сфері. З розвитком технологій і збільшенням обсягу цифрових даних, розслідування злочинів стає все більш складним завданням. Стаття аналізує основні методи криміналістичного аналізу, такі як фізичне вилучення даних, логічний аналіз та мережевий аналіз. Особлива увага приділяється використанню сучасного програмного забезпечення, такого як EnCase, FTK, Wireshark, Cellebrite UFED, а також методам машинного навчання для автоматизації процесів аналізу даних. Обговорюються правові та етичні аспекти використання цифрових доказів, а також нові можливості, які надають хмарні технології та Інтернет речей. Інновації в цій галузі сприяють підвищенню ефективності криміналістичних розслідувань і наданню достовірних доказів для судових процесів. Зроблено висновок, що криміналістичний аналіз цифрових доказів стикається з численними викликами, пов'язаними з розвитком технологій, великими обсягами даних та правовими питаннями. Проте, інновації в галузі машинного навчання, хмарних технологій, Інтернету речей та інтегрованих платформ аналізу надають нові можливості для ефективного розслідування та збору доказів. Розвиток цих технологій та методів дозволить криміналістам краще справлятися з сучасними викликами та підвищити ефективність криміналістичних розслідувань.

Ключові слова: хмарні платформи, спільний доступ, співпраця, організації, інтегровані платформи, методи аналізу, ефективність, обмін інформацією.

Prokopenko N.M. Methods and forensic analysis of digital evidence: challenges and innovations
Summary

The relevance of the article lies in the fact that the analysis of digital evidence is associated with numerous challenges. The constant development of technology, the growth of the volume of data and new methods of encryption complicate the process of detecting and analyzing such evidence. In addition, the rapid evolution of cybercrime requires forensic scientists to constantly improve their skills and use new tools and methods. In this context, there is a need to study and evaluate modern methods and tools of forensic analysis of digital evidence, as well as innovations that can facilitate the investigation process. This article reviews the main methods of collecting, analyzing and storing digital evidence, examines the most effective tools, and analyzes the challenges and innovations in this field. The purpose of the article is to study and analyze modern methods and tools of digital forensic analysis, their challenges and innovations, in particular regarding their application in modern conditions of criminal investigations. This article examines methods and tools for forensic analysis of digital evidence, as well as challenges and innovations in this field. With the development of technology and the increase in the volume of digital data, the investigation of crimes is becoming an increasingly complex task. The article analyzes the main methods of forensic analysis, such as physical data extraction, logical analysis and network analysis. Special attention is paid to the use of modern software such as EnCase, FTK, Wireshark, Cellebrite UFED, as well as machine learning methods to automate data analysis processes. Legal and ethical aspects of the use of digital evidence are discussed, as well as new opportunities provided by cloud technologies and the Internet of Things. Innovations in this field contribute to increasing the effectiveness of forensic investigations and providing reliable evidence for legal proceedings. It is concluded that the forensic analysis of digital evidence faces numerous challenges related to the development of technology, large volumes of data and legal issues. However, innovations in machine learning, cloud technologies, the Internet of Things, and integrated analytics platforms provide new opportunities for effective investigation and evidence gathering. The development of these technologies and methods will allow forensic scientists to better cope with modern challenges and increase the effectiveness of forensic investigations.

Key words: cloud platforms, shared access, cooperation, organizations, integrated platforms, methods of analysis, efficiency, information exchange.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України: від 19.06.2024. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text
2. Колодіна А.С., Федорова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*. 2020. № 1. С. 176-180.
3. гриців О. І. Криміналістика в комп'ютерних системах : процеси, готові рішення. *Вісник* Національного університету «Львівська політехніка». Автоматика, вимірювання та керу-вання. 2013. № 774. С. 120–126.
4. Тіхонов С.В., Кобець М.В. Застосування апаратно-програмного комплексу «CELLEBRITE UFED» під час виявлення та розслідування кримінальних правопорушень: методичні рекомендації. 2023. К.: НАВС. URL: http://elar.naiau.kiev.ua/jspui/handle/123456789/25590
5. Дронюк І.М., Федевич О. Ю. Аналіз трафіку комп'ютерної мережі на основі експериментальних даних середовища WIRESHARK». *Вісник Національного університету "Львівська політехніка"*. 2015. № 1. URL: https://science.lpnu.ua/uk/sisn/vsi-vypusky/vypusk-814-2015/analiz-trafiku-kompyuternoyi-merezhi-na-osnovi-eksperymentalnyh