УДК 343.98:004.056.5(477)
DOI https://doi.org/10.32782/1813-338X-2025.3.22

В. Г. Пядишев
доктор юридичних наук, професор,
професор кафедри кримінального аналізу
та інформаційних технологій,
Одеського державного університету внутрішніх справ,
ORCID ID: 0000-0002-5174-1891

О. А. Балтовський
доктор технічних наук, доцент,
професор кафедри кримінального аналізу
та інформаційних технологій,
Одеського державного університету внутрішніх справ,
ORCID ID: 0000-0003-1762-1295

СУЧАСНІ ПРОБЛЕМИ ЦИФРОВОЇ КРИМІНАЛІСТИКИ – ЗАРУБІЖНИЙ ПОГЛЯД

Цифрова криміналістика – це найновіший напрямок у криміналістиці, викликаний бурхливим зростанням та широким використанням цифрових технологій у всіх соціальних сферах. Подальший стрімкий розвиток цифрових технологій, а також широке використання їх у злочинній діяльності стали породжувати в усьому світі нові проблеми для цифрової криміналістики. Відповідно, мета дослідження – встановити та систематизувати виявлені за кордоном сучасні проблеми цифрової криміналістики. У дослідженні використовувалися історичний та функціональний методи, а також метод системного підходу. У ході роботи встановлені проблеми були організовані по групах: проблеми, пов'язані з особливостями даних, технологічні (технічні) та методологічні проблеми, проблеми компетентності співробітників, проблеми ресурсного забезпечення, правові та етичні проблеми. До складу проблем, викликаних особливостями даних, входять такі. Суть проблем, зумовлених складністю даних, полягає в тому, що цифровими доказами є необроблені дані, одержувані з пристроїв, різних за своєю природою. І ця різноманітність зростає з кожним днем. Також широко поширюється шифрування даних. З іншого боку, злочинці застосовують різні способи знищення даних. Щодо технологічних та методологічних проблем, то вони зумовлені, насамперед, широким застосуванням хмарних обчислень, Інтернету речей, розробкою та використанням злочинцями методів протидії цифровій криміналістиці, а також відсутністю належної стандартизації. Проблеми компетентності працівників виявляються, насамперед, у нестачі кваліфікованого персоналу, у людських помилках, зумовлених, зокрема, різноманіттям пристроїв та форматів, у неефективності робочих процесів. Проблеми ресурсного забезпечення, по суті, не дозволяють належним чином вирішувати всі перелічені вище проблеми, оскільки перешкоджають придбанню новітньої техніки, програмного забезпечення, здійсненню необхідного навчання персоналу. Правові та етичні проблеми мають своїми компонентами такі питання, як надійність та достовірність доказів, різні правові рамки, зміну правових ландшафтів, допустимість доказів у суді, а також проблеми конфіденційності. Цифрова криміналістика, будучи, зокрема, породженням бурхливого впровадження цифрових технологій у злочинну діяльність, через подальший розвиток цих технологій набуває нових і нових проблем, подолання яких потребує значних зусиль.

Ключові слова: *цифрова криміналістика, цифрові докази, дані, методологічні проблеми, компетентність, правові та етичні проблеми, ресурсне забезпечення.*

Постановка проблеми. Потреба в цифровій криміналістиці виникає через зростаючу залежність суспільства від цифрових технологій практично у всіх аспектах сучасного життя, що призводить до сплеску злочинів, пов'язаних з електронними доказами. Цифрова криміналістика є життєво важливою галуззю, яка сприяє правоохоронним органам, корпораціям

та юридичним особам у розслідуванні та переслідуванні злочинної діяльності, реагуванні на порушення даних та інциденти безпеки, а також відновлення після атак для запобігання майбутнім випадкам. Це забезпечується завдяки таким можливостям цифрової криміналістики, як виявлення та запобігання кіберзлочинам, надання допустимих юридичних доказів, сприяння реагуванню на інциденти для пом'якшення наслідків порушень, захист корпоративних даних та інтелектуальної власності, відновлення втрачених або видалених даних, допомогу у дотриманні нормативних вимог, ідентифікація порушників, роз'яснення методології атак, розкриття масштабів інцидентів, підсилення кіберзахисту. Одночасно цифрова криміналістика на шляху свого застосування зустрічає певні проблеми, навмисні завади, та навіть протидію. Зазначене ускладнює її застосування. Проте для ефективного їх подолання, необхідно усвідомити увесь спектр зазначених перешкод.

Стан дослідження теми. Цифрова криміналістика є відносно новим напрямом діяльності і, відповідно, науки. Однак в Україні вже є певні наукові напрацювання у цій галузі, серед авторів якої слід згадати таких науковців та практиків, як Авдєєва Г. К., Бутузов В. М., Власова С. В., Іщенко Є. П., Колодіна А.С., Нечаєва Н. Б., Перлін С.І., Степанюк Р.Л., Шматко О.В., Якименко І.З. Деякі з них певною мірою торкаються і проблем цифрової криміналістики, і досить вдало розкрили деякі проблеми її застосування. Проте закордонні фахівці на підставі матеріалів, зібраних правоохоронними органами та окремими корпораціями, висвітлюють цілий спектр проблем, що виникають при застосуванні цифрової криміналістики.

Метою статті є дослідження і систематизація сучасних проблем, що виникають при застосуванні цифрової криміналістики.

Викладення основного матеріалу.

Проблеми, пов'язані з даними

Великий обсяг даних. Створення даних зросло до небачених раніше рівнів завдяки публікаціям у соціальних мережах, онлайн-взаємодії та розгалуженій мережі підключених гаджетів. Масштаби цього інформаційного буму вражають [1, с. 3]. Зокрема згідно зі 171-сторінковим звітом «Стан Інтернету речей у літніх умовах 2024» від IoT Analytics, до кінця 2023 року було підключено 16,6 мільярда пристроїв Інтернету речей (зростання на 15% порівняно з 2022 роком) [2, с. 3]. Це негативно впливає на роботу систем цифрової криміналістики [3, с. 4].

Складність даних. Докази існують у вигляді складних, необроблених цифрових даних на різних пристроях, таких як телефони, комп'ютери та хмарні системи, що вимагає використання спеціалізованих інструментів для їх пошуку та аналізу в розслідуваннях цифрової криміналістики, яка займається отриманням, зберіганням та аналізом електронних даних, корисних у кримінальних розслідуваннях. Це включає інформацію з комп'ютерів, жорстких дисків, мобільних телефонів та інших пристроїв зберігання даних [4, с. 1]. Зазначене спонукає криміналістів застосовувати спеціалізовані інструменти, такі як:

– Cellebrite UFED – широко використовуваний інструмент для вилучення та аналізу даних з мобільних пристроїв;

– Magnet AXIOM – комплексна платформа цифрової криміналістики, яка збирає та аналізує дані з різних джерел;

– EnCase Forensic – встановлений набір інструментів для поглибленої комп'ютерної криміналістики та аналізу даних;

– Інструменти на основі SQL – необхідні для вилучення та аналізу даних з баз даних SQLite, які поширені на мобільних пристроях.

При цьому є актуальним питання інтеграції даних – об'єднання даних з різних джерел в єдине подання, спрямоване на забезпечення узгодженої та єдиної версії правдивої інформації, доступної для всієї організації [5, с. 1].

Шифрування даних. Подвійна природа шифрування слугує метафорою для ширшого цифрового світу: сфери величезного потенціалу, як для прогресу, так і для шахрайства. Отже, шифрування діє і як захист даних, і як інструмент, що сприяє шахрайській діяльності [6, с. 2]. Злочинці використовують складне шифрування для захисту своїх даних та комунікацій, створюючи значні перешкоди для слідчих. Такі методи, як Розширений Стандарт Шифрування (AES) та складніші методи, такі як Повністю Гоморфне Шифрування (FHE), захищають дані шляхом їх перестановки за допомогою математичних алгоритмів, що перешкоджатиме здатності розкривати злочини [7, с. 282]. Динамічний характер технологій шифрування означає, що експерти-криміналісти повинні постійно розробляти нові стратегії та інструменти для дешифрування даних. [8, с. 2].

Знищення даних. Злочинці часто намагаються знищити цифрові докази, стираючи дані з пристроїв або фізично пошкоджуючи їх, щоб перешкоджати розслідуванню, що є кримінальним

злочином у багатьох юрисдикціях і може призвести до суворих покарань. Методи включають і дистанційне стирання даних з телефонів. За законами, наприклад, Австралії злочин навмисного пошкодження доказів викладено у статті 129 Кримінального кодексу. Щоб визнати підсудного винним у навмисному пошкодженні доказів, обвинувачення повинно довести такі елементи [9, с. 2]:

– підсудний знав, що відповідна річ може бути потрібна як доказ у судовому провадженні;

– підсудний пошкодив відповідну річ;

– підсудний зробив це з наміром перешкодити використанню відповідної речі як доказу.

Технологічні та методологічні виклики

Хмарні обчислення. Дослідження даних у хмарних середовищах, відомі як хмарна криміналістика – процес забезпечення хмарної безпеки, який використовує різні методи безпеки для дослідження хмарного середовища після кіберінциденту [10, с. 2]. Ключовими аспектами хмарної криміналістики є такі:

– спеціалізовані інструменти хмарної криміналістики;

– збір доказів (журнали, знімки системи та дані з хмарного сховища);

– аналіз за допомогою штучного інтелекту та машинного навчання;

– відповідність технічним вимогам та правовим стандартам;

– волатильність та розподіл і поширення даних;

– багатокористувацька оренда та віртуалізація – хмарні середовища часто передбачають спільні ресурси;

– правова та регуляторна складність, транскордонне управління даними тощо;

– залежність від постачальника хмарних послуг;

– проблеми взаємодії зацікавлених сторін.

Ця взаємодія часто створює значні проблеми хмарної криміналістики, включаючи неузгодженість між сторонами, що може призвести до затримок [11, с. 5].

Методи протидії цифровій криміналістиці (антифорензика). Їх розроблено для запобігання відновленню даних та для забезпечення неприйнятності доказів у суді. До їх складу входить багатий інструментарій. [12, с 14]. Отже, прикладами методів антифорензики є:

– стирання/очищення даних, щоб зробити їх невідновними.

– шифрування конфіденційних даних;

– руткіти – для приховування свою присутність та інших шкідливих дії;

– стеганографія – для ускладнити виявлення прихованих даних

– часові мітки – зміна часових позначок цифрових артефактів;

– VPN – для приховування справжньої IP-адреси та місцезнаходження;

– приховане каналізування - надсилання даних через приховані канали;

– обфускація на базі штучного інтелекту.

Цілями антифорензики є наступні:

– знищення або зміна доказів;

– приховування особи та місцезнаходження;

– приховування шкідливої діяльності від програмного забезпечення безпеки та слідчих;

– затримка або запобігання кримінальному переслідуванню.

На особливу увагу заслуговує здійснення цифрового обману через застосування генеративного штучного інтелекту у соціальній інженерії та фішингу [13, с. 2].

Відсутність належної стандартизації – призводить до непослідовності, зниження надійності та достовірності доказів, потенційних юридичних проблем щодо допустимості, неможливості порівняльного аналізу та негативного впливу на право обвинувачених на справедливий суд. Це також перешкоджає науковій перевірці, оскільки немає стандарту для тестування нових методів або забезпечення цілісності даних, що створює значну перешкоду для всієї галузі. Без стандартизованих методів докази цифрової криміналістики можуть не відповідати критеріям Стандарту Добера, що ускладнює доведення їхньої достовірності в суді [14, с. 4].

Проблеми з компетентністю персоналу

Нестача кваліфікованого персоналу. Для усвідомлення гостроти проблеми достатньо згадати назву статті «Індійська служба цифрової криміналістики стикається з дефіцитом 90 000 фахівців» [15, с. 2]. Цей пробіл призводить до затримок розслідувань, проблем із допустимістю доказів та потенційних судових помилок, що підкреслює необхідність більших інвестицій у навчання, розробку інструментів та стандартизовані судово-медичні процеси. Причинами зазначеного дефіциту вважаються наступні:

– швидкий технологічний прогрес потребує від слідчих нових знань;

– відсутність скоординованого реагування – часто працюють незалежні спеціалізовані команди;

– недостатня підготовка та ресурси – брак інвестицій у навчання, інструменти та достатня кількість персоналу;

– організаційна фрагментація – у деяких регіонах поліцейські сили працюють ізольовано, маючи різні інструменти та пріоритети;

– попит на послуги цифрової криміналістики значно перевищує можливості

Досвід Великої Британії довів, що «багато сил не мали достатнього рівня розуміння роботи щодо вилученням доказів з мобільних телефонів» [16, с. 2].

Людські помилки та упередженість. Дослідження судових помилок у цифровій криміналістиці та оманливих доказів у Великій Британії та США, висвітлили людські помилки як проблему в криміналістиці [17, с. 101].

Неефективні робочі процеси. Причинами неефективних робочих процесів вважаються наступні [18, с. 2]:

– величезний обсяг даних – множина цифрових доказів з різних джерел;

– ручні та повторювані завдання;

– недостатній обмін даними – небезпечні методи, такі як фізичні usb-накопичувачі та електронна пошта для обміну доказами;

– відсутність автоматизації – неможливість автоматизувати рутинні завдання;

– фрагментовані та недоступні докази – дані зберігаються в різних місцях;

– проблеми з навігацією по хмарним даним, зашифрованим програм обміну ускладнює ефективність та дотримання вимог.

Різноманітність пристроїв та форматів. Відповідні специфічні ускладнення пов'язані з наступним [19, с. 37]:

– великий обсяг даних та різноманітність пристроїв;

– проблеми роботи зі сховищами даних;

– волатильність даних та віддалений доступ;

– складність роботи з необробленими даними, отриманими з пристроїв

– виникнення нових технологій вимагає нових методів та інструментів;

– виникнення мобільні пристрої створює нові унікальні проблеми..

Все це призводять до значних затримок у роботі цифрової криміналістики.

Ресурсні проблеми цифрової криміналістики

Ключовими ресурсними прогалинами вважаються такі:

– перевантаження даними – слідчі стикаються з постійно зростаючим обсягом різнорідних цифрових даних, що створює значні проблеми зі зберіганням, управлінням та аналізом;

– застарілі інструменти та технології – правоохоронні органи намагаються встигати за швидкими темпами технологічного прогресу, що вимагає постійного оновлення інструментів та методів цифрової криміналістики;

– відсутність стандартизованих практик – критично бракує єдиних, міжнародно визнаних стандартів, правил та рамок для збору, зберігання, аналізу та представлення цифрових доказів;

– недостатня підготовка та компетентність – персоналу, від слідчих до прокурорів та суддів, часто необхідних технічних навичок та постійного професійного розвитку для ефективної роботи з цифровими доказами;

– науково-методологічні прогалини – існує потреба в більш комплексних практичних та наукових розробках;

Існування зазначених прогалин призводить до наступного:

– порушення надійності доказів;

– збільшення часу обробки;

– недостатнє використання цифрових доказів;

– неефективне розкриття злочинів.

Недостатнє фінансування цифрової криміналістики створює кризу, що призводить до накопичення нерозглянутих справ, проблем із якістю та судових помилок, заважаючи агентствам придбати необхідні технології, навчати персонал та йти в ногу з цифровим прогресом. [20, с.3].

Правові та етичні проблеми

Необхідність транскордонного обміну даними суперечить правилам захисту даних, що ускладнює доступ до критичної інформації [21, с. 4]. Нормативні акти, як GDPR ЄС [22, с. 1], встановлюють суворі правила обробки персональних даних, що може суперечити потребам розслідувань, тоді як такі концепції, як Закон США про хмарні технології (CLOUD Act) [23, с. 1-2], намагаються вирішити питання доступу до даних для правоохоронних органів у міжнародному контексті.

Надійність та достовірність. Не всьому цифровому контенту можна довіряти. Автентифікувати цифрові докази означає показати, що файл є оригінальним, незмінним, прив'язаним до певного пристрою, часу, користувача. До того ж без цілісності — гарантії того, що нічого не змінилося з моменту захоплення файлу — його доказова цінність втрачається [31, с. 2].

Дотримання правових норм та стандартів у цифровій криміналістиці гарантує автентичність, надійність та допустимість в суді. Правовими та етичними принципами є такі:

– законність – дотримання місцевих, національних та міжнародних законів;

– автентичність – доведено, що докази знаходяться в їхньому первісному стані, а їх збір та обробка повинні ретельно задокументовані.

– допустимість – гарантовано, що зібрані докази відповідають правовим стандартам;.

Різні правові рамки. Правові рамки цифрової криміналістики суттєво відрізняються залежно від країни, але загалом спираються на національне законодавство, судові прецеденти та встановлені міжнародні стандарти, такі як ISO/IEC 27037 [24, с. 1]. Ключові елементи включають статути, що регулюють обшук та вилучення, збереження доказів, захист даних (наприклад, Закон Великої Британії про захист даних 2018 року [25, с. 1-2]). До ключових аспектів правових рамок цифрової криміналістики належать такі:

– національні закони та статут;

– ланцюг зберігання;

– допустимість доказів;

– закони про захист даних та конфіденційність;

– міжнародні стандарти;

– судова практика та прецеденти.

Зміна правових ландшафтів. Зміна законів створює нові правила доступу до даних, їх збору та обробки. Вплив змін у законах стосується наступного:

– конфіденційність та захист даних;

– шифрування – закони стикаються з проблемою шифрування;

– доступ до даних та ордери;

– міжнародна співпраця.

Природа цифрових розслідувань ставить питання конфіденційності даних та правові питання на перший план у криміналістичній практиці. Завдання – розкрити правду, але й забезпечити відповідність методів законам та мають поважати права на приватність [26, с. 2].

Допустимість доказів у суді. Її критеріями вважаються наступні [27, с. 9]:

– релевантність – докази повинні мати значення для провадження;

– автентичність – повинно бути показано, що файл є оригінальним, справжнім та прив'язаним до певного пристрою, часу чи користувача;

– цілісність – повинно бути доведено, що докази незмінні від отримання;

– надійність – доведена достовірність та точність;

– повнота – докази повинні відображати повну картину фактів.

Проблеми конфіденційності в цифровій криміналістиці є наступними [28, с. 5-6]:

– централізація даних;

– неправильна оцінка даних;

– необґрунтоване повідомлення про результати експертизи;

– порушення конфіденційності третіх осіб;

– прихований пошук;

– продаж приватних судово-медичних даних;

– злочинне використання цифрової криміналістики;

– складність оцінки шкоди порушення конфіденційності;

– відсутність підтримки управління конфіденційністю постачальниками криміналістичних інструментів.

Висновки

Прогрес у розвитку цифрової техніки та стрімке застосування його досягнень злочинним світом обумовили необхідність ефективної боротьби з останнім. Це призвело до народження цифрової криміналістики. При цьому продовження розвитку і застосування злочинцями найновітніших досягнень цифрової техніки спонукає і цифрову криміналістику постійно перебувати у стані динамічного розвитку з тим, щоб встигати компенсувати найновітніші проблеми, що вже виникли та виникатимуть у подальшому та сьогодні укладаються у таку схему.

Проблеми, пов'язані з особливістю даних обумовлені великими обсягами даних, що треба обробити, їхньою складністю, шифруванням та знищенням даних злочинцями. Технологічні та методологічні проблеми, у свою чергу, обумовлені впровадженням у світі (та у злочинному світі) хмарних обчислень, впровадженні злочинцями методів протидії цифровій криміналістиці, відсутністю належної стандартизації. Зазначене призводить до наступних проблем з компетентністю персоналу: нестача кваліфікованого персоналу, людські помилки та упередженість, неефективні робочі процеси, різноманітність пристроїв та форматів. Боротьба з усім цим вимагає все зростаючих ресурсів і, відповідно, упирається в ресурсні проблеми

Список використаної літератури:

1. Dey, R. The Data Deluge: How Much Information Do We Generate Every Day? Rajesh Dey. Jun 11, 2023. Site. URL: https://rajeshdey-27.medium.com/the-data-deluge-how-much-information-do-we-generate-every-day-2b51c643f414 (дата звернення: 10.09.2025).
2. Sinha, S. State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally. *IoT-Analytics. September 3, 2024*. Site. URL:

https://iot-analytics.com/number-connected-iot-devices/ (дата звернення: 10.09.2025).
3. Big Data Uses, Challenges, Technologies. *BuiltIn.Com*. p. 11. Site. URL: https://builtin.com/big-data (дата звернення: 10.09.2025).
4. Digital evidence. *National Institute of Standards and Technology, US Department of Commerce*. Site. URL: https://www.nist.gov/digital-evidence#:~:text=What%20is%20digital%20forensics?,and%20other%20data%20storage%20devices. (дата звернення: 10.09.2025).
5. Johnson, J. How to Integrate Data from Different Sources: What You Need to Know in 8 Actionable Tips. *C Data. June 6, 2024*. Site. URL: https://www.cdata.com/blog/how-to-integrate-data-from-different-sources#:~:text=Data%20integration%20is%20the%20process,large%20datasets%20in%20cloud%20environments. (дата звернення: 10.09.2025).
6. Ibitola, J. Encryption Challenges in Fraud Activities and Their Solutions. *FlagRight. June 23, 2025*. Site. URL: https://www.flagright.com/post/encryption-challenges-in-fraud-activities-and-their-solutions (дата звернення: 10.09.2025).
7. Singh, A., Chauhan, P. S. Breaking the code: Legal responses to encryption in cybersecurity threat scenarios. *International Journal of Law, Justice and Jurisprudence 2024; 4(2*): P. 281-285. Site. URL: https://www.lawjournal.info/article/148/4-2-42-323.pdf#:~:text=Investigators%20and%20intelligence%20agencies%20may%20be%20unable,devices%2C%20hindering%20their%20ability%20to%20solve%20crimes%2C (дата звернення: 10.09.2025).
8. Modern Challenges of Forensic Data Recovery. *Flashback Data LLC*. Site. URL: https://www.flashbackdata.com/forensic-data-recovery-challenges/#:~:text=Encryption%20stands%20as%20one%20of,used%20to%20shield%20digital%20information. (дата звернення: 10.09.2025).
9. Destruction of Evidence (QLD). *Armstrong Legal*. Site. URL: https://www.armstronglegal.com.au/criminal-law/qld/offences/destruction-of-evidence/#:~:text=The%20offence%20of%20damaging%20evidence,thing%20being%20used%20in%20evidence (дата звернення: 10.09.2025).
10. Cloud forensic analysis: all you need to know. *Ackcent.Com*. P. 10. Site. URL: https://ackcent.com/cloud-forensic-analysis-all-you-need-to-know/#:~:text=cloud%20security%20management.-,What%20is%20cloud%20forensics?,investigation%20within%20the-%20cloud%20environment. (дата звернення: 10.09.2025).
11. Cloud Forensics Challenges: An In-depth Analysis. *SearchInform. 2024/.*p. 24. Site. URL: https://searchinform.com/articles/cybersecurity/analytics/digital-forensics/cloud-forensics/challenges/#:~:text=Cloud%20forensics%20investigations%20typically%20involve,and%20streamline%20the%20investigation%20process. (дата звернення: 10.09.2025).
12. SentinelOn. Cybersecurity Forensics: Types and Best Practices. SentinelOne. August 17, 2025. P. 16. Site. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-forensics/#:~:text=These%20techniques%20include%20wiping%20off,investigators%20from%20gathering%20meaningful%20evidence. (дата звернення: 10.09.2025).
13. Schmitt, M.., Flechais, I. Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. *Research Gate. January 2023*. p. 18. Site. URL: https://www.researchgate.net/publication/375570831_Digital_Deception_Generative_Artificial_Intelligence_in_Social_Engineering_and_Phishing (дата звернення: 10.09.2025).
14. Noland, A. Current Challenges of Digital Forensics. Themis: Research Journal of Justice Studies and Forensic Sciences. Volume 12, Issue. 5-2024. P. 15. Site. URL: https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1120&context=themis#:~:text=Challenges%20of%20Standardization-,Reliability%20and%20Credibility,351). (дата звернення: 10.09.2025).
15. India's Digital Forensics sees 90,000 talent shortage. *The Finance Story.Com. 30th August, 2025*. P. 12. Site. URL: https://thefinancestory.com/india-digital-forensics-market-to-reach-%E2%82%B911800-crore-by-2030 (дата звернення: 10.09.2025).
16. Police forces overwhelmed and ineffective when it comes to digital forensics, new report finds. *His Majesty's Inspectorate of Constabulary and Fire & Rescue Services. 1 December 2022.* P. 4. Site. URL: https://hmicfrs.justiceinspectorates.gov.uk/news/news-feed/police-forces-overwhelmed-and-ineffective-when-it-comes-to-digital-forensics/#:~:text=But%20in%20our%20inspection%2C%20we,start%20taking%20this%20more%20seriously.%E2%80%9D2030 (дата звернення: 10.09.2025).
17. Sunde, N., Dror, I.E. Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation. Volume 29, June 2019, Pages 101-108*. Site. URL: https://www.sciencedirect.com/science/article/pii/S1742287619300441 (дата звернення: 10.09.2025).

18. Lorentz, P. Navigating the Challenges of Modern Digital Investigations. *Cellebrite.Com. March 26, 2025.* P. 10. Site. URL: https://cellebrite.com/en/navigating-the-challenges-of-modern-digital-investigations/ (дата звернення: 10.09.2025).
19. Montasari, R., Hill, R., Parkinson, S., Peltola, P. Digital Forensics: Challenges and Opportunities for Future Studies. *IGI Global Scientific Publishing. International Journal of Organizational and Collective Intelligence. January 2020. P. 37-53*. Site. URL: file:///C:/Users/User/Downloads/Digital_Forensics_Challenges_and_Opportunities_for.pdf (дата звернення: 10.09.2025).
20. Hernández, A. Forensic crime labs are buckling as new technology increases demand. A major federal funding cut could make labs' struggles worse. *Stateline*. July 21, 2025. Site. URL: https://stateline.org/2025/07/21/forensic-crime-labs-are-buckling-as-new-technology-increases-demand/#:~:text=It%20can%20lead%20to%20quality,up%20with%20the%20increased%20demand.&text=In%20Colorado%2C%20officials%20are%20dealing,cases%20from%20the%20Memphis%20area. (дата звернення: 10.09.2025).
21. It's all about the data – regulatory barriers to cross-border investigations. *ForensicRisk. December 19, 2024*. Site. URL: https://www.forensicrisk.com/news-and-insights/its-all-about-the-data---regulatory-barriers-to-cross-border-investigations#:~:text=Data%20privacy%20is%20a%20fundamental,personal%20data%20across%20external%20borders. (дата звернення: 10.09.2025).
22. General Data Protection Regulation GDPR. *Intersoft Consulting services AG*. URL: https://gdpr-info.eu/ (дата звернення: 10.09.2025).
23. What Is the CLOUD Act? *Business Software Alliance. P. 5.* URL: https://www.bsa.org/files/policy-filings/08192025bsacloudact.pdf (дата звернення: 10.09.2025).
24. ISO/IEC 27037:2012. *The International Organization for Standardization*. URL: https://www.iso.org/ru/standard/44381.html (дата звернення: 10.09.2025).
25. Data Protection Act 2018. *UK Public General Acts 2018 c. 12.* Site. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents (дата звернення: 10.09.2025).
26. Exploring the Frontier: 7 – Navigating Legal and Privacy Issues in Digital Forensics. *LCGDiscovery.Com. Sep 20, 2024. P. 8.* Site. URL: https://lcgdiscovery.com/exploring-the-frontier-7-navigating-legal-and-privacy-issues-in-digital-forensics/ (дата звернення: 10.09.2025).
27. Admissibility of Digital Evidence: a Definitive Guide. *TrueScreen.IO. 2025. P. 23*. Site. URL: https://truescreen.io/admissibility-of-digital-evidence/ (дата звернення: 10.09.2025).
28. Rowe, N.C. Current Privacy Concerns with Digital Forensics. *US Naval Postgraduate School, United States. 2020. P. 19*. URL:https://faculty.nps.edu/ncrowe/forensicpriv.pdf (дата звернення: 10.09.2025).

Piadyshev V. H., Baltovskyi O. A. Current problems of digital forensics – a foreign view

Digital forensics is the newest direction in forensics, caused by the rapid growth and widespread use of digital technologies in all social spheres. The further rapid development of digital technologies, as well as their widespread use in criminal activities, began to generate new problems for digital forensics worldwide. Accordingly, the purpose of the study is to identify and systematize the modern problems of digital forensics identified abroad. The study used historical and functional methods, as well as the method of a systems approach. In the course of the work, the identified problems were organized into groups: problems related to data features, technological (technical) and methodological problems, problems of employee competence, problems of resource provision, legal and ethical problems. The problems caused by data features include the following. The essence of the problems caused by the complexity of data is that digital evidence is raw data obtained from devices of different nature. And this diversity is growing every day. Data encryption is also widely used. On the other hand, criminals use various methods of data destruction. As for technological and methodological problems, they are caused, first of all, by the widespread use of cloud computing, the Internet of Things, the development and use by criminals of methods to counter digital forensics, as well as the lack of proper standardization. Problems of employee competence are manifested, first of all, in the lack of qualified personnel, in human errors caused, in particular, by the variety of devices and formats, in the inefficiency of work processes. Problems of resource provision, in fact, do not allow to properly solve all the problems listed above, as they prevent the acquisition of the latest equipment, software, and the implementation of the necessary training of personnel. Legal and ethical problems have as their components such issues as the reliability and authenticity of evidence, different legal frameworks, changing legal landscapes, admissibility of evidence in court, as well as confidentiality issues. Digital forensics, being, in particular, a product of the rapid introduction of digital technologies into criminal activity, due to the further development of these technologies acquires new and new problems, overcoming which requires significant efforts.

Key words: *digital forensics, digital evidence, data, methodological problems, expertise, legal and ethical problems, resource.*

Дата першого надходження рукопису до видання: 21.07.2025
Дата прийнятого до друку рукопису після рецензування: 25.08.2025
Дата публікації: 30.09.2025