https://doi.org/10.31649/1997-9266-2026-185-2-55-64

УДК 004.056:343.98

Ю. В. Синявіна[1]
І. В. Чалий[1]
Т. А. Бутенко[1]
В. М. Сирий[1]
Н. М. Проценко[1]

АНАЛІЗ ІНСТРУМЕНТІВ І ТЕХНОЛОГІЙ ОТРИМАННЯ ДАНИХ З МОБІЛЬНИХ ПРИСТРОЇВ У КОНТЕКСТІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

[1]Державний біотехнологічний університет, Харків

Проаналізовано сучасні технології отримання даних з мобільних пристроїв у контексті цифрової форензики та розслідування кіберзлочинів. Обґрунтовано зростання ролі мобільних пристроїв як ключових носіїв цифрових доказів у кримінальних провадженнях, пов'язаних з протиправною діяльністю у кіберпросторі. Подано класифікацію основних методів екстракції даних та їхні технічні особливості, що дозволяє обирати оптимальні підходи до їх використання. Проаналізовано специфіку застосування актуальних технологічних рішень мобільної форензики в Україні, з урахуванням інституційних, технічних, правових та освітніх аспектів, євроінтеграції, воєнного стану, постійного ускладнення технічних викликів, пов'язаних із захистом даних та адаптацією правового поля до реалій цифрових доказів. Досліджено функціональні можливості провідних комерційних, відкритих і допоміжних рішень у забезпеченні повноти та достовірності цифрового аналізу. Особливу увагу приділено процесуальній придатності цифрових доказів, а також адаптації інструментів до умов національної юридичної практики та специфіки науково-дослідної роботи у сфері кібербезпеки. Описано власний досвід інтеграції університетської освіти з національними проєктами, які є частиною загальної екосистеми кібербезпеки в Україні й об'єднують просвітництво та взаємодію з правоохоронцями. Зазначено роль хмарної форензики в аспекті можливості підвищення повноти доказової бази та дотримання національних процесуальних вимог доступу до персональних даних. Обґрунтовано доцільність інтегрованого підходу до використання інструментів мобільної форензики для підвищення ефективності, надійності та об'єктивності розслідувань у цифровому середовищі. Визначено перспективні напрями розвитку методів отримання доказів в умовах посилення криптографічного захисту.

Ключові слова: мобільна форензика, кіберзлочини, цифрові докази, екстракція даних, інструменти мобільної форензики, правова адаптація.

Вступ

Стрімка еволюція мобільних технологій суттєво трансформувала підходи до розслідування злочинів. Сучасний смартфон вже давно вийшов за межі звичайного засобу комунікації й фактично став персональним центром зберігання даних, що містить значні масиви відомостей про свого власника — від інформації про місцезнаходження та фінансові операції до біометричних параметрів і записів комунікацій. У сфері кіберзлочинності мобільні пристрої можуть відігравати подвійну роль: слугувати інструментом здійснення протиправних дій (зокрема у випадках фішингу чи DDoS-атак) або бути їх безпосереднім об'єктом. Сучасний стан кіберзлочинності демонструє чітку тенденцію до переорієнтації атак із традиційних десктопних систем на мобільні платформи.

Смартфон перетворився на ключовий носій цифрових доказів як у справах загальнокримінального характеру, так і під час розслідування інцидентів, пов'язаних з національною безпекою. В українському контексті ця проблематика набуває особливої важливості, оскільки мобільні пристрої активно застосовуються і як складові системи бойового управління (інструмент забезпечення ситуаційної обізнаності), так і як цілі для ворожих інформаційно-психологічних операцій (ІПСО) та кібершпигунства.

Однією з центральних задач правоохоронних органів є отримання цифрових доказів у спосіб, що забезпечує їхню достовірність, цілісність і юридичну значущість. Проблематика ускладняється постійним розвитком систем захисту мобільних операційних систем (Android та iOS), що зумовлює необхідність безперервного оновлення застосовуваних інструментів і методик експертного аналізу.

Актуальність теми зумовлена постійним протистоянням між розробниками мобільних операційних систем (iOS та Android) і фахівцями з цифрової криміналістики. З одного боку, виробники впроваджують дедалі складніші механізми захисту, наприклад, повне шифрування диска, Secure Enclave [1] та апаратні модулі безпеки (HSM) [2], що мають на меті захист приватності користувача. З іншого боку, кіберзлочинці використовують ці самі технології для приховування слідів своєї діяльності. Проблема, що постає перед правоохоронними органами та експертами, полягає у високій мінливості цифрових даних та ризику їх безповоротного знищення у разі спроби несанкціонованого доступу. Традиційні методи отримання даних часто виявляються неефективними проти нових версій прошивок або зашифрованих месенджерів (Signal, Telegram, WhatsApp).

Під час розслідування кіберзлочинів, де зловмисники застосовують мобільні пристрої для координації атак або зберігання компрометуючих матеріалів, критичною є ефективна екстракція даних, яка суттєво ускладнюється через апаратне шифрування, механізми блокування та хмарне зберігання даних.

Метою дослідження є систематизація актуальних технологічних рішень мобільної форензики, визначення специфіки її застосування в Україні та перспективних напрямів розвитку методів отримання доказів в умовах посилення криптографічного захисту.

Аналіз останніх досліджень

У сучасному світі кіберзлочини становлять серйозну загрозу, а мобільні пристрої є ключовим джерелом цифрових доказів. Згідно з даними Digital 2025 Global Overview Report за 2025 рік, приблизно 5,78 млрд людей користуються мобільними телефонами, що становить 70,5 % від загальної чисельності населення світу. Смартфони зараз становлять майже 83,7 % доступних у світі мобільних телефонів [3].

Як зазначається в роботі [4], для вдосконалення методів здійснення злочинів передусім застосовуються смартфони. Наслідки цього явища започаткували науку «мобільна форензика», яка стала невід'ємною частиною вітчизняної криміналістики. Зі зростанням обсягів даних, що зберігаються на смартфонах та планшетах, виникає необхідність у використанні ефективних методів отримання, аналізу та збереження інформації.

Основна мета мобільної форензики — забезпечення вилучення даних без їх пошкодження чи спотворення. Для цього застосовуються технології, які дозволяють дослідникам отримати доступ до файлової системи повідомлень, історії дзвінків, геолокаційних даних, відновлювати видалені дані, аналізувати логи, реконструювати події тощо.

З огляду на широке використання смартфонів для комунікації, фінансових операцій, навігації та споживання медіаконтенту, в сучасних кримінальних, контртерористичних і корпоративних розслідуваннях мобільна форензика виступає ключовим джерелом цифрових доказів, набула вирішального значення для виявлення доказово значущих даних.

Розвиток мобільної цифрової криміналістики в Україні має специфічні риси, пов'язані з правовими вимогами, організаційною структурою силових органів та сучасним контекстом кіберзагроз, зокрема в період активних воєнних дій. Сьогодні мобільна форензика є одним з ключових напрямів роботи кіберпідрозділів Національної поліції, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації, військових структур, а також приватних лабораторій цифрової криміналістики.

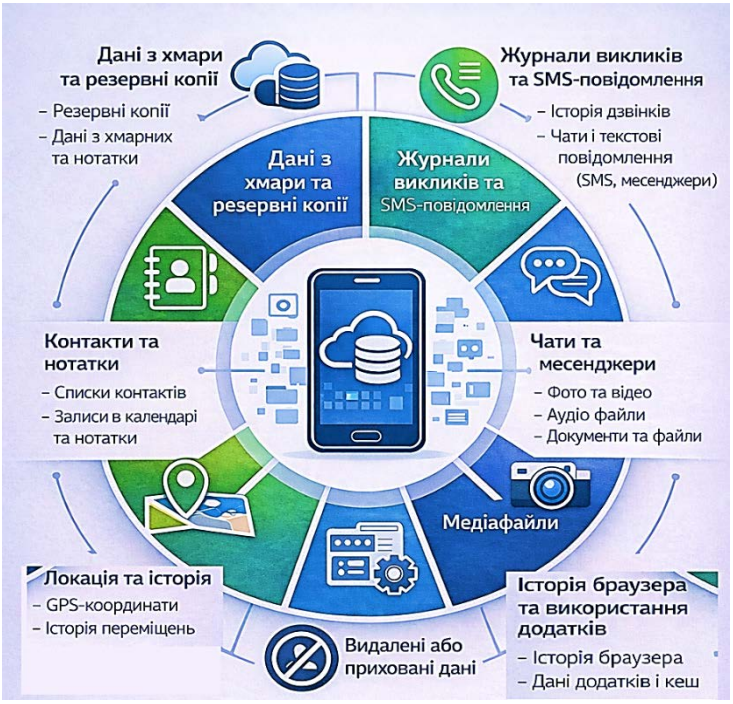
Вітчизняні наукові дослідження переважно зосереджені на правових та процесуальних аспектах використання мобільних даних як цифрових доказів. У працях українських авторів наголошується на необхідності дотримання принципів цілісності, автентичності та відтворюваності електронних доказів, що безпосередньо впливає на допустимість результатів мобільної форензики у судовій практиці [5], [6].

Оскільки мобільні пристрої містять широкий спектр інформації, що відображає активність користувача, у сучасних розслідуваннях кіберзлочинів, доцільно розглянути питання класифікації даних, які можуть бути вилучені та передані на криміналістичну експертизу [7].

Результати досліджень

Для ефективного проведення цифрового розслідування дані потрібно систематизувати за категоріями: контактна інформація, журнали викликів та повідомлень, медіафайли, дані локальних і хмарних додатків, історія браузера та геолокаційні відомості, а також системні та службові артефакти, зокрема метадані і кеш. Така структуризація дозволяє не лише забезпечити цілісність та відтворюваність отриманих доказів, але й оптимізувати вибір методів та інструментів мобільної криміналістики залежно від цілей конкретного розслідування.

На рисунку показані основні категорії цифрових даних, які можуть бути отримані та проаналізовані в процесі мобільної форензики. До них належать дані резервного копіювання та хмарної синхронізації, журнали викликів і текстові повідомлення, вміст месенджерів, мультимедійні файли, геолокаційна інформація, історія браузера та використання додатків, контакти й нотатки, а також видалені або приховані дані. Аналіз зазначених категорій дозволяє відтворити дії користувача та встановити хронологію подій у межах цифрового розслідування.



Основні категорії цифрових даних, що підлягають аналізу в мобільній форензиці

Різноманітність інформації, що зберігається на смартфонах, визначає вибір методів і програмних засобів форензики, а також стратегічний підхід до збору доказів. Визначення та класифікація типів даних на мобільних пристроях дозволяє не лише зрозуміти, яка інформація має доказове значення, а й вибрати оптимальні методи її вилучення та аналізу. Від типу даних залежить, чи буде застосовано фізичне або логічне копіювання, роботу з хмарними резервними копіями чи спеціалізовані інструменти для відновлення видалених файлів.

Ефективність використання інструментів мобільної форензики значною мірою залежить від вибраного методу отримання даних, який визначається типом операційної системи, рівнем захисту пристрою та станом даних. У зв'язку з цим доцільним є детальний розгляд методів екстракції даних з мобільних пристроїв, що застосовуються у процесі розслідування кіберзлочинів.

Вибір конкретного методу залежить від типу операційної системи, рівня захисту пристрою та характеру досліджуваних даних, що детально регламентується міжнародними рекомендаціями з цифрової форензики [8].

Логічне вилучення даних є базовим методом мобільної форензики, який дозволяє отримати доступ до інформації завдяки стандартним механізмам операційної системи. Цей підхід широко застосовується на початкових етапах розслідування завдяки своїй швидкості та мінімальному впливу на пристрої.

Файлове та фізичне вилучення забезпечують глибший рівень доступу до даних, зокрема можливість аналізу системних файлів і відновлення видалених артефактів. Водночас застосування цих методів часто ускладнюється використанням сучасних механізмів шифрування та апаратного захисту [9].

Хмарна екстракція передбачає вилучення даних з віддалених сервісів, таких як Google Drive чи iCloud, за допомогою автентифікаційних токенів або облікових даних. Таке вилучення критичне для кіберзлочинів з віддаленим зберіганням інформації [10].

Додаткові технології містять оминання механізмів блокування (PIN-коди, біометрія), дешифрування (з певними обмеженнями) та карвінг (метод відновлення видалених або пошкоджених файлів шляхом пошуку за сигнатурами) для відновлення видалених фрагментів даних.

Згідно з рекомендаціями NIST та міжнародними стандартами, виділяють чотири основні рівні

отримання даних: логічне, файлове, фізичне та хмарне вилучення [11], [12].

У табл. 1 показано, що жоден з методів отримання даних з мобільних пристроїв не є універсальним. Практика цифрової форензики свідчить про доцільність комбінованого застосування декількох методів з урахуванням технічних характеристик пристрою та цілей розслідування кіберзлочинів.

Таблиця 1

Порівняльна характеристика методів отримання даних з мобільних пристроїв

Метод отримання даних	Рівень доступу	Типи даних	Переваги	Обмеження
Логічна екстракція	Користувацький рівень ОС	Контакти, журнали викликів, SMS, мультимедіа, дані застосунків	Швидкість, мінімальний вплив на пристрій, простота реалізації	Відсутність доступу до видалених і прихованих даних
Файлова екстракція	Рівень файлової системи	Бази даних застосунків, системні файли, історія активності	Глибший аналіз структури даних, можливість часткового відновлення	Обмежена підтримка нових версій ОС, потребує спеціалізованих інструментів
Фізичне копіювання	Рівень фізичної пам'яті	Повний образ пам'яті, включно з видаленими даними	Найповніший доступ до інформації, можливість глибокого аналізу	Висока складність, проблеми з шифруванням, ризик втрати даних
Отримання даних з хмарних сервісів	Серверний рівень	Резервні копії, листування, журнали синхронізації	Незалежність від стану пристрою, доступ до історичних даних	Залежність від облікових даних і правового доступу

Порівняльний аналіз методів отримання даних свідчить про доцільність їх комплексного використання з метою підвищення повноти та достовірності цифрових доказів у процесі розслідування кіберзлочинів.

Застосування методів і технологій отримання даних з мобільних пристроїв створює методологічну основу цифрового криміналістичного дослідження, проте їх практична реалізація безпосередньо залежить від конкретних програмно-апаратних інструментів.

Кожний з розглянутих методів: логічний, файловий, фізичний або аналіз резервних копій, — має власні технічні обмеження та особливості реалізації, які визначаються функціональними можливостями використовуваних засобів. У зв'язку з цим виникає необхідність детального аналізу сучасних інструментів мобільної форензики, які забезпечують реалізацію зазначених методів, з метою оцінювання їхньої ефективності, сумісності з різними операційними системами та придатності для застосування у процесі розслідування кіберзлочинів.

Аналіз інструментів для екстракції даних з мобільних пристроїв починається з визначення ключових критеріїв оцінювання, які дозволяють об'єктивно порівняти їхню ефективність у розслідуваннях кіберзлочинів. Серед основних критеріїв: підтримувані методи (логічне, фізичне, хмарне), сумісність з операційними системами (Android, iOS, Windows Phone), здатність до відновлення видалених даних, інтеграція з іншими платформами, вартість, зручність інтерфейсу та юридична придатність доказів. Ці критерії базуються на сучасних вимогах цифрової форензики, де інструменти повинні не тільки витягувати дані, але й забезпечувати їхню цілісність для судового використання.

Після визначення ключових критеріїв оцінювання, які забезпечують об'єктивний підхід до аналізу, подальшим кроком є класифікація інструментів за їхнім типом та функціональністю. Така класифікація дозволяє систематизувати інструменти, враховуючи їхню доступність, рівень підтримки та застосування у професійних середовищах.

Зокрема, інструменти можна розділити на комерційні, з відкритим кодом та гібридні, кожний з яких має свої особливості в контексті мобільної форензики та розслідування кіберзлочинів. Така класифікація полегшує порівняння та вибір оптимальних рішень для конкретних завдань екстракції чи автоматизованого аналізу даних. Комерційні інструменти домінують у професійних розслідуваннях завдяки розширеній підтримці та оновленням, тоді як відкритий код корисний для бюджетних організацій або досліджень. Наразі перевага надається інструментам з AI-аналітикою для автоматизованого виявлення прихованих даних та кореляції з хмарними джерелами, що критично для кіберзлочинів на кшталт фішингу чи поширення шкідливого програмного забезпечення [13].

Варто зауважити, що застосування інструментів мобільної форензики в реальних умовах значною мірою визначається національними особливостями організації цифрових розслідувань, рівнем технічного забезпечення експертних підрозділів та нормативно-правовими вимогами до роботи з електронними доказами.

В Україні використання таких інструментів здійснюється в межах кримінального процесуального законодавства та методичних рекомендацій судово-експертної діяльності, що зумовлює необхідність адаптації програмно-апаратних рішень до наявних ресурсів і процесуальних процедур [14]. Тому подальший аналіз зосереджено на особливостях застосування інструментів мобільної форензики в українській практиці, з урахуванням доступності, функціональних можливостей та доцільності використання їх в умовах вітчизняної системи кіберрозслідувань.

У табл. 2 подано ключові інструменти мобільної форензики з урахуванням практики застосування в Україні.

Таблиця 2

Порівняльна характеристика ключових інструментів мобільної форензики в Україні [15]—[25]

Інструменти	Підтримка ОС	Типи екстракції	Основні категорії даних	Тип ліцензії	Придатність для використання в Україні
Cellebrite UFED	Android, iOS	логічна, файлова, фізична	контакти, SMS, чати, медіафайли, геолокаційні дані, системні дані	комерційний	Висока — є основним інструментом для правоохоронців, та СБУ
Magnet AXIOM	Android, iOS, ПК	імпорт даних (UFED, XRY тощо)	всі категорії даних	комерційний	Висока — у лабораторіях, приватних експертизах
MSAB XRY	Android, iOS	логічна, файлова, обмежена фізична	контакти, SMS, чати, медіафайли, геолокаційні дані, системні дані	комерційний	Середня — обмежена комерційними ресурсами
Autopsy + Mobile Apps	Android, iOS	логічна, файлова (через плагіни)	контакти, чати, файли, метадані	відкритий	Висока — для навчання та первинного аналізу
Andriller	Android	логічна, файловий аналіз	SQLite, XML, кеш, журнали	умовно відкритий чи безкоштовний	Середня —у навчальному секторі
ALEAPP / ILEAPP	Android, iOS	аналіз артефактів (імпорт даних)	чати, системні дані, месенджери	відкритий	Середня — незалежні експертизи для відновлення логів
Oxygen Forensic Detective	Android, iOS	логічна, файлова, часткова фізична	контакти, чати, медіафайли, геолокаційні дані	комерційний	Середня — приватні експерти

Специфіка мобільної форензики в Україні полягає в комплексному поєднанні інституційних, технічних, правових та освітніх аспектів, які стрімко розвиваються в умовах війни та євроінтеграції. Ця сфера характеризується активним впровадженням спеціалізованого програмно-апаратного забезпечення, постійним ускладненням технічних викликів, пов’язаних із захистом даних, та адаптацією правового поля до реалій цифрових доказів.

Українські правоохоронці та експерти використовують провідні світові програмно-апаратні комплекси. Платформа UFED (Universal Forensic Extraction Device) від Cellebrite є основним інструментом, який використовують правоохоронні органи України. Їх застосування дозволяє значно скоротити час збору та аналізу даних, підвищуючи точність і надійність вилучених доказів, а також загальний рівень розкриття правопорушень.

Комерційні рішення (Cellebrite UFED, Magnet AXIOM, MSAB XRY, Oxygen Forensic Detective), демонструють найвищий рівень функціональної повноти та автоматизації, що забезпечує їхню ефективність у складних цифрових розслідуваннях. Водночас практичне застосування цих інструментів в Україні обмежується фінансовими, технічними та кадровими чинниками. У зв’язку з цим відкриті та умовно відкриті інструменти (Autopsy у поєднанні з ALEAPP/ILEAPP, Andriller) залишаються доцільними для первинного аналізу, верифікації результатів і використання в освітньо-науковій діяльності.

У дослідженні під придатністю інструментів мобільної форензики до застосування розуміється сукупна відповідність програмно-апаратних рішень організаційним, технічним, фінансовим та процесуально-правовим умовам здійснення цифрових розслідувань у національній практиці. Оцінювання придатності має експертно-аналітичний характер та ґрунтується на міжнародних стандартах цифрової форензики (NIST, ENFSI) і національній практиці використання електронних доказів [26]—[28].

Придатність для використання інструментів мобільної форензики в Україні оцінюється з урахуванням реальних практик, доступності ліцензій, технічної підтримки, готовності експертних груп, бюджетних обмежень та актуальності для розслідування кіберзлочинів на національному рівні:

– висока — широко застосовується у структурних підрозділах (експертні центри МВС, СБУ, приватні лабораторії), має локальну підтримку та адаптацію;

– середня — застосовується, але не в усіх випадках; може потребувати додаткових ресурсів або інтеграції з іншими інструментами;

– низька/обмежена — практичне застосування обмежене через технічні або ресурсні причини [29].

Сучасна мобільна форензика в Україні стикається з низкою серйозних технологічних перешкод, які постійно еволюціонують. Виробники смартфонів впроваджують дедалі складніші механізми захисту, що ускладнює роботу експертів (табл. 3).

Таблиця 3

Технологічні проблеми мобільної форензики в Україні [30], [31]

Виклики	Опис
Багаторівнева система безпеки Android	Поєднання захисту на рівні додатків (Application Sandbox), ОС (SEAndroid) та апаратному рівні (TrustZone). TrustZone є своєрідною «чорною скринькою» для експертів
Шифрування даних	Шифрування на рівні диска (FDE) та на рівні файлів (FBE) робить дані практично недоступними без ключів дешифрування
Біометрична автентифікація	Шаблони біометричних даних зберігаються в ізольованому середовищі TrustZone, що значно ускладнює доступ до пристрою
Оновлення безпеки	Виробники (Apple, Google) регулярно випускають оновлення протоколів безпеки для iOS та Android, що ускладнює або унеможливлює розблокування пристрою та дешифрування даних навіть для спеціалізованих криміналістичних інструментів
Докази в месенджерах	Інформація в месенджерах може зберігатися як на самому мобільному пристрої, так і на віддалених серверах, часто розташованих за межами юрисдикції України, що ускладнює її отримання

Окрім даних на самому пристрої, важливим джерелом інформації є білінгові дані операторів телекомунікацій. Цей процес збору, аналізу та систематизації даних дозволяє отримати інформацію про номери абонентів, IMEI, час, дату, тривалість дзвінків та ідентифікатори базових станцій.

Правове поле України перебуває в процесі активної адаптації до викликів цифровізації. Кримінальний процесуальний кодекс України (КПК) досі не містить визначення поняття «електронні докази», на відміну від Цивільного, Господарського та Кодексу адміністративного судочинства. Це створює труднощі в правозастосовній практиці, особливо щодо визнання таких доказів допустимими.

Науковці та практики пропонують два шляхи розв’язання цієї проблеми: закріплення поняття «електронні докази» безпосередньо в КПК або прийняття окремого закону, який би детально регулював процедури збору, дослідження, зберігання та аналізу електронних доказів.

Важливу роль відіграє імплементація міжнародних стандартів, зокрема Другого додаткового протоколу до Будапештської конвенції про кіберзлочинність та Регламенту ЄС про європейські ордери на надання та збереження електронних доказів.

Верховний Суд України поступово формує правові позиції щодо оцінки електронних доказів, що є важливим орієнтиром для слідчих та суддів. Інституційно мобільна форензика розвивається через мережу експертних установ, зокрема в системі МВС, Міністерства юстиції, СБУ та інших правоохоронних органів, які взаємодіють між собою та з міжнародними партнерами для обміну досвідом.

Програма «Цифровий детектив» (D30) ініційована у 2021 році Консультативною місією ЄС (EUAM) в Україні та спрямована на підвищення цифрових слідчих спроможностей українських правоохоронців. З 2022 року вона розширила фокус на впровадження нових цифрових професійних стандартів та створення професії «цифровий детектив». До програми залучені Національна поліція, БЕБ, НАБУ, ДБР та провідні університети. Спеціалізовані центри (як-от CyberLab) регулярно проводять міжнародні науково-практичні заходи, де обговорюються інноваційні методики, зокрема дослідження мобільних пристроїв, робота з віртуалізацією, дешифрування даних та використання штучного інтелекту в атаках і захисті. Розробляються спеціалізовані мобільні застосунки (такі як InvestigatorDesk), які мають стати цифровим «робочим столом» слідчого, надаючи інструменти для управління часом, ведення кримінальних проваджень, доступу до баз даних та комунікації з колегами.

Усвідомлюючи потребу у висококваліфікованих фахівцях, в Україні реалізуються масштабні освітні програми. Так Державний біотехнологічний університет активно долучається до національного проєкту «КіберБрама», який є важливою освітньо-просвітницькою ініціативою, що органічно доповнює технічний та інструментальний аспекти мобільної форензики в Україні. Якщо мобільна форензика зосереджена на розслідуванні вже скоєних злочинів та вилученні доказів, то «КіберБрама» працює на випередження, підвищує рівень цифрової грамотності населення та навчає громадян уникати кіберзагроз [32].

Проєкт реалізовано за підтримки Консультативної місії Європейського Союзу (EUAM) в Україні та Міжнародного Фонду «Відродження» та Представництва ЄС в Україні з метою надання кожному українцю знань та інструментів для безпечної роботи в інтернеті. Його ключові завдання безпосередньо корелюють з викликами мобільної форензики: протидія дезінформації (знищення російських пропагандистських осередків та навчання громадян відрізняти фейки від правдивої інформації); запобігання злочинам (зменшення рівня онлайн-шахрайства, булінгу та протидія розповсюдженню наркотичних речовин через мережу; кібергігієна (надання доступу до інформації про захист особистих даних, безпечні комунікації, шифрування та захист від фішингу).

Платформа є практичним інструментом, який об’єднує просвітництво та взаємодію з правоохоронцями. Вона містить адаптовані до широкого загалу методичні матеріали, практичні рекомендації, інструменти перевірки підозрілих веб-сайтів на предмет шахрайства. Зворотний зв’язок через портал дозволяє громадянам повідомляти про кіберінциденти чи шахрайство, що допомагає кіберполіції оперативно реагувати на загрози.

«КіберБрама» виконує важливу просвітницьку функцію, яка є частиною загальної екосистеми кібербезпеки в Україні. Інтеграція з навчанням в університетах за участю представників кіберполіції у проведенні занять формує у майбутніх фахівців цілісне бачення: від запобігання злочинам до їх розслідування. Автори статті у певних правових межах використовують та накопичують власний досвід впровадження такої інтеграції в освітньому процесі.

В умовах війни проєкт навчає громадян критично мислити та не піддаватися на ворожі інформаційні атаки, що є елементом національної безпеки. «КіберБрама» є публічним обличчям зусиль української держави та міжнародних партнерів, завдяки якому знання з кібергігієни є доступними для всіх верств населення і слугує мостом між громадянами та фахівцями з кіберполіції.

Окрему роль відіграє хмарна форензика, яка дозволяє підвищити повноту доказової бази, проте її застосування в Україні потребує суворого дотримання процесуальних вимог доступу до персональних даних.

Важливою методологічною особливістю є відсутність універсального інструменту мобільної форензики, здатного повністю охопити всі етапи отримання та аналізу даних з мобільних пристроїв. Вибір інструменту залежить від конкретних умов розслідування, типу пристрою, його операційної системи та версії програмного забезпечення. Результати досліджень підтверджують доцільність інтегрованого підходу до використання інструментів мобільної форензики, що забезпечує баланс між ефективністю аналізу, економічною доцільністю та процесуальною коректністю отриманих цифрових доказів.

В умовах посилення криптографічного захисту фокус цифрової та мобільної форензики зміщується від прямого зламу шифрування до комплексного аналізу цифрового середовища, побічних артефактів і поведінкових моделей. Саме інтеграція технічних, аналітичних та правових підходів є ключовим напрямом розвитку методів отримання доказів. В умовах посилення криптографічного захисту перспективними напрямами розвитку методів отримання доказів є: орієнтація на побічні (непрямі) цифрові артефакти, розвиток методів live-forensics, хмарно-орієнтовані методи отримання доказів, інтелектуальний аналіз великих масивів даних, аналіз екосистеми пов’язаних пристроїв, дослідження реалізацій криптографічних механізмів, процесуальна та правова адаптація методів. Подальші дослідження мобільної форензики варто зосередити на розробці уніфікованих методик та стандартів, адаптованих до національного законодавства.

Висновки

У результаті проведеного дослідження встановлено, що мобільні пристрої є одним з ключових джерел цифрових доказів у розслідуванні кіберзлочинів, а ефективність їх криміналістичного дослідження безпосередньо залежить від правильного вибору та поєднання методів та інструментів мобільної форензики.

Аналіз методів отримання даних засвідчив, що логічна, файлова та фізична екстракція мають різну інформаційну цінність і доцільність застосування залежно від технічного стану пристрою, рівня його захищеності та процесуальних умов розслідування.

Порівняльний аналіз сучасних інструментів мобільної форензики показав, що комерційні програмно-апаратні комплекси забезпечують найвищий рівень автоматизації, глибини аналізу та процесуальної відтворюваності результатів, що зумовлює їх провідну роль у складних кримінальних провадженнях. Водночас відкриті та умовно відкриті інструменти залишаються важливими складовими цифрових розслідувань, зокрема на етапах первинного аналізу, верифікації результатів та підготовки фахівців у закладах вищої освіти.

Дослідження особливостей застосування інструментів мобільної форензики в Україні свідчить, що їх придатність визначається не лише технічними характеристиками, а й відповідністю вимогам кримінального процесуального законодавства, доступністю для експертних підрозділів та можливістю забезпечення ланцюга збереження цифрових доказів. У цих умовах найдоцільнішим є інтегрований підхід, що передбачає комбіноване використання комерційних, відкритих і хмарних інструментів.

Отримані результати підтверджують, що впровадження інтегрованих схем використання інструментів мобільної форензики сприяє підвищенню повноти та достовірності цифрових доказів, а також підвищує ефективність розслідування кіберзлочинів у сучасних умовах.

Визначено перспективні напрями розвитку методів отримання доказів в умовах посилення криптографічного захисту. Подальші дослідження мобільної форензики варто зосередити на розробленні уніфікованих методик та стандартів, адаптованих до національного законодавства, системному тестуванні інструментів, впровадженні автоматизації та штучного інтелекту для аналізу даних, розвитку хмарної та віддаленої форензики, а також підвищенні кваліфікації фахівців для забезпечення ефективності та процесуальної допустимості цифрових доказів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] *Операційна система Apple про яку мало хто знає та Secure Enclave*. [Електронний ресурс]. Режим доступу: https://iland.ua/articles/operatsiyna-systema-apple-pro-iaku-malo-khto-znaie-ta-secure-enclave/ . Дата звернення 02.01.2026.

[2] А. Сайко, «Розуміння апаратних модулів безпеки в адмініструванні ключів блокчейну». [Електронний ресурс]. Режим доступу: https://blockchain-development-solutions.com/uk/blog/hardware-security-modules-blockchain-key-management . Дата звернення 02.01.2026.

[3] *Digital 2025: Global Overview Report*. [Electronic resource]. Available: https://datareportal.com/reports/digital-2025-global-overview-report . Accessed: 02.01.2026.

[4] В. В. Марков, і Р. Р. Савченко, «Принципи належності електронних доказів, отриманих з мобільних пристроїв», *Право і безпека*, № 1 (52). с. 89-95, 2014.

[5] А. В. Коваленко, «Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання», *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*, вип. 4. с. 237-245, 2018. [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/Vlduvs_2018_4_30 . Дата звернення 05.01.2026.

[6] В. Ю. Шепітько, та ін., *Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі.* Харків, Україна: *Право*, 2024. [Електронний ресурс]. Режим доступу: https://ivpz.kh.ua/wp-content/uploads/2025/01/Монографія-Криміналістів-2024.pdf . Дата звернення 10.01.2026.

[7] *Mobile Device Forensics in Criminal Investigations: Challenges and Innovations. 2025*. [Electronic resource]. Available: https://innefu.com/mobile-device-forensics-in-criminal-investigations-challenges-and-innovations/ . Accessed: 10.01.2026.

[8] *NIST Special Publication 800-101 Revision 1. Guidelines on Mobile Device Forensics*. National Institute of Standards and Technology, 85 p., 2014. [Electronic resource]. Available: https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final . Accessed: 10.01.2026.

[9] *Cellebrite. Mobile Forensic Extraction Methods Overview*, technical documentation, 2023. [Electronic resource]. Available: https://www.cellebrite.com/en/mobile-forensics/ . Accessed: 10.01.2026.

[10] Jason E. James, "Foundations of mobile forensics: an academic approach," *Issues in Information Systems*, vol. 25, Iss. 3 pp. 94-108, 2024. https://doi.org/10.48009/3_iis_2024_108 . [Electronic resource]. Available: https://www.iacis.org/iis/2024/3_iis_2024_94-108.pdf . Accessed: 12.01.2026.

[11] Rick Ayers, Sam Brothers, and Wayne Jansen, "Guidelines on Mobile Device Forensics (Draft)," National Institute of Standards and Technology, 88 p., 2014. [Electronic resource]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf . Accessed: 15.01.2026.

[12] ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. 2012. [Electronic resource]. Available: https://www.iso.org/standard/44381.html . Accessed: 15.01.2026.

[13] *Top 10 Digital Forensic Tools Every Investigator Must Know*. [Electronic resource]. Available: https://www.cyberforensicacademy.com/blog/top-10-digital-forensic-tools-every-investigator-must-know . Accessed: 05.01.2026.

[14] А. С. Колодіна, і Т. С. Федорова, «Цифрова криміналістика: проблеми теорії і практики, » *Київський часопис права*, № 1. с. 176-180, 2022. https://doi.org/10.32782/klj/2022.1.27 . Дата звернення 10.01.2026.

[15] *Cellebrite. UFED Ultimate – Mobile Forensic Extraction and Analysis*. [Electronic resource]. Available: https://www.cellebrite.com/en/ufed . Accessed: 15.01.2026.

[16] *Magnet Forensics. Magnet AXIOM – Digital Investigation Platform*. [Electronic resource]. Available: https://www.magnetforensics.com/products/magnet-axiom/ . Accessed: 15.01.2026.

[17] *MSAB. XRY – Mobile Forensics Software*. [Electronic resource]. Available: https://www.msab.com/products/xry/ . Accessed: 15.01.2026.

[18] *Oxygen Forensics. Oxygen Forensic Detective*. [Electronic resource]. Available: https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective . Accessed: 15.01.2026.

[19] *National Institute of Standards and Technology. Digital Forensics Guidelines*. [Electronic resource]. Available: https://www.nist.gov/itl/ssd/software-quality-group/digital-forensics . Accessed: 15.01.2026.

[20] *SWGDE Best Practices for Mobile Phone Forensics*. [Electronic resource]. Available: https://www.swgde.org/documents/published-complete-listing/12-f-002-swgde-best-practices-for-mobile-phone-forensics/ . Accessed: 15.01.2026.

[21] E. Casey, "Digital Evidence and Computer Crime," 3rd ed. London: Academic Press, p. 840, 2011. [Electronic resource]. Available: https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf . Accessed: 15.01.2026.

[22] J. Lessard, and G. Kessler, "Android forensics: Simplifying cell phone examinations" *Small Scale Digital Device Forensics Journal*, vol. 4, no. 1, pp. 1-12, 2010. [Electronic resource]. Available: https://www.researchgate.net/publication/254591932_Android_Forensics_Simplifying_Cell_Phone_Examinations . Accessed: 15.01.2026.

[23] A. Hoog, *iPhone and iOS Forensics*, Burlington: Syngress, pp. 464, 2011. https://doi.org/10.1016/C2010-0-68895-X . Accessed: 15.01.2026.

[24] N. R. Roy, A. K. Khanna, and L. Aneja, "Android phone forensic: Tools and techniques," *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Greater Noida, India, pp. 605-610, 2016, https://doi.org/10.1109/CCAA.2016.7813792 . Accessed: 15.01.2026.

[25] *Open Source Digital Forensics*, [Electronic resource]. Available: https://www.sleuthkit.org/autopsy . Accessed: 15.01.2026.

[26] NIST SP 800-101 Rev. 1. *Guidelines on Mobile Device Forensics*. [Electronic resource]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf . Accessed: 15.01.2026.

[27] *NIST Computer Forensics Tool Testing (CFTT).* [Electronic resource]. Available: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt . Accessed: 12.01.2026.

[28] *ENFSI Best Practice Manuals for Digital Evidence.* [Electronic resource]. Available: https://enfsi.eu/documents/ . Accessed: 12.01.2026.

[29] *Union Advisory Mission for Civilian Security Sector Reform Ukraine (EUAM Ukraine).* [Electronic resource]. Available: https://www.euam-ukraine.eu . Accessed: 12.01.2026.

[30] В. С. Макаров, «Особливості судово-медичної експертизи мобільних пристроїв, що працюють на операційній системі Android», *Вісник Харківського національного університету внутрішніх справ.* № 111(4), с. 378-384, 2025. https://doi.org/10.32631/v.2025.4.30 . Дата звернення 20.02.2026.

[31] А. Я. Пенчарський, «Месенджери як засоби вчинення кримінальних правопорушень: окремі аспекти досудового розслідування та міжнародно-правове регулювання», *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Журнал. Серія Право*, вип. 19 (31), с. 388-1395, 2025. https://doi.org/10.33098/2078-6670.2025.19.31.388-395 . Дата звернення 20.02.2026.

[32] *Практична підготовка студентів у співпраці з кіберполіцією.* [Електронний ресурс]. Режим доступу: https://biotechuniv.edu.ua/novyny-fakultety-menedzhmentu-administruvannya-ta-prava/kaf-it-news/praktychna-pidgotovka-studentiv-u-spivpratsi-z-kiberpolitsiyeyu/ . Дата звернення 22.02.2026.

Рекомендована кафедрою менеджменту та безпеки інформаційних систем ВНТУ

Дата надходження: 29.01.2026
Дата прийняття до друку після рецензування: 27.03.2026
Дата публікації: 8.04.2026

Синявіна Юлія Вікторівна — канд. екон. наук, доцент, завідувачка кафедри інформаційних технологій, кібернетики та захисту інформації, e-mail: jusin2016@gmail.com . https://orcid.org/0000-0002-2015-810X;

Чалий Ігор Вільович — канд. техн. наук, доцент, доцент кафедри інформаційних технологій, кібернетики та захисту інформації, e-mail: ivchaly@gmail.com . https://orcid.org/0000-0003-4896-133X ;

Бутенко Тетяна Андріївна — канд. екон. наук, доцент, доцент кафедри інформаційних технологій, кібернетики та захисту інформації, e-mail: buttan29@gmail.com . https://orcid.org/0000-0002-7723-0790;

Сирий Володимир Миколайович — старший викладач кафедри інформаційних технологій, кібернетики та захисту інформації, e-mail: syryvn@gmail.com . https://orcid.org/0000-0002-1060-1710;

Проценко Наталія Миколаївна — канд. екон. наук, доцент, доцент кафедри інформаційних технологій, кібернетики та захисту інформації, e-mail: pronatanic@gmail.com . https://orcid.org/0000-0002-7467-0491.

Державний біотехнологічний університет, Харків

Yu. V. Synyavina[1]
I. V. Chaly[1]
T. A. Butenko[1]
V. M. Syry[1]
N. M. Protsenko[1]

Analysis of Tools and Technologies for Obtaining Data from Mobile Devices in the Context of Cybercrime Investigations

[1]State Biotechnological University, Kharkiv

The article presents the analysis of modern technologies for obtaining data from mobile devices in the context of digital forensics and cybercrime investigation. The growing role of mobile devices as key carriers of digital evidence in criminal proceedings related to illegal activities in cyberspace is substantiated. The classification of the main data extraction methods and their technical features is presented, which allows choosing the optimal approaches to their use. The specific features of the application of current technological solutions for mobile forensics in Ukraine are analyzed, taking into account institutional, technical, legal and educational aspects, European integration, martial law, the constant complication of technical challenges related to data protection, and the adaptation of the legal field to the realities of digital evidence. The functional capabilities of leading commercial, open and auxiliary solutions in ensuring the completeness and reliability of digital analysis are investigated. Particular attention is paid to the procedural suitability of digital evidence, as well as the adaptation of tools to the conditions of national legal practice and the specifics of scientific and research work in the field of cybersecurity. The author presents his own experience in integrating university education with national projects that are part of the general cybersecurity ecosystem in Ukraine and combine education and interaction with law enforcement officers. The role of cloud forensics in terms of the possibility of increasing the completeness of the evidence base and compliance with national procedural requirements for access to personal data is noted. The feasibility of an integrated approach to the use of mobile forensics tools to increase the efficiency, reliability and objectivity of investigations in the digital environment is substantiated. Promising directions for the development of methods for obtaining evidence in the context of increased cryptographic protection are identified.

Keywords: mobile forensics, cybercrime, digital evidence, data extraction, mobile forensics tools, legal adaptation.

Synyavina Yuliya V. — Cand. Sc. (Econ.), Associate Professor, Head of the Chair of Information Technologies, Cybernetics and Information Protection, e-mail: jusin2016@gmail.com . https://orcid.org/0000-0002-2015-810X;

Chaly Igor V. — Cand. Sc. (Eng.), Associate Professor, Associate Professor of the Chair of Information Technologies, Cybernetics and Information Protection, e-mail: ivchaly@gmail.com . https://orcid.org/0000-0003-4896-133X;

Butenko Tetiana A. — Cand. Sc. (Econ.), Associate Professor, Associate Professor of the Chair of Information Technologies, Cybernetics and Information Protection, e-mail: buttan29@gmail.com . https://orcid.org/0000-0002-7723-0790;

Syry Volodymyr M. — Senior Lecturer, Chair of Information Technologies, Cybernetics and Information Protection, e-mail: syryvn@gmail.com . https://orcid.org/0000-0002-1060-1710;

Protsenko Nataliia M. — Cand. Sc. (Econ.), Associate Professor, Associate Professor of the Chair of Information Technologies, Cybernetics and Information Protection, e-mail: pronatanic@gmail.com . https://orcid.org/0000-0002-7467-0491