УДК 343.98
DOI https://doi.org/10.24144/2788-6018.2023.05.95

# МОБІЛЬНІ ТЕЛЕКОМУНІКАЦІЙНІ ЗАСОБИ ЯК НОСІЇ ВАЖЛИВОЇ ДОКАЗОВОЇ ІНФОРМАЦІЇ: ПЕРСПЕКТИВНІСТЬ ТА ПРОБЛЕМИ ДОСЛІДЖЕННЯ

**Курман О.В.,**
*кандидат юридичних наук, доцент*
*кафедри криміналістики*
*Національного юридичного університету*
*імені Ярослава Мудрого,*
*ORCID ID: https://orcid.org/0000-0002-5432-7215*

**Курман О.В. Мобільні телекомунікаційні засоби як носії важливої доказової інформації: перспективність та проблеми дослідження.**

Статтю присвячено проблемам дослідження сучасних мобільних телекомунікаційних засобів. Актуальність роботи визначається тим, що сьогодні не залишилося сфері суспільного життя, де б не використовувалися сучасні електронні засоби комунікації. Будь-яка діяльність для підтримання належного рівня у сучасних умовах потребує активного застосування сучасних технічних комунікаторів, що дозволяють майже миттєво отримувати, обробляти, відправляти великі масиви інформації. Вагому частину таких технічних пристроїв складають мобільні телефони або смартфони, які являють собою приклад поширених знарядь (засобів) при вчиненні кримінальних правопорушень.

Мобільний телефон, як і будь-яке інше знаряддя чи засіб вчинення злочину, під час його використання залишає відповідні сліди у просторі та часі. Певна частина цих слідів відноситься до електронних (цифрових), які зберігаються на самому телефоні. У науковій роботі розглядаються основні шляхи отримання інформації, яка зберігається на мобільному пристрої, зокрема, через: 1) проведення його огляду на місці події; 2) проведення слідчого огляду вже вилученого під час кримінального провадження пристрою; 3) призначення та проведення судової експертизи. Слідчий огляд має серйозну перевагу щодо призначення експертизи у контексті швидкості його проведення та отримання результатів. Це дуже важливий фактор, особливо, якщо необхідна інформація або незначна за обсягом, або така, що перебуває у відкритому вигляді. Проте, огляд повністю виключає процес дослідження телефону. Детальне дослідження є частиною судової експертизи, цей процес є значно довшим у процесуальному, організаційному та технічному аспекті. Але обсяг одержуваної інформації в даному випадку є незрівнянно більшим й частину інформації може бути отримано лише в процесі глибокого аналізу вмісту носія інформації мобільного пристрою. Окрім перспектив зазначених підходів, паралельно в роботі висвітлюються і деякі проблеми, пов'язані з підготовкою та проведенням експертних досліджень мобільних телефоні або смартфонів, зокрема, процесуальні та технічні (необхідність отримання дозволів на застосування руйнівних методів дослідження, відсутність необхідного технічного та програмного оснащення у експертів тощо).

**Ключові слова:** криміналістичні методи дослідження, слідчий огляд, дослідження мобільних пристроїв, комп'ютерно-технічна експертиза, методика експертного дослідження.

**Kurman O.V. Mobile telecommunication devices as carriers of important evidentiary information: prospects and research problems.**

The article is devoted to the problems of studying modern mobile telecommunications. The relevance of the work is determined by the fact that today there is no sphere of public life where modern electronic means of communication are not used. Any activity to maintain its level requires the active use of modern technical communicators that allow almost instantaneous receipt, processing, and sending of large amounts of information. A significant part of such technical devices are mobile phones or smartphones, which are one of the most common tools (means) in the commission of criminal offences.

A mobile phone, like any other instrument or means of committing a crime, leaves traces in space and time when it is used. Some of these traces are electronic (digital), which are stored on the phone itself. The research paper examines the main ways to obtain information stored on a mobile device, in particular, through: 1) inspection of the device at the scene of the incident; 2) investigative inspection of the device already seized during criminal proceedings; 3) appointment and conduct of forensic examination. The investigative

examination has a serious advantage over the appointment of an expert examination in the context of the speed of its conduct and obtaining results. This is a very important factor, especially if the required information is either small in volume or in the public domain. However, the review completely excludes the process of examining the phone. A detailed investigation is part of a forensic examination, which is a much longer process in terms of procedural, organisational and technical aspects. However, the amount of information obtained in this case is incomparably greater and some of the information can be obtained only through in-depth analysis of the contents of the mobile device. In addition to the prospects of these approaches, the paper also highlights some problems associated with the preparation and conduct of expert investigations of mobile phones or smartphones, in particular, procedural and technical ones (the need to obtain permits for the use of destructive research methods, the lack of necessary technical and software equipment for experts, etc.).

**Key words:** forensic research methods, forensic expertise, mobile device research, computer and technical expertise, expert research methodology.

**Постановка проблеми.** Сьогодні не залишилося сфері суспільного життя де б не використовувалися сучасні електронні засоби комунікації. Будь яка діяльність для підтримання свого рівня потребує активне застосування сучасних технічних комунікаторів, що дозволяють майже миттєво отримувати, обробляти, відправляти великі масиви інформації. Державне управління, медицина, наука, військова сфера, правоохоронна діяльність, товарне виробництво, зв'язок тощо – все перейшло на електронний документообіг, цифрову обробку, збереження та використання інформації. Вагому частину таких технічних пристроїв складають мобільні телефони або смартфони.

**Стан опрацювання**. Проблематиці отримання, вилучення, дослідження інформації в електронних засобах комунікації, її оцінці в криміналістичній науці приділялася досить вагома увага з боку вчених. Так, зокрема, свої наукові дослідження цим питанням присвятили такі вчені, як: Бутузов В. [1], Довженко О. [2], Коршенко В. [3], Мотлях О. [4], Пашнєв Д. [5], Теплицький Б. [6] тощо. Однак, з урахуванням швидкісних змін в законодавстві, науково-технічному прогресі (створення нейромереж, розроблення нового програмного забезпечення, виробництва нових, потужних та одночасно компактних мобільних пристроїв, устаткування, виникнення нових способів вчинення кримінальних правопорушень, питання, пов'язані з дослідженням інформації, яка зберігається в смартфонах (телефонах), планшетах тощо залишаються актуальними й потребують постійного дослідження та оновлення наукових знань.

**Мета статті.** Дослідити особливості отримання, вилучення, вивчення інформації, що зберігається в мобільних телефонах або смартфонах, виявити проблемні моменти процедури дослідження.

**Виклад основного матеріалу.** Одними із поширених знарядь (засобів) при вчиненні кримінальних правопорушень виступають мобільні телефони або смартфони. Мобільний телефон, як і будь-яке інше знаряддя чи засіб вчинення злочину, під час його використання залишає відповідні сліди у просторі та часі. Певна частина цих слідів відноситься до електронних (цифрових), які зберігаються на самому телефоні, наприклад: 1) IMEI-код; 2) SMS-повідомлення; 3) відомості про надіслані або відправлення через месенджери повідомлення, телефонні з'єднання; 4) абонентська книга пристрою тощо; так і машинних носіях оператора зв'язку, наприклад: 1) дані початкового номера телефону, що використовувався для зв'язку з LOG-файлом реєстрації; 2) дати сеансу зв'язку; 3) інформація про час зв'язку, статичні або динамічні IP адреси; швидкість передачі повідомлення; 4) дані вихідних журналів сеансів зв'язку, що включають тип використаних протоколів тощо.

З процесуальної точки зору отримати дані з пристроїв можна різними ними шляхами: 1) проведення огляду на місці події; 2) проведення огляду вже вилученого під час кримінального провадження пристрою; 3) призначення та проведення судової експертизи.

Проведення огляду має серйозну перевагу щодо призначення експертизи у контексті швидкості його проведення та отримання результатів. Це дуже важливий фактор, тим більше, якщо необхідна інформація або незначна за обсягом, або перебуває у відкритому вигляді. Проте, огляд повністю виключає процес дослідження телефону. Детальне дослідження є частиною судової експертизи, а це набагато довший процес у процесуальному, організаційному та технічному аспекті. Але обсяг одержуваної інформації в даному випадку незрівнянно більший і частина інформації може бути отримана лише в процесі глибокого аналізу вмісту носія інформації мобільного пристрою.

Під час статичної стадії слідчого огляду мобільного телефону (смартфону) встановлюється їхній: 1) розмір, модель, колір, наявність чохлів або інших аксесуарів для захисту пристрою від пошкоджень, подряпин на ньому, слідів та пошкоджень; 2) захищеність пристрою від пошкоджень, наявність на ньому подряпин, слідів та пошкоджень.

На динамічній стадії в основному визначається можливість увімкнення телефону. Наступним кроком визначається факт встановлення захисту та обмеження несанкціонованого доступу до телефону (смартфону) (кнопка ввімкнення, інші кнопки, дактилоскопічний датчик тощо), доступу до пристрою стороннім особам (пароль, цифровий код, графічний ключ, доступ за відбитком пальця, доступ за скануванням тощо). За відсутності пароля або інших заходів безпеки проводиться детальний аналіз інформації, що зберігається на телефоні.

Всі сучасні смартфони мають додаток «Галерея», в якому зберігаються фотографії та відео. Вміст «Галереї» може мати значну цінність для слідчих цілей. Часто злочинці інтенсивно використовують фотографії та відео своєї діяльності, знущань над жертвами (наприклад, полоненими) показові страти тощо. Окрім безпосереднього змісту фотографій (присутність конкретних осіб, місцевості, будівель і споруд та інших елементів обстановки), криміналістичне значення може мати додаткова інформація, позначена на кадрі: дата і час зйомки, геотеги. Властивості файлу зображення також включають інформацію про час і дату зйомки.

Ще одним елементом інформаційного наповнення сучасних смартфонів є датчики геопозиціонування. Робота цих датчиків використовується в багатьох програмах. Окрім згаданого вище геотегування фотографій, більшість смартфонів мають карти та навігатори. Перевіривши ці програми, можна визначити останні результати пошуку, встановити нещодавно знайдені адреси, пройдені маршрути, проміжні точки та ключові точки (дім, робота тощо). Ключові точки можуть бути встановлені самим користувачем. Частково такі дані можуть допомогти у визначенні маршруту руху підозрюваних, наближення до цілі спостереження (військовий об'єкт, потенційний потерпілий тощо. Об'єм інформації, що вилучається та вивчається слідчим під час огляду залежить від слідчої ситуації та завдань розслідування. В умовах одних ситуацій достатньо слідчого огляду, в інших – краще та ефективніше призначати комп'ютерно-технічну експертизу.

Результатом комп'ютерно-технічної експертизи мобільного телефону (смартфона) може стати отримання таких видів даних: 1) користувацьких графічних/текстових файлів, аудіо- та відеозаписів, у тому числі знищених; 2) списків контактів; 3) відомостей про здійснені дзвінки; 4) відомостей про різні повідомлення (у тому числі чатах популярних месенджерів Viber, Telegram. WhatsApp тощо); 5) історій відвідувань Інтернет-ресурсів; 6) нотатків. Окрім зазначеної інформації, слідчий за результатами експертизи також може отримати відомості про тип, марку, модель, версію прошивки, робочий стан та технічні характеристики мобільного пристрою; місцезнаходження телефону (геолокацію); відомості про точки wi-fi, до яких пристрій підключався; історію роботи з пристроєм; логіни і паролі від різних соціальних мереж і сервісів; вирішити питання щодо походження інформації в пам'яті мобільного телефону або на SIM-карті.

Дослідження телефону підозрюваного може виявити встановлене на ньому спеціалізоване програмне забезпечення, наприклад, для розрахунку балістичної траєкторії польоту снаряда або об'єму і точки закладання вибухових зарядів на об'єкті, перехоплення та управління системами контролю доступу або відеоспостереження тощо.

Більшість мобільних пристроїв з'єднуються з мобільними та іншими мережами через Bluetooth, інфрачервоний порт і модуль Wi-Fi. На цьому етапі експерт ізолює смартфон (планшет) від усіх мереж. Це дозволяє уникнути зміни даних, доступних у пам'яті пристрою. Крім того, деякі пристрої підтримують віддалений доступ, який може бути використаний підозрюваним для знищення цифрових доказів. Для цього, наприклад, може бути використана клітка Фарадея, яка захищає пристрій від зовнішніх електромагнітних полів. Крім того, більшість смартфонів і планшетів мають вбудований режим «У літаку», який також дозволяє відключити пристрій від усіх мереж.

Після того, як смартфон (планшет) ізольовано від мережі, експерт приступає до безпосереднього вилучення та аналізу даних за допомогою обраного програмного забезпечення. Існує кілька основних експертних методів вилучення інформації з електронних мобільних пристроїв.

1. Ручний пошук. Цей метод передбачає доступ до комп'ютерної інформації, наявної в пам'яті мобільного пристрою, через клавіатуру або сенсорний екран. Виявлена під час розслідування інформація документується шляхом фотографування екрану смартфона або планшета.

2. Пошук інформації логічним методом завантаження. Цей рівень передбачає підключення мобільного пристрою до робочої станції експерта за допомогою USB-кабелю, інфрачервоного порту або «Bluetooth». Потім виконується побітове копіювання файлів і каталогів, розташованих на логічних дисках мобільного пристрою. Для цього використовується інтерфейс прикладного програмування, розроблений виробником і призначений для синхронізації телефону або планшета з персональним комп'ютером. Однак цей рівень відновлення даних також надає обмежений доступ до комп'ютерної інформації і не дозволяє відновити видалені дані, за деякими винятками. На цьому рівні також можливо відновити бази даних, що містять мініатюри зображень і відеофайли на пристрої, в тому числі і видалені файли цього типу.

3. Вилучення даних на фізичному рівні. Цей рівень означає отримання побітової копії всієї внутрішньої пам'яті мобільного пристрою, що дозволяє, серед іншого, відновити видалені записи і файли. Незважаючи на привабливість цього методу, виконати відновлення даних на цьому рівні не завжди можливо: виробники часто обмежують можливість читання внутрішньої пам'яті мобільного пристрою для забезпечення максимальної безпеки. Щоб обійти ці обмеження, експерти використовують програмні завантажувачі власного розроблення або ліцензійні продукти сторонніх виробників, які не тільки дозволяють отримати доступ до внутрішньої пам'яті, але й іноді обходять встановлені користувачами паролі.

4. Вилучення даних із вбудованого модуля пам'яті. Цей рівень передбачає вилучення даних безпосередньо з інтегрованого чіпа пам'яті мобільного пристрою. Модуль виймається з телефону або планшета і поміщається у відповідний зчитувальний пристрій. Цей метод складний у використанні, оскільки чіпи пам'яті, що використовуються в мобільних пристроях, досить різноманітні. Однак перевагою вилучення даних на цьому рівні є те, що інформацію можна відновити навіть з пам'яті пошкоджених мобільних пристроїв [7, с. 443-444].

Під час дослідження мобільних телефонів виникає необхідність перегляду, копіювання та відновлення видаленої інформації, що міститься у вбудованій пам'яті телефону або встановлюваних у нього карті пам'яті та SIM-карті. Однак слід врахувати, що через великий спектр наявних мобільних телефонів обладнання, наявне в розпорядженні експертів, не завжди може відновити видалену інформацію та/або скопіювати її. В експертній практиці виділяють і інші проблеми, пов'язані з дослідженням мобільних телефонів: 1) компактний розмір сучасних пристроїв, що вимагає спеціалізованих інтерфейсів, носіїв даних і апаратних засобів; 2) на противагу традиційним об'єктам комп'ютерно-технічної експертизи, де дані знаходяться в енергонезалежній пам'яті, у мобільних телефонів файлова система знаходиться в енергозалежній пам'яті, що обмежує використання деяких методів; 3) режим зниженого енергоспоживання, що призупиняє процеси під час вимкнення живлення або під час простою, залишаючи, однак, пристрій активним, в подальшому може призвести до змін у файловій структурі мобільного пристрою при підключенні стороннього лабораторного обладнання; 4) велика різноманітність використовуваних операційних систем; 5) короткий термін між випусками нових моделей портативних пристроїв.

Відповідно до ч. 5 ст. 69 КПК України експерт зобов'язаний забезпечити збереження об'єкта експертизи. Якщо специфіка дослідження передбачає повне або часткове знищення об'єкта експертизи або зміну його властивостей, експерт повинен одержати на це дозвіл від суб'єкта, який призначив експертизу. Особливістю комп'ютерно-технічної експертизи є те, що у разі дослідження програмних об'єктів та неможливості роботи з їх копіями майже завжди відбуваються зміни у файлових системах та реєстрах технічних пристроїв (наприклад, під час його включення). Така ситуація вимагає отримання експертом дозволу на застосування так званих руйнівних (частково руйнівних) методів.

Використання тільки неруйнівних методів (за відсутності необхідних апаратно-програмних засобів) може призвести до затягування термінів виконання експертизи і мати негативні наслідки для розслідування, а також для судового розгляду кримінальних проваджень. [8, с. 298]

Закон України «Про судову експертизу» визначає у ст. 3 принципи судово-експертної діяльності, серед яких принцип законності посідає перше місце, що в контексті методики проведення комп'ютерно-технічної експертизи означає заборону та неприпустимість використання експертами контрафактного програмного забезпечення і застосування тільки ліцензійного програмного продукту або спеціальних програм власного розроблення, зареєстрованих у встановлений законом спосіб.

Головна вимога до упаковки об'єктів для комп'ютерно-технічної експертизи – це збереження первісного стану інформації на носіях та їх фізичної цілісності і придатності для дослідження. Упаковка вилучених об'єктів повинна виключати можливість непроцесуальної роботи з ними, розукомплектування і фізичного пошкодження. Для збереження наданих на дослідження носіїв інформації в робочому стані вони надаються в окремих пакуваннях. Такі технічні пристрої потрібно упаковувати у спеціальну екрануючу тару, що виключає можливість впливу на кнопки управління і дистанційного доступу до апарата. Важливо не порушувати комплектність телефону (не витягувати з нього SIM-карту і карту пам'яті). У разі вилучення невстановлених у телефон SIM-карток не слід намагатися самостійно переглянути інформацію за допомогою будь-яких пристроїв читання SIM-карток або мобільних телефонів, оскільки це може призвести до зміни та втрати службової інформації на носії. Електронні пристрої, щодо яких планується в майбутньому проведення експертизи, не рекомендується досліджувати слідчому самостійно через можливі зміни у службовій та іншій інформації, що може створити складнощі в подальшому щодо відновлення та дослідження видалених файлів. Відкриття електронних листів, активація встановленого програмного забезпечення, запуск застосунків і навігація по сайтах мережі Інтернет

викликає зміни у службових файлах операційної системи, залишає сліди в історії роботи, папках, що містять тимчасові і log-файли, а також реєстрах щодо роботи в Інтернеті.

**Висновки.** Важливість розроблення нових, сучасних експертних методів дослідження електронних засобів комунікації, вдосконалення вже існуючих не викликає сумнівів, адже науково-технічний прогрес не стоїть на місці і розвивається дуже стрімко. Такий стан речей впливає й на технічну оснащеність представників злочинного світу, які прямо або опосередковано використовують мобільні засоби комунікації на всіх стадіях вчинення кримінального правопорушення. А тому значення комп'ютерно-технічних експертних досліджень мобільних телефонів (смартфонів) в процесі досудового розслідування все більше зростатиме, що вже сьогодні спонукає до проведення постійного оновлення існуючих криміналістичних методик розслідування та експертних науково-технічних методів досліджень.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**


1. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки: наук.-практ. посіб. / В.М. Бутузов та ін. / ред. Л.П. Скалозуб, І.В. Бондаренко. Київ, 2010. 245 с.
2. Довженко О.Ю. Основи методики розслідування кіберзлочинів: автореф. дис. ... канд. юрид. наук (д-ра філософії): 12.00.09 / Харк. нац. ун-т внутр. справ. Харків, 2020. 20 с.
3. Коршенко В.А. Теоретичні та методичні основи судової телекомунікаційної експертизи: автореф. дис. ... канд. юрид. наук: 12.00.09 / Харк. нац. ун-т внутр. справ. Харків, 2017. 20 с.
4. Мотлях О.І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій: автореф. дис. ... канд. юрид. наук: 12.00.09 / Акад. адвокатури України. Київ, 2005. 20 с.
5. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій»: автореф. дис. ... канд. юрид. наук: 12.00.09 / Харк. нац. ун-т внутр. справ. Харків, 2007. 18 с.
6. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз: наук.-практ. посіб. / Б.Б. Теплицький та ін. Київ: Паливода А.В. [вид.], 2019. 167 с.
7. Hagani Gajiyev, Azizbek Xudoyberdiyev Some aspects of mobile device research:Uzbekistan's experience. *Society and innovations.* Special Issue – 2. 2020. № 1. С. 438–448. URL: https://inscience.uz/index.php/socinov/article/view/327/409 (дата звернення: 10.09.2023).
8. Стецик Б.В, Марко С.І. Методика проведення судової комп'ютерно-технічної експертизи. Юридичний науковий електронний журнал. 2022. № 1. С. 296–299.