Комп'ютерно-технічне дослідження мобільних телефонів

Олександр Гожий

старший судовий експерт відділу комп'ютерно-технічних та телекомунікаційних досліджень, Черкаський науково-дослідний експертно-криміналістичний центр Міністерства внутрішніх справ України, м. Черкаси, Україна,
ORCID: https://orcid.org/0000-0001-5320-3432, e-mail: hozhyi@ndekc.ck.ua

Розглянуто значення комп'ютерно-технічного дослідження мобільних телефонів у судово-експертній практиці, зокрема для фіксування злочинів проти інфраструктури. Проаналізовано інструменти Cellebrite UFED, Oxygen Forensic, MSAB XRY та Passware Kit Mobile, а також труднощі роботи із заблокованими пристроями.

Ключові слова: *комп'ютерно-технічне дослідження; мобільний телефон; судовий експерт; цифрові докази.*

Forensics of Mobile Phones

Oleksandr Hozhyi

The report examines the significance of computer-technical examination of mobile phones in forensic practice, particularly in documenting crimes against infrastructure. The tools Cellebrite UFED, Oxygen Forensic, MSAB XRY, and Passware Kit Mobile are analyzed, as well as the challenges of working with locked devices.

Keywords: *computer-technical examination; mobile phone; forensic expert; digital evidence.*

У сучасних умовах більшість загальнокримінальних протиправних діянь здійснюється із застосуванням мобільного телефону як засобу комунікації, фіксування подій та координування дій. Мобільні пристрої виконують роль не лише каналів передачі інформації, а й сховищ великого масиву цифрових слідів: журнали дзвінків, повідомлення, мультимедійні файли, метадані геолокації, журнал активності додатків, резервні копії та дані хмарних сервісів. В умовах повномасштабної військової агресії проти України виникла окрема категорія протиправних посягань, спрямованих на підрив обороноздатності та інфраструктури держави, зокрема підпали елементів енергетичної інфраструктури, об'єктів логістики та оборони [1]. Практика свідчить, що в абсолютній більшості таких епізодів події документуються за допомогою відео- та фотоматеріалів, отриманих за допомогою мобільних телефонів; в окремих випадках ключовими доказами є записи безпосередньо з камер цих пристроїв.

З огляду на зазначене, комп'ютерно-технічне дослідження мобільного телефону набуває статусу обов'язкового етапу досудового розслідування. Судовий експерт, виконуючи таке дослідження, повинен дотримувати встановлених криміналістичних правил фіксування, вилучення, збереження та відтворення електронних доказів, забезпечуючи їх цілісність та допустимість у судовому провадженні. Процедури мають містити попереднє блокування пристрою від мережевих з'єднань, фотографічне фіксування його стану, документування кожного етапу дослідження та дотримання вимог щодо мінімізації

впливу на оригінальні дані [2]. Важливо, щоб технічні заходи супроводжувалися процесуальними дозволами та відповідними дорученнями, адже законність отриманого масиву даних безпосередньо впливає на їх процесуальну цінність.

Сучасні програмні засоби для комп'ютерно-технічного дослідження мобільних пристроїв значно розширили можливості експертної практики. До провідних рішень належать комплекси для логічного та фізичного вилучення даних, декодування резервних копій і розшифрування контейнерів збереження: *Cellebrite UFED*, *Oxygen Forensic Detective* та *MSAB XRY* (або альтернативні рішення типу *Magnet AXIOM*). Застосування згаданих продуктів у практиці судового експерта дає змогу отримувати структуровані набори артефактів, інтерпретувати метадані, виявляти сліди видалення інформації, відновлювати мультимедіа, а також проводити кореляцію часових позначок із зовнішніми джерелами. Водночас жодне програмне забезпечення не є універсальним; вибір інструмента зумовлено моделлю пристрою, версією операційної системи, наявністю шифрування та технічним станом пам'яті [2, 3].

Окремої уваги потребує дослідження заблокованих телефонів. Наявність пароля, *PIN*-коду, графічного ключа або біометричних механізмів автентифікації суттєво ускладнює доступ до внутрішнього сховища. Судовий експерт застосовує комплексний підхід: спочатку безпечні логічні методи вилучення даних та аналізування доступних резервних копій, далі — спеціалізовані апаратно-програмні рішення для брутфорсу або розблокування, а за потреби — фізичні методи вилучення [3]. Застосування *Passware Kit Mobile* у судово-експертній практиці є прикладом інструмента, що дає змогу декодувати зашифровані резервні копії та здійснювати підбір паролів до окремих контейнерів даних; у поєднанні з іншими засобами воно може забезпечити доступ до шифрованих архівів, резервних копій *iTunes* та деяких типів захищених контейнерів. Застосовуючи подібні інструменти, судовий експерт повинен оцінювати ризики для цілісності оригіналу, документувати всі кроки та послуговуватися методиками, що апробовані на практиці та мають можливість відтворення результатів іншими експертами.

У практиці комп'ютерно-технічного дослідження мобільних телефонів ключове значення має верифікація автентичності цифрових доказів. Судовий експерт виконує аналіз метаданих, порівнює часові мітки файлів із системним часом пристрою, оцінює кореляцію *GPS*-координат з іншими джерелами, перевіряє відсутність слідів маніпуляцій із файлами або недоцільного редагування. Оцінка відео та фото містить вивчення властивостей камери, аналіз *EXIF*-даних, визначення можливих артефактів перекодування та визначення достовірності формату запису.

Окрім того, деякі проблемні питання судово-експертної практики обумовлені постійним розвитком апаратного та програмного забезпечення мобільних пристроїв. Різні виробники, моделі та версії операційних сис-

тем впливають на доступні методи вилучення та декодування даних. Нестандартні прошивки, локалізовані модифікації, застосування апаратного шифрування на рівні контролера пам'яті або наявність захищених інкапсульованих елементів створюють технічні бар'єри, що потребують від судового експерта індивідуального підходу. Додатковим викликом є постійні оновлення операційної системи, що змінюють структури збереження даних та механізми автентифікації, а також широке застосування месенджерів із наскрізним шифруванням, що ускладнює доступ до корисної інформації за відсутності відповідних ключів або резервних копій.

Отже, комп'ютерно-технічне дослідження мобільних телефонів у судово-експертній практиці має доволі вагоме значення для встановлення обставин та хронології подій, особливо пов'язаних із підривною діяльністю проти національної інфраструктури. Значущість таких досліджень полягає не лише в наданні фактичних даних, а й у здатності експертизи забезпечити їхню юридичну допустимість та науково обґрунтовану інтерпретацію. Водночас складність виконання цих досліджень є суттєвою й пов'язана з непередбачуваністю технічного стану кожного конкретного пристрою: наявність або відсутність пароля, рівень шифрування, версія операційної системи, застосовані оновлення та модифікації, стан апаратної пам'яті — усе це потребує від судового експерта гнучкості методів, широкого інструментального арсеналу та чіткої процедури документування кожного етапу дослідження.

Перелік джерел посилання

1. Річні звіти. 2024 рік / Національна поліція України : офіц. вебпортал. URL: https://npu.gov.ua/diyalnist/zvitnist/richni-zviti (дата звернення: 12.09.2025).
2. Колесник В. А., Гора І. В., Попович І. І. Цифрова криміналістика в забезпеченні діяльності з протидії злочинності. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 85. С. 63—70. DOI: 10.24144/2307-3322.2024.85.4.9 (дата звернення: 12.09.2025).
3. Онищук О. Криміналістичні дослідження мобільних пристроїв: порівняння апаратно-програмних засобів шифрування мобільного зв'язку. *Кібербезпека: освіта, наука, техніка*. 2024. № 2 (26). С. 246—257. DOI: 10.28925/2663-4023.2024.26.687 (дата звернення: 12.09.2025).