УДК 343.983.2 **DOI:** https://doi.org/10.32631/v.2025.4.30

Володимир Сергійович Макаров,
Харківський науково-дослідний
експертно-криміналістичний центр МВС України,
відділ комп'ютерно-технічних та телекомунікаційних
досліджень (головний судовий експерт);
https://orcid.org/0009-0006-1300-3616,
e-mail: makarov1900@ukr.net

ОСОБЛИВОСТІ КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ МОБІЛЬНИХ ПРИСТРОЇВ НА ОПЕРАЦІЙНІЙ СИСТЕМІ ANDROID

Метою цієї статті є комплексний аналіз особливостей криміналістичного дослідження мобільних пристроїв на операційній системі Android, систематизація наявних методів вилучення даних та оцінка перспективних напрямів подолання ключових викликів, що перешкоджають процесу дослідження. Проведено огляд інструментів для аналізу й окреслено перспективи галузі, зокрема застосування штучного інтелекту. Наголошено на необхідності комплексного підходу для ефективного використання цифрових доказів.

Ключові слова: цифрова криміналістика, мобільна криміналістика, ОС Android, електронні докази, вилучення даних, шифрування, криміналістичний аналіз.

Оригінальна стаття

Постановка проблеми

Стрімка глобальна експансія смартфонів перетворила їх на невід'ємну частину життя сучасної людини. Серед ринків мобільних операційних систем домінує Android, частка якої становить понад 70 %. Ця панівна присутність робить пристрої на її базі критично важливим джерелом цифрових доказів у кримінальних, корупційних, терористичних та інших розслідуваннях. Мобільний пристрій сьогодні – це концентрований архів особистого, професійного та соціального життя користувача, що містить листування, місцезнаходження, фінансові операції, історію переглядів і соціальні зв'язки. Однак ефективне вилучення та аналіз цих даних у криміналістичних цілях стикаються з низкою складних викликів. Таким чином, актуальність цього дослідження зумовлена гострою потребою в систематизації знань і методів, спрямованих на подолання цих перешкод.

Стан дослідження проблеми

Проблематика вилучення та дослідження інформації з електронних носіїв, зокрема безпосередньо з мобільних пристроїв, а також використання цієї інформації у криміналістичному контексті, привертає

значну увагу науковців. Зокрема, цій тематиці присвятили свої наукові праці Р. Ейерс, С. Бразерс, В. Янсен [1], О. В. Курман [2], К. В. Латиш [3], В. Г. Хахановський, М. В. Гуцалюк [4]. Однак слід ураховувати, що науково-технічний прогрес, вдосконалення програмного забезпечення та зміни в законодавстві постійно змінюють актуальність цієї проблеми, що, своєю чергою, вимагає систематичного оновлення досліджень та наукових знань.

Мета і завдання дослідження

Метою статті є дослідження проблем, що виникають під час криміналістичного вилучення та аналізу інформації, збереженої на мобільних пристроях, які працюють на операційній системі (далі – ОС) Android.

Для досягнення поставленої мети передбачається вирішення таких *завдань*: проаналізувати особливості файлових систем і засобів захисту інформації на пристроях з ОС Android; розглянути їхній вплив на можливість вилучення даних із пристроїв; визначити методи подолання перешкод для вилучення захищених даних; порівняти інструменти для вилучення даних та оцінити їхню ефективність; виявити проблемні аспекти з юридичної точки зору; висвітлити перспективні напрями розвитку галузі цифрової криміналістики.

Наукова новизна дослідження

Доповнено теоретичні засади системного підходу до криміналістичного аналізу пристроїв на ОС Android, який поєднує архітектурні особливості платформи з конкретними методами подолання захисту.

Виклад основного матеріалу

Відкрита архітектура ОС Android, яка сприяє її популярності, водночас призводить до значної фрагментації як програмного, так і апаратного забезпечення, що її підтримує. Постійне вдосконалення механізмів захисту даних, таких як шифрування та біометрична аутентифікація, створює серйозні перешкоди для криміналістичного дослідження. Операційна система Android має унікальну багаторівневу структуру, що безпосередньо впливає на розташування та захист цифрових слідів.

Історично ОС Android використовувала файлову систему YAFFS2, розроблену для NAND-пам'яті. Однак з версії 4.4 система перейшла на ext4, а з версії 7.0 і вище переважно використовується F2FS (Flash-Friendly File System), оптимізована для флешпам'яті. Ця еволюція впливає на методи фізичного вилучення та відновлення даних після їх видалення.

Ключовим аспектом є механізм ізоляції застосунків (Application Sandbox). Кожен застосунок працює у власному ізольованому середовищі з унікальним ідентифікатором користувача (UID). Дані зберігаються в

каталозі /data/data/[package_name]/, до якого за замовчуванням має доступ лише сам застосунок та система. Це забезпечує безпеку, але ускладнює доступ до даних застосунків без відповідних привілеїв.

Архітектура безпеки ОС Android реалізована на кількох рівнях:

– рівень застосунку – використання дозволів, наданих користувачем;

– рівень ОС – захист на рівні ядра Linux, мандатний контроль доступу (SEAndroid), ізоляція застосунків;

– апаратний рівень – захищені області, такі як TrustZone, які забезпечують ізольоване виконання критичних операцій (обробка біометричних даних, шифрувальних ключів)[1].

Ця багаторівнева система безпеки безпосередньо визначає, які методи вилучення даних можуть бути застосовані.

У криміналістичній практиці сформувався спектр методів вилучення даних, ефективність яких залежить від версії ОС Android, апаратного забезпечення та стану пристрою. До них належать логічне, фізичне та гібридне вилучення.

Логічне вилучення передбачає отримання даних через програмні інтерфейси (API) операційної системи. Найпоширеніші способи – використання режиму налагодження по USB (USB Debugging) та протоколу ADB (Android Debug Bridge). Цей метод дозволяє отримати файли, бази даних, списки контактів, SMS-повідомлення та іншу користувацьку інформацію. Його перевагами є простота і швидкість, однак основний недолік – обмеженість, а саме неможливість отримати видалені дані, інформацію із захищених областей або повну копію пам'яті.

Фізичне вилучення (дамп) – це створення біт-в-біт копії флеш-пам'яті пристрою. Цей метод є найбільш повним, оскільки дозволяє відновити видалені файли й отримати доступ до всіх секторів пам'яті. Для його реалізації часто використовують апаратні вразливості, вбудовані інженерні режими, наприклад режим завантажувача (Bootloader Mode), або спеціалізоване обладнання для прямого зчитування мікросхем пам'яті (ChipOFF). Водночас фізичне вилучення є технічно складним, витратним за часом і коштами, а також неможливим при увімкненому шифруванні всього диска (FDE) або файлової системи (FBE) без доступу до ключів дешифрування [1].

Сучасні підходи часто поєднують логічні та фізичні методи. *Гібридне вилучення* може передбачати:

– використання привілейованих оболонок (*root*-доступ) для отримання прав суперкористувача, що дає змогу обійти програмні обмеження та отримати доступ до системних даних;

---

[1] Android Security Bulletins // Source : сайт. URL: https://source.android.com/docs/security/bulletin (дата звернення: 15.10.2025).

– застосування власних режимів діагностики, передбачених виробниками пристроїв (наприклад, Qualcomm EDL Mode);

– використання експлойтів для підвищення привілеїв та доступу до захищених розділів.

Еволюція засобів захисту в ОС Android постійно підвищує планку для фахівців із цифрової криміналістики, які стикаються з перепонами у вигляді:

1) шифрування даних:

– повне шифрування диска (FDE):** – було основним механізмом в ОС Android 5.0–9.0. Ключ шифрування прив'язаний до графічного ключа або ПІН-коду, що робить дані недоступними без його знання навіть при фізичному вилученні;

– шифрування на рівні файлів (FBE):** – запроваджене в ОС Android 10, шифрує кожен файл окремо. Це дозволяє пристрою працювати і надавати доступ до деяких даних навіть без розблокування, але закриті дані залишаються недоступними. Ключі дешифрування захищені апаратним модулем безпеки;

2) біометричної аутентифікації – сканери відбитків пальців, розпізнавання обличчя та райдужки ока забезпечують зручний, але складний для обходу захист. Біометричні шаблони зазвичай зберігаються в захищеній області (TrustZone) і не експортуються. Юридично і технічно примус до розблокування за допомогою біометрії є складнішим, ніж вимагання пароля;

3) апаратного захисту за допомогою технології TrustZone – створює ізольоване апаратне середовище (Secure World), відокремлене від основної ОС (Normal World). У ньому виконуються операції з обробки біометрії, зберігання криптографічних ключів і перевірки цілісності системи. Прямий доступ до захищеної області (TrustZone) з основної ОС неможливий, що робить її «чорною скринькою» для експертів у галузі цифрової криміналістики.

Розбираючи спектр цифрових слідів на пристроях з ОС Android, слід зазначити, що вони містять великий обсяг потенційних доказів, зокрема [2]:

– системні артефакти – журнали системи та застосунків (*logcat*), файли кешу, інформація про підключення до Wi-Fi та Bluetooth, історія GPS-локацій;

– користувацькі дані – SMS, MMS, журнали дзвінків, контакти, фотографії, відео- та аудіозаписи;

– дані застосунків третьої сторони – листування в месенджерах (Telegram, WhatsApp, Viber, Signal), історія браузера, файли кешу соціальних мереж, дані фінансових застосунків;

– мережеві докази – інформація про IP-адреси, MAC-адреси, дані використаних VPN-сервісів [3].

Для аналізу вилучених цифрових даних використовуються спеціалізовані програмні засоби, які можна поділити на комерційні рішення та відкриті платформи (Open Source).

Комерційні рішення, такі як програмні продукти Cellebrite UFED (Physical Analyzer) та Oxygen Forensic Detective, є одними з найбільш ефективних інструментів у сфері цифрової криміналістики. Вони забезпечують автоматизоване вилучення даних, зокрема за допомогою фізичних методів, парсинг інформації та зручну візуалізацію різноманітних форматів даних із численних мобільних застосунків[1].

Відкриті платформи включають інструменти, такі як AFLogical (OSSM), Mobilyze, Santoku Linux (спеціалізований дистрибутив), а також інші спеціалізовані рішення, зокрема Android SDK (для низькорівневого аналізу), SQLite Forensic Tools (для роботи з базами даних), Volatility Framework (для аналізу пам'яті) та Wireshark (для мережевого аналізу). Ці інструменти пропонують альтернативу комерційним продуктам, даючи можливість адаптувати процес розслідування відповідно до конкретних завдань. Однак вони часто вимагають більш глибоких технічних знань і значно більше часу для проведення аналізу.

Вибір інструменту для цифрової криміналістики безпосередньо залежить від бюджету організації, складності справи і технічної кваліфікації експерта.

Криміналістичне дослідження мобільних пристроїв здійснюється суворо в межах правового поля. Недостатньо лише технічної можливості для вилучення даних – необхідно забезпечити дотримання принципів цілісності інформації та незмінності доказів після їх вилучення. Експерт зобов'язаний зберігати конфіденційність, не розголошувати інформацію, що стала відома у процесі дослідження, і діяти виключно в межах наданих йому повноважень [4].

Висновки

Для протидії сучасним викликам у сфері цифрової криміналістики необхідний системний підхід до організації досліджень, що поєднує технічну експертизу, правову обізнаність і здатність адаптуватися до стрімкого технологічного розвитку. Відкрита архітектура ОС Android, з одного боку, сприяє поширенню методів отримання прав суперкористувача, а з іншого – призводить до фрагментації, яка ускладнює стандартизацію процесів.

---

[1] The Industry Standard for Lawfully Accessing and Collecting Digital Data // Cellebrite : сайт. URL: https://www.cellebrite.com/en/ufed (дата звернення: 15.10.2025); Bringing insight and truth to data // Oxygen Forensic : сайт. URL: https://www.oxygen-forensic.com/en/solutions/features/extraction-methods (дата звернення: 15.10.2025).

Сьогодні не існує універсального методу, який би гарантував повне вилучення даних із будь-якого пристрою на ОС Android. Це зумовлює необхідність гнучкого поєднання логічного та фізичного вилучення, спроб отримання *root*-доступу й використання комерційних інструментів, що містять спеціалізовані експлойти. Перспективні напрями подальших досліджень пов'язані з розробленням методів аналізу даних з екосистеми «розумного» дому (IoT), інтегрованих із пристроями на ОС Android, а також з упровадженням технологій штучного інтелекту для автоматизації оброблення великих обсягів мобільних даних.

Отже, криміналістичне дослідження пристроїв на ОС Android є динамічною та складною галуззю, що перебуває на перетині комп'ютерних наук, юриспруденції та криміналістики. Сучасний експерт стикається з потужними архітектурними бар'єрами, вдосконаленими механізмами шифрування й апаратного захисту. Ефективне подолання цих викликів неможливе без глибокого розуміння архітектури ОС Android, володіння широким спектром методів вилучення даних (від логічного до фізичного) та постійного оновлення інструментарію.

Майбутнє криміналістичного аналізу пристроїв на ОС Android пов'язане з інтеграцією штучного інтелекту, розширенням на суміжні технологічні сегменти (IoT, хмарні сервіси) та поглибленням міжнародної співпраці у сфері стандартизації та підготовки фахівців. Лише системний і проактивний підхід дасть змогу правоохоронним органам відповідати темпам технологічного розвитку й ефективно використовувати цифрові докази для розкриття злочинів у цифрову добу.

Список бібліографічних посилань: **1.** Ayers R., Brothers S., Jansen W. NIST Special Publication 800-101 Rev. 1. Guidelines on Mobile Device Forensics. USA, 2014. DOI: https://doi.org/10.6028/NIST.SP.800-101r1. **2.** Курман О. В. Мобільні телекомунікаційні засоби як носії важливої доказової інформації: перспективність та проблеми дослідження. *Аналітично-порівняльне правознавство.* 2023. № 5. С. 532–536. DOI: https://doi.org/10.24144/2788-6018.2023.05.95. **3.** Латиш К. В. Судова комп'ютерно-технічна експертиза мобільних телефонів: аспекти призначення // Інновації в криміналістиці та судовій експертизі : матеріали міжвідом. наук.-практ. конф. (м. Київ, 25 листоп. 2021 р.) / МВС України ; Нац. акад. внутр. справ. Київ, 2021. С. 206–209. **4.** Хахановський В. Г., Гуцалюк М. В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* 2019. № 1 (31). С. 13–18. DOI: https://doi.org/10.37025/1992-4437/2019-31-1-13.

Надійшла до редколегії 17.10.2025

Прийнята до опублікування 20.11.2025

Makarov V. S. Features of Forensic Examination of Mobile Devices Running on the Android Operating System

This article is devoted to a comprehensive analysis of modern methods, challenges, and prospects for forensic examination of mobile devices running on the Android operating system. The architecture of the Android operating system is studied in detail as a fundamental factor determining the examination methodology. The evolution of file systems (from YAFFS2 to F2FS) and the application isolation mechanism (Application Sandbox) are considered. Particular attention is paid to the multi-level security system of the Android operating system, which combines protection at the application level, the operating system level (using SEAndroid mandatory control) and the hardware level through TrustZone technologies.

Particular attention is paid to the analysis of the main challenges facing digital forensics specialists. One of them is data encryption at both the disk level (FDE) and the file level (FBE), which makes data virtually inaccessible without the appropriate decryption keys. In addition, the spread of biometric authentication, whose templates are stored in the isolated TrustZone environment, is a significant obstacle, as it also complicates access to data. An important technical problem is the TrustZone technology itself, which acts as a kind of "black box" for forensic experts. A classification of digital traces that may be available on mobile devices is provided, ranging from system artefacts and user data to information from messengers and network evidence.

A comparative analysis of the tools used by experts in the field of digital forensics has been carried out. It is concluded that the choice of tool depends on the specific conditions of the investigation, as there is no universal method that would be effective in all cases. Attention is drawn to the need for clear regulation of the process of investigating digital evidence within the framework of current legislation, as well as the importance of ensuring appropriate standards for data storage and processing.

Promising areas for development in the field are outlined, including the integration of artificial intelligence technologies for analysing large amounts of data, expanding research to new segments (in particular, the IoT), and the need for international cooperation to standardise forensic investigation methods and train qualified specialists. It is concluded that forensic examination of devices running on the Android operating system is a dynamic interdisciplinary field, the success of which requires in-depth technical knowledge, constant updating of methods, and a clearly structured systematic approach.

Keywords: digital forensics, mobile forensics, Android OS, electronic evidence, data extraction, encryption, forensic analysis.