ISSN 2524-0374

УДК 343.98:004.056.5(477)
DOI https://doi.org/10.32782/2524-0374/2025-9/91

ШЛЯХИ ПОДОЛАННЯ СУЧАСНИХ ПРОБЛЕМ ЦИФРОВОЇ КРИМІНАЛІСТИКИ – ЗАРУБІЖНИЙ ПОГЛЯД

WAYS TO OVERCOME CURRENT PROBLEMS OF DIGITAL FORENSICS – A FOREIGN VIEW

Пядишев В.Г., д.ю.н, професор,
професор кафедри кримінального аналізу
та інформаційних технологій
Одеський державний університет внутрішніх справ

Калугін В.Ю., к.ю.н., доцент,
професор кафедри кримінального аналізу
та інформаційних технологій
Одеський державний університет внутрішніх справ

Козін О.Б., к.фіз.-мат.н., доцент,
доцент кафедри фізико-математичних нау
Державний університет інтелектуальних технологій і зв'язку

Становлення і розвиток цифрової криміналістики стали важливим кроком у розвитку криміналістики. Воно ж наслідком бурхливого зростання та впровадження цифрових технологій у всіх сферах соціального життя. Проте досягнення цифрових технологій стали також активно застосовуватись і у кримінальному світі. Це стало неминуче позначатися і на цифровій криміналістиці, створюючи для неї нові, невідомі досі проблеми. Зазначені проблеми потребують свого рішення. Оскільки цифрова криміналістики зародилася у державах з найвищим рівнем інформатизації суспільства, то і проблеми цифрової криміналістики, і рішення щодо її подолання у першу чергу висвітлися саме у тих державах.

Отже, метою дослідження є встановлення і систематизація сучасних проблем цифрової криміналістики та засобів, методів, технік їх подолання. .при проведенні дослідження застосовувалися метод системного підходу, а також історичний та функціональний методи. У ході роботи встановлені загальні вимоги до цифрових доказів, щоб вони могли застосовуватись у судовому розгляді. Було розглянуто проблеми, пов'язані з великими обсягами та складністю даних, а також напрями їх подолання через застосування інтелектуального аналізу даних, застосування розподіленої обробки, методи обробки неструктурованих даних. Розглянуто проблеми, обумовлені прискоренням технічного прогресу, а також відповідні технологічні, стратегічні та оперативні контрзаходи. Окремо розглянуто кримінальні виклики цифровій криміналістиці, такі, як очищення диска, шифрування файлів, стеганографія, стиснення файлів, шкідливе програмне забезпечення та найвідоміші інструменти для злочинної протидії цифровій криміналістиці. Розглянуто відповідні профілактичні заходи (до інциденту) та слідчі контрзаходи (під час та після інциденту) тощо. Розглянуто причини проблем, обумовлених людськими помилками, неефективними робочими процесами та прогалинами в ресурсах, а також рішення для покращення ситуації.

Ключові слова: цифрові докази, цифрова криміналістика, проблеми великих обсягіви та складності даних, протидія цифровій криміналістиці, контрзаходи.

The formation and development of digital forensics have become an important step in the development of forensics. It is a consequence of the rapid growth and implementation of digital technologies in all spheres of social life. However, the achievements of digital technologies have also begun to be actively used in the criminal world. This has inevitably affected digital forensics coming across new, previously unknown problems for it. These problems require solutions. Since digital forensics originated in countries with the highest level of informatization of society, both the problems of digital forensics and solutions to overcome them first emerged in those countries.

Therefore, the purpose of the study is to identify and systematize modern problems of digital forensics and the means, methods, and techniques for overcoming them. While conducting the study, the method of a systems approach was used, as well as historical and functional methods. In the course of the work, general requirements for digital evidences were established so that they could be used in court proceedings. The problems associated with large volumes and complexity of data were considered, as well as ways to overcome them through the application of intellectual data analysis, the use of distributed processing, methods for processing unstructured data. The problems caused by the acceleration of technological progress were considered, as well as the corresponding technological, strategic and operational countermeasures. Criminal challenges to digital forensics were separately considered, such as disk wiping, file encryption, steganography, file compression, malware and the most famous tools for criminal countermeasures against digital forensics. The corresponding preventive measures (before the incident) and investigative countermeasures (during and after the incident), etc. were considered. The reasons of problems caused by human errors, inefficient workflows and resource gaps, as well as solutions to improve the situation were considered.

Key words: digital evidence, digital forensics, problems of large volumes and complexity of data, opposition to digital forensics, countermeasures.

Постановка проблеми. Необхідність застосування цифрової криміналістики обумовлена залежністю суспільства від можливостей, що надають цифрові технології в усіх аспектах сучасного сферах людської діяльності. Останнє призводить до стрімкого зростання злочинів, що залишають за собою цифрові докази. Саме цифрова криміналістика займається ідентифікацією, отриманням, аналізом та представленням електронних даних з цифрових пристроїв для розслідування кримінальних, цивільних або внутрішніх справ. Вона забезпечує можливість ретельно збирати, зберігати та досліджувати цифрові докази з комп'ютерів, смартфонів та мереж, забезпечуючи їх цілісність та юридичну допустимість у суді. Отже, забезпечується можливість реконструювати події, розкрити деталі злочину чи інциденту та встановити винних. При цьому на шляху цифрової криміналістики зустрічаються численні проблеми, зокрема, пов'язані з великими обсягами та складністю даних, обумовлені прискоренням технічного прогресу, кримінальними викликами цифровій криміналістиці, а також людськими помилками, неефективними робочими процесами та прогалинами в ресурсах. Вже сьогодні для розв'язання певної кількості з перелічених проблем напрацьовано певні рішення, які потребують свого детального вивчення, вдосконалення та розповсюдження.

Стан дослідження теми. Відносно новий напрям криміналістики – цифрова криміналістика – спочатку сформувався у державах з максимальним рівнем інформатизації. Але помітні наукові досягнення у цій галузі зроблені і українськими науковцями, такими як Бутузов В. М., Авдєєва Г. К., Власова С. В., Іщенко Є. П., Колодіна А.С., Нечаєва Н. Б., Перлін С.І., Пясковський В. В. , Степанюк Р. Л., Шепітько В. Ю., Шматко О.В., Якименко І З. Вони розкривають напрями застосування цифрової криміналістики, а також певні проблеми, що виникають на цьому шляху. Але у державах, де цифрові технології взагалі та цифрова криміналістика зокрема почали розвиватися раніше, напрацьовано певну кількість напрямів подолання проблем, що виникають на шляху застосування цифрової криміналістики.

Метою статті є дослідження і систематизація шляхів подолання сучасних проблем при застосуванні цифрової криміналістики.

Викладення основного матеріалу

1. **Загальні вимоги до цифрових доказів**

Приступаючи до проблем цифрової криміналістики та до шляхів їх подолання, по-перше слід звернутися до загальних вимог до цифрових доказів. Щоб цифрові докази (ЦД) були **допустимими в суді**, слід дотримуватись жорсткого, стандартизованого процесу цифрової криміналістики, який забезпечу є автентичність, цілісність та повноту шляхом збору, збереження, аналізу та звітності, одночасно підтримуючи ланцюг зберігання, щоб гарантувати точність доказів та запобігти змінам. Необхідно виконувати ключові правові та технічні вимоги, включаючи юридичний дозвіл на вилучення, релевантність ЦД та дотримання встановлених процедур [1, с. 2-5].

При цьому можуть виникати наступні проблеми:

– Неадекватність процедур, тобто недотримання належних юридичних процедур, недотримання належного ланцюга зберігання та забезпечення цілісності даних може зробити ЦД неприйнятними.

– Модифікація ЦД, тобто випадкові або навмисні зміни цифрових даних під час криміналістичного процесу можуть знищити їхню доказову цінність.

– Складність, обумовлена абстрактним та технічним характером ЦД, що вимагає спеціалізованих знань та суворого дотримання протоколів, щоб ЦД були прийняті у суді.

Отже, щоб бути прийнятими у суді, ЦД мають бути надійними (тобто результати мають бути узгодженими при послідовному застосуванні методу або інструменту) та достовірними (тобто вони мають точно відображати оригінальні дані) [2, с. 7]. Досягнення зазначених властивостей ЦД слід добиватися наступним:

Процедури повинні відповідати встановленим принципам, стандартам та передовим практикам цифрової криміналістики [3, с. 7].

Інструменти, що використовуються для аналізу, повинні бути надійними та точно оцінювати свої базові алгоритми, рівень помилок та відповідність найкращим практикам.

Судові експерти та слідчі повинні ретельно перевіряти свої інструменти та методології, щоб продемонструвати їхню надійність та точність.

Цілісність ЦД від збору до пред'явлення в суді, їхню надійність та достовірність може гарантувати тільки дотримання суворого ланцюга зберігання.

2. Проблеми, пов'язані з великими обсягами та складністю даних

Великі обсяги. Серйозним викликом для аналізу цифрової криміналістики є постійне зростання обсягу вилучених та представлених для аналізу даних. Це є результатом постійного розвитку технологій зберігання даних, включаючи збільшення ємності сховищ у споживчих пристроях та хмарних сервісах зберігання даних, а також збільшення кількості пристроїв, вилучених у кожній справі. Як наслідок, це призвело до збільшення обсягів доказів, що очікують аналізу, часто від багатьох місяців до років, що впливає навіть на найбільші лабораторії цифрової криміналістики. Отже, експоненціальне зростання даних у сучасних підприємствах ставить серйозний виклик для фахівців з цифрової криміналістики [4, с. 3]. З поширенням цифрових пристроїв та взаємопов'язаних систем обсяг даних, доступних для криміналістичного аналізу, досяг безпрецедентного рівня. Наприклад, одна корпоративна мережа може щодня генерувати терабайти даних, включаючи журнали, електронні листи, документи та мультимедійні файли [5, с. 274].

Сортування цього потоку інформації вимагає складних стратегій управління даними та потужних аналітичних інструментів, здатних ефективно обробляти та співвідносити різні джерела даних.

Тобто, рішення щодо подолання проблеми містять такі поради: застосування інтелектуального аналізу даних, скорочення обсягу даних, збільшення обчислювальної потужності, застосування розподіленої обробки, штучного інтелекту, інших інноваційних методів.

Неструктурованість даних. Інша релевантна проблема – дані, що генеруються різними програмами реального часу, сайтами соціальних мереж та сенсорними пристроями, маючи величезний обсяг, неструктуровані, що ускладнює обробку даних реляційними системами управління базами даних (SQL). Тому потрібна система управління базами даних NoSQL, яка також може обробляти напівструктуровані дані. Реляційні бази даних забезпечують найпростіший спосіб керування даними, але зі зростанням використання NoSQL виникає необхідність міграції даних з реляційних до NoSQL баз даних. Сьогодні пропонуються різні механізми для здійснення міграції даних з реляційних до NoSQL баз даних

Шифрування даних. Хоча шифрування є важливим для конфіденційності та кібербезпеки, воно створює слідчий бар'єр, який вимагає від експертів цифрової криміналістики розробки передових методів, таких як спеціалізовані методології отримання даних у реальному часі та відновлення ключів для отримання цифрових доказів для юридичних та слідчих цілей [6, с. 7].

Складність даних. Розміри потенційних носіїв цифрових доказів зросли експоненційно, будь то жорсткі диски в настільних комп'ютерах та ноутбуках чи твердотільні пам'яті в мобільних пристроях, таких як смартфони та планшети, навіть за умови значного відставання часу затримки. Хмарні сервіси зараз є джерелами потенційних доказів у широкому спектрі розслідувань, а мережевий трафік також слідує зростаючій тенденції, та в кібербезпеці необхідність швидкого просіювання величезної кількості даних зараз є першочерговою [7, с. 6].

Для розпізнавання складних шаблонів у мережевій криміналістиці. підходять нейронні мережі. Тут використовується контрольований підхід, де послідовні знімки файлової системи використовуються для навчання мережі розпізнавати нормальну поведінку програми. Після події система може бути використана для автоматичного побудови часової шкали виконання на криміналістичному зображенні файлової системи.

3. **Проблеми, обумовлені швидким технічним прогресом**

Говорячи про проблеми, що обумовлені зазначеним чинником, зазвичай згадують наступні *новітні технології* [8, с. 2]:

– хмарні обчислення, при яких дані зберігаються на різних платформах [9, с. 2];

– блокчейн та криптовалюти;

– інтернет речей (IoT);

– Мобільні та розумні пристрої (шифрування, мережі 5G тощо);

– дарквеб;
– штучний інтелект та машинне навчання [10, с. 3].

Зазначене створює наступні *виклики*.

– збільшення обсягу та складності даних;
– розвиток кримінальної тактики;
– нові джерела цифрових доказів;
– правові та етичні перешкоди.

Одночасно з боку цифрової криміналістики робляться *наступні кроки*:

– автоматизація аналізу даних та кримірналістичних робочих процесів;
– створення спеціалізованих інструментів, таких як Chainalysis для блокчейну, Maltego та SpiderFoot для відстеження даних;
– вдосконалення виявлення дипфейків.

Хмарні технології. У контексті теми роботи вони заслуговують на окреме місце тому, що з ними пов'язані наступні *ключові проблеми*:

– розпорошення та волатильність даних;
– розсіяність даних.;
– ефемерність даних;
– обмеженість контролю та доступу;
– відсутність фізичного контролю;
– перешкоди для отримання даних;
– технічна складність;
– наявність шифрування;
– багатокористувацька оренда кількома користувачами
– правові та регуляторні питання [11, с. 4];
– юрисдикційні конфлікти (коли дані зберігаються в різних юрисдикціях);
– відсутність стандартизації для хмарної криміналістики;
– співпраця та стандартизація;
– потрібна тісна співпраця постачальників;
– потрібні нові інструменти для хмарної криміналістики.

Сьогодні зарубіжні фахівці поділяють заходи протидії викликам, обумовленим технічним прогресом, за наступними напрямами.

Технологічні контрзаходи:

– застосування штучного інтелекту (ШІ) та машинного навчання (МН);
– впровадження хмарної криміналістики;
– впровадження мобільної та IoT-криміналістики;
– впровадження блокчейн-криміналістики;
– впровадження квантово-стійких методів криміналістики;
– розробка інструментів віртуалізації – для створення знімків віртуальних машин, аналізу пам'яті та відстеження змін на рівні гіпервізора;
– впровадження «криміналістики в режимі реального часу» (поєднання цифрової криміналістики з кібербезпекою) [12, с. 13];
– впровадження «криміналістики як послуги» – нової концепції в галузі кібербезпеки.

Стратегічні та оперативні контрзаходи:

– забезпечення готовності організацій до цифрової криміналістики;
– інвестування у безперервне навчання та розвиток навичок;
– удосконалення та впровадження відповідних інструментів та систем;
– адекватний розподіл ресурсів (включаючи фінансування спеціалізованих інструментів та персоналу)..

Отже, сьогодні на трансформацію цифрової криміналістики впливають такі важливі тенденції:

1. хмарна криміналістика;
2. штучний інтелект та машинне навчання;
3. криміналістика Інтернету речей;
4. аналітика прийняття рішень;
5. цифрова криміналістика як послуга (DFaaS).

4. **Кримінальні виклики цифровій криміналістиці**

Окрім вищезазначених проблем, спостерігаються і такі, що викликані діяльністю злочинців безпосередньо проти цифрової криміналістики [13, с. 2-8].

Найвідоміші методи боротьби з цифровою криміналістикою. Серед методів боротьби з криміналістикою, що використовуються для приховування цифрових слідів, найбільш важливими вважаються наступні п'ять [14, с. 2-3]:

1) очищення диска;
2) шифрування файлів;
3) стеганографія;
4) стиснення файлів;
5) шкідливе програмне забезпечення.

На жаль, цей список не є остаточним. До того ж, сьогодні навіть існує певна кількість антифоренсичних інструментів, що наведено, наприклад, у таблиці [15, с. 215].

Таблиця 1

Інструменти для злочинної протидії цифровій криміналістиці

Антикриміналістичні методи	Доступні інструменти
Видалення джерела доказів	Knoppix, Портативне програмне забезпечення
Видалення артефактів	Eraser,File Shedder, R –wipe, DBAN
Приховування доказів	Slacker, Truecrypt
Заплутування слідів	Transmogrify, Timestomp
Атака на криміналістичні методи/інструменти	42.zip USBKill

Відповідно, боротьба з «антикриміналістикою» передбачає використання таких захисних інструментів та заходів безпеки.

Профілактичні заходи (до інциденту):

– встановлення мережевих брандмауерів;
– встановлення програмного забезпечення для захисту від шкідливого ПЗ;
– безпечна конфігурація та виправлення;
– навчання персоналу;
– повне шифрування диска;
– вимкнення невикористовуваних мережевих функцій, як Wi-Fi та Bluetooth.

Слідчі контрзаходи (під час та після інциденту):

– розуміння методів злочинної боротьби з криміналістикою, таких, як Зміна файлів журналів з метою видалення / приховування слідів шкідливої діяльності, приховування даних через застосування стеганографії;
– використання «Інструментів цифрової криміналістики реагування на інциденти» (DFIR);
– використання розширених методів та інструментів аналізу для виявлення та обходу антифоренсичних методів та інструментів;
– безперервне навчання щодо нових антифоренсичних методів та інструментів.

Знищення даних, як засіб протидії криміналістиці розглянемо окремо. Знищення даних має на меті безповоротне стирання даних, з метою запобігти їх поверненню, тоді як цифрова криміналістика прагне витягувати, зберігати та аналізувати дані для виявлення доказів для юридичних розслідувань [16, с. 3].

Протидія знищенню даних. Щоб впоратися з неправомірним використанням стирання даних, пропонується метод, заснований на функціях транзакцій NTFS та алгоритмі машинного навчання [17, с. 7]. Цей метод дозволяє отримувати інформацію про те, «які файли стираються» та «які інструменти стирання даних та стандарти очищення даних використовуються».

Розвиток кіберзлочинності також доцільно віднести до цього розділу, тому що він створює складні загрози, що

ґрунтуються на штучному інтелекті та Інтернеті речей, що зумовлює потребу в удосконаленнях цифрової криміналістики. Отже, новітні тенденції розвитку кіберзлочинності – такі [18, с. 7] :

– автоматизація атак на основі штучного інтелекту;

– експлойти інтернету речей (iot);

– складні (зокрема, адаптивні) та важковиявлювані загрози;

– хмарні та децентралізовані середовища.

Реагування та інновації цифрової криміналістики:

– застосування штучного інтелекту та машинного навчання;

– розвиток хмарної криміналістики;

– здійснення аналізу у режимі реального часу та постійного моніторингу;

– розвиток криміналістики інтернету речей;

– розробка лабораторій/інструментів для роботи з розумними пристроями;

– розробка нових методів для відновлення та аналізу даних.

5. Проблеми, обумовлені людськими помилками та неефективними робочими процесами

Людська помилка та когнітивне упередження є значними проблемами в цифровій криміналістиці, що потенційно призводить до неправильного тлумачення доказів, неточних висновків та помилкових обвинувальних вироків,

Приклади джерел когнітивних упереджень:

– контекстуальне упередження – може впливати на інтерпретацію експертами цифрових доказів;

– емоційне упередження, наприклад, через вплив жахливих зображень;

– упередженість експерта проти істинного доказу через підозру у діпфейку;

– системні проблеми з інструментами через їхній дизайн та алгоритми;

– низька надійність експертів – потенціал для людської помилки.

Наслідки упередженості та помилок:

– неточні та оманливі докази (неправильні висновки з цифрових доказів);

– неправильні засудження (через недосконалі цифрові докази);

– ерозія довіри громадськості до надійності цифрових доказів.

Стратегії пом'якшення наслідків:

– наукові та структуровані підходи (зменшення кількості помилок);

– управління контекстом (захист від нерелевантної / упередженої інформації);

– розробка та валідація інструментів цифрової криміналістики;

– прозорість та стандарти (етичних принципів, прозорості в розробці) [19, с. 146];

– дослідження упередженості у цифровій криміналістиці та контрзаходів.

Неефективні робочі процеси в цифровій криміналістиці мають свої причини, наслідки та шляхи подолання [20, с. 3].

Причини неефективних робочих процесів:

– величезні обсяги даних (особливо через хмарні технології);

– ручні та повторювані завдання, що призводить до втрати часу та помилок;

– розрізнені інструменти та системи вимагають ручної передачі даних;

– складність нових технологій – нові типи пристроїв та форматів даних;

– відсутність стандартизації через ізольованість традиційних підходів.

Наслідки неефективності:

– затримки та відставання;

– збільшення витрат – через трудомісткий характер ручних завдань та реактивне прийняття рішень.

– вигорання та втрата продуктивності:

– порушення цілісності доказів – через людські помилки – через неефективність.

Рішення для покращення:

– автоматизація для повторюваних завдань та обробки даних;

– централізоване управління справами – через централізовану платформу, як Magnet One.;

– системи управління робочими процесами – для налаштування завдань обробки даних;

– стандартизація процесів сприятиме переходу до «конвеєрної стрічки;

– інтеграція аналізу даних та розширеної аналітики в існуючі системи.

Висновки. Стрімке зростання застосувань цифрових технологій у житті суспільства, а також їх застосування у злочинній діяльності породили новий напрям криміналістики – цифрову криміналістику. Це – досить складна сфера діяльності. До того ж, сьогодні визначено широкий спектр проблем, що виникають на шляху застосування цифрової криміналістики. Їх можна поділити за укрупненими напрямами.

Для розв'язання проблем, пов'язаних з великими обсягами та складністю даних, сьогодні передбачено застосування інтелектуального аналізу даних, застосування розподіленої обробки, методи обробки неструктурованих даних.

Проблеми, що обумовлені прискоренням технічного прогресу та кримінальними викликами цифровій криміналістиці, пропонується усувати сукупністю певних технологічних та стратегічних контрзаходів, застосуванням штучного інтелекту та розвитком хмарної криміналістики тощо.

Проблеми, що обумовлені людськими помилками та неефективними робочими процесами та прогалинами в ресурсах. пропонується зменшувати автоматизацією повторюваних завдань, централізацією управління інтеграцією аналізу даних тощо.

Подальший розвиток застосування цифрових досягнень у кримінальній діяльності є неминучим. Зазначене вимагає від фахівців у кримінальній криміналістиці готовності постійно оновлювати свій арсенал програмних засобів, а також розширювати свої знання та відточувати навички.

ЛІТЕРАТУРА

1. Kennedy, I. Presenting digital evidence in court. *BSC*. 23 January 2023. P. 9. URL: https://www.bcs.org/articles-opinion-and-research/presenting-digital-evidence-in-court/ (дата звернення: 02.09.2025).

2. Hughes, N., Karabiyik, U. Towards reliable digital forensics investigations through measurement science. Wiley. WIRE's Reviews Forensic Science. January 2020. P. 11. DOI:10.1002/wfs2.1367. Site. URL: https://wires.onlinelibrary.wiley.com/doi/epdf/10.1002/wfs2.1367 (дата звернення: 02.09.2025).

3. Standards and best practices for digital forensics. *United Nations Office on Drugs and Crime*. 2018. P. 10. URL: https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html (дата звернення: 02.09.2025).

4. Semakula, J. Hurdles in Digital Forensic Investigations: Discovering Strategies for Implementation and Practice.*Linkedin.Com*. March 22, 2024. URL: https://www.linkedin.com/pulse/hurdles-digital-forensic-investigations-discovering-john-semakula-c0orf/ (дата звернення: 02.09.2025).

5. Quick, D., Kim-Kwang Raymond Choo. Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*. Volume 11, Issue 4, December 2014, Pages 273-294. URL: https://www.sciencedirect.com/science/article/abs/pii/S1742287614001066 (дата звернення: 02.09.2025).

6. Noland, A. Current Challenges of Digital Forensics. Themis: Research Journal of Justice Studies and Forensic Science.Volume 12. Issue 1. Article 1. 5-20-2024. P. 1-15. URL: https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1120&context=themis (дата звернення: 02.09.2025).

7. Guarino, A. Digital Forensics as a Big Data Challenge. research gate. January 2013. DOI: 10.1007/978-3-658-03371-2_17. URL: https://www.researchgate.net/profile/Alessandro-Guarino/publication/312819425_Digital_Forensics_as_a_Big_Data_Challenge/links/5f4f9062299bf13a31974d3a/Digital-Forensics-as-a-Big-Data-Challenge.pdf?origin=publication_detail&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uRG93bmxvYWQiLCJwcmV2aW91c1BhZ2UiOiJwdWJsaWNhdGlvbiJ9fQ (дата звернення: 02.09.2025).

8. The Impact of Emerging Technologies on Digital Evidence. *EclipseForensics*. December 11, 2024. Site. URL: https://eclipseforensics.com/the-impact-of-emerging-technologies-on-digital-evidence/ (дата звернення: 02.09.2025).

9. Bharadiya, J., Cinar, B. Cloud Computing Forensics; Challenges and Future Perspectives: A Review. *ResearchGate. Asian Journal of Computer Science and Information.* May 2023.Technology 16(1):P. 1-14. DOI:10.9734/ajrcos/2023/v16i1330. Sitre. URL: https://www.researchgate.net/publication/371004671_Cloud_Computing_Forensics_Challenges_and_Future_Perspectives (дата звернення: 02.09.2025).

10. AI and Machine Learning in Digital Forensics: Tackling the Backlog. deckchair.ai. September 11, 2025. P. 9. Site. URL: vhttps://deckchair.ai/resources/ai-and-machine-learning-in-digital-forensics-tackling-the-backlog (дата звернення: 02.09.2025).

11. Adelusi, J.B. Legal and Ethical Considerations in Digital Forensics and Risk Mitigation. researchgate. February 2025. P. 6. Site. URL: https://www.researchgate.net/publication/389853645_Legal_and_Ethical_Considerations_in_Digital_Forensics_and_Risk_Mitigation (дата звернення: 02.09.2025).

12. Nishchal Soni, N. Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges. Journal of Forensic Legal & Investigative Sciences. Jun 05, 2025. P. 24. DOI:10.24966/FLIS-733X/100105. URL: https://www.heraldopenaccess.us/openaccess/digital-forensics-confronting-modern-cyber-crimes-technological-advancements-and-future-challenges (дата звернення: 02.09.2025).

13. Top 15 Skills For Computer Forensics Careers. Champlain College Online. August 15, 2025. P. 11. Site. URL: https://online.champlain.edu/blog/top-skills-required-for-computer-forensics-careers https://online.champlain.edu/blog/top-skills-required-for-computer-forensics-careers (дата звернення: 02.09.2025).

14. Five Anti-Forensic Techniques Used to Cover Digital Footprints. Computer Forensics. *Cybersecurity-Exchange* March 24, 2022. P. 1-5. Site. URL: https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/anti-forensic-techniques-used-to-cover-digital-footprints/ (дата звернення: 02.09.2025).

15. Abdullahi, Z.H., Nidhi Sagarwal N., Soni M. An Overview of Anti-forensic Techniques and their Impact on Digital Forensic Analysis. *4th OnlineMultidisplinary Research Conference. Osmania University Centre International for International Program*. 23th October 2020. P. 207-217. URL: file:///C:/Users/User/Downloads/ZHAbdullahi2_2.pdf (дата звернення: 02.09.2025).

16. Field, T. Forensics: When is Data Truly Lost? *BankInfoSecurity.*December 26, 2012. Sit. URL: https://www.bankinfosecurity.com/forensics-when-data-truly-lost-a-5380 (дата звернення: 02.09.2025).

17. Yadav, A., Yadav, E., Singh, N., Nazeer, Kh. AI in machine learning-A Forensic Approach. *ResearchGate.Net*. October 2024Gradiva 10(10):234-241. Site. URL: https://www.researchgate.net/publication/393843734_AI_in_machine_learning-A_Forensic_Approach (дата звернення: 02.09.2025).

18. Ahmed, A.A., Farhan, Kh., Jabbar, W.A. et al. IoT Forensics: Current Perspectives and Future Directions. *MDPI.* 12 August 2024. P. 31. Site. URL: https://www.mdpi.com/1424-8220/24/16/5210 (дата звернення: 02.09.2025).

19. Rowe, N. Privacy Concerns with Digital Forensics. February 2016. DOI:10.4018/978-1-4666-9905-2.ch008. In book: Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance (pp.145-162). URL: https://www.researchgate.net/publication/306313595_Privacy_Concerns_with_Digital_Forensics (дата звернення: 02.09.2025).

20. Standards and best practices for digital forensics. *United Nations Office on Drug and Crime*. 2018. P. 10. Site. URL: https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html (дата звернення: 02.09.2025).

Дата першого надходження рукопису до видання: 24.09.2025
Дата прийнятого до друку рукопису після рецензування: 26.10.2025
Дата публікації: 29.10.2025