Технічні науки

УДК 004.001

Золотарьов Сергій Олександрович

головний судовий експерт

відділу комп'ютерно-технічних та телекомунікаційних досліджень

Харківський науково-дослідний експертно-криміналістичний центр

Міністерства внутрішніх справ України

Золотарёв Сергей Александрович

главный судебный эксперт

отдела компьютерно-технических и телекоммуникационных исследований

Харьковский научно-исследовательский

экспертно-криминалистический центр

Министерства внутренних дел Украины

Zolotarov Serhii

Chief Forensic Expert at the Department of

Computer and Telecommunication Studies

Kharkov Scientific Research Forensic Center of the

Ministry of Internal Affairs of Ukraine

ПРОБЛЕМНІ ПИТАННЯ, ЯКІ МОЖУТЬ ВИНИКНУТИ ПІД ЧАС СТВОРЕННЯ ЗАГАЛЬНОЇ МЕТОДИКИ ДОСЛІДЖЕННЯ МОБІЛЬНИХ ТЕЛЕФОНІВ (СМАРТФОНІВ)

ПРОБЛЕМНЫЕ ВОПРОСЫ, КОТОРЫЕ МОГУТ ВОЗНИКНУТЬ ПРИ СОЗДАНИИ ОБЩЕЙ МЕТОДИКИ ИССЛЕДОВАНИЯ МОБИЛЬНЫХ ТЕЛЕФОНОВ (СМАРТФОНОВ)

PROBLEM ISSUES THAT MAY OCCUR DURING THE DEVELOPMENT OF A GENERAL TECHNIQUE OF RESEARCH OF MOBILE PHONES (SMARTPHONES)

Анотація. *У статті розглянуто проблемні питання, які можуть виникнути під час розробки загальної методики проведення дослідження мобільних телефонів (смартфонів) судовими експертами за напрямком комп'ютерно-технічних досліджень Науково-дослідних експертно-криміналістичних центрів МВС України, запропоновано модель етапів дослідження мобільних телефонів (смартфонів) та їх короткий аналіз.*

Ключові слова: *смартфон, методика, операційна система, вилучення інформації.*

Аннотация. *В статье рассмотрены проблемные вопросы, которые могут возникнуть при разработке общей методики проведения исследования мобильных телефонов (смартфонов) судебными экспертами по направлению компьютерно-технических исследований Научно-исследовательских экспертно-криминалистических центров МВД Украины, предложена модель этапов исследования мобильных телефонов (смартфонов) с их кратким анализом.*

Ключевые слова: *смартфон, методика, операционная система, извлечение информации.*

Summary. *The article considers the problematic issues that may arise during the development of general methodology for research of mobile phones (smartphones) by forensic experts in the field of computer and technical research in the Research forensic centers of the Ministry of Internal Affairs of Ukraine, offers a model of research stages of mobile phones (smartphones) and their brief analysis.*

Key words: *smartphone, technique, operating system, information extraction.*

На сьогоднішній час важко уявити сучасну людину без переносних розумних пристроїв, до яких відносяться смартфони. Смартфоном

визначається окрема категорія мобільних телефонів, які – на відміну від простих стільникових телефонів – керуються операційною системою та окрім прямих функцій мобільного телефона здійснювати дзвінки та обмінюватись повідомленнями у деяких випадках можуть заміщати ролі переносних персональних комп'ютерів, адже мають все необхідне задля виконання майже всього об'єму роботи, яку можна виконати за допомогою персонального комп'ютера, за умови наявності відповідного програмного забезпечення, а саме: працювати з текстовими документами та таблицями, графічними, аудіо та відеофайлами, вести електронне листування, навіть створювати програмне забезпечення та інші. Виходячи із існуючої потреби, набір корисних функцій з кожним роком лише розширюється, роблячи смартфон невід'ємним помічником не тільки для пересічних громадян та правоохоронних структур, а і для злочинців. У зв'язку з чим, смартфони являються невіднятним об'єктом сучасної цифрової криміналістики, адже у деяких випадках судовим експертом при проведенні дослідження може бути виявлена інформація, яка може суттєво змінити хід справи, у випадку, якщо дослідження буде проведене якісно та у повній мірі. Зокрема, дослідження смартфонів в Україні може бути проведене у Експертних установах України, судовими експертами за напрямком комп'ютерно-технічної експертизи. У своїй роботі судовий комп'ютерно-технічний експерт повинен мати спеціальні знання у галузі інформаційних технологій, вміло володіти ними застосовуючи їх при проведенні досліджень, дотримуватись існуючих методик, брати до уваги методичні рекомендації та напрацювання у галузі комп'ютерно-технічних експертиз, за можливості приймати участь у створенні нових та приведення до відповідності сьогоднішнім реаліям вже існуючих, постійно вдосконалювати свої навички, отримувати нові знання.

Слід зазначити, що у комп'ютерно-технічній експертизі в підрозділах науково-дослідних центрів МВС України судовими експертами у при проведенні досліджень використовується методики дослідження

комп'ютерної техніки, відеореєстраторів, SIM-карт, є методичні рекомендації щодо дослідження смартфонів на базі операційної системи Android, але у деяких випадках, таких як дослідження смартфонів, інколи важко визначити чіткий детальний алгоритм дослідження того чи іншого смартфона.

Перш за все одна з головних проблем, яка виникає на шляху узагальнення всіх напрацювань при дослідженнях смартфонів у єдину методику є те, що галузь створення смартфонів постійно розвивається, тому забезпечення судових експертів повинно постійно вдосконалюватись для досягнення максимальної результативності. Також стрімко змінюються способи і методи дослідження, а також є виняткові унікальні випадки для дослідження окремих груп смартфонів, тому вже у випадку підходів до описання початку дослідження у майбутній методиці виникають труднощі, а саме – визначення необхідного програмного та апаратного забезпечення. Постійній розвиток галузі створення смартфонів, впровадження нових технологій, удосконалення вже існуючих основних складових частин смартфона, є другою причиною. Третьою, але не менш важливою причиною є особливість операційних систем, які використовуються у сучасних смартфонах, алгоритми систем захисту даних, які використовуються у цих операційних системах та напрацювання окремих виробників смартфонів щодо удосконалення та впровадження унікальних напрацювань у цій області.

Всі три основних причини пов'язані між собою. На даний час не можливо визначити чіткі програмні та апаратні продукти, які були б актуальними протягом тривалого часу, так само як і кількість програмного забезпечення, яке може бути використане експертом при проведенні дослідження, це є особливістю напрямку комп'ютерно-технічної судової експертизи не тільки в Україні, а у і всьому світі. Пояснення цьому – неможливість всеосяжного охоплення розробниками у підтримці у одному

програмному продукті або у апаратно-програмному комплексі всіх моделей смартфонів, тому для проведення дослідження відносно наданого на дослідження смартфона судовим експертом можуть бути застосовані декілька програмних продуктів для проведення аналізу та перевірки отриманих результатів, або їх доповнення. При чіткому закріпленні у методиці одного або декількох програмних продуктів, з великою ймовірністю, у майбутньому виникне проблема, яка порушить у питання повноти дослідження, та автоматично перетворить цю методику на неактуальну. У цьому випадку, одним із варіантів вирішення цієї проблеми – створення широкого алгоритму дій судового експерта у виборі методів та способу дій. Мінусом цього рішення можуть бути об'єми методики: на кожному етапі, виходячи із першого (на якому експерт описує наданий на дослідження смартфон, ідентифікуючи ознаки), алгоритм дій експерта буде розгалужуватися в залежності від ідентифікуючих ознак, які будуть доповнюватися в ході дослідження, у зв'язку з чим, необхідно максимально охопити всі ці алгоритми у тексті методики. Опираючись на практичний досвід, можна виділити три основних етапи дослідження мобільних телефонів:

1. Візуальне дослідження, встановлення ідентифікуючих ознак таких як інформація про виробника, модель, IMEI, серійний номер, наявність або відсутність SIM-карт, карт пам'яті.

Саме на цьому етапі у експерта повинний бути розроблений етап подальшого дослідження з врахуванням необхідних програмних та апаратних засобів.

2. Підготовка до дослідження (підготовка до вилучення інформації).

На цьому етапі експертом виконується заряджання акумуляторної батареї, увімкнення смартфона без SIM-карти, виявлення способів захисту та їх подолання, встановлення інформації щодо операційної системи,

налаштувань, вибір способу подальшого дослідження (способу та методу вилучення інформації із пам'яті пристрою).

3. Основний етап (вилучення та обробка/аналіз інформації).

В залежності від виробника мобільного телефону (смартфону), типу, виробника та моделі процесора, версії операційної системи та версії захисних оболонок доцільно буде використовувати методи та способи вилучення інформації з пам'яті досліджуваного об'єкта виходячи із принципу найбільш повного вилучення інформації, яка необхідна, але з найменшими змінами властивостей.

Перелічені етапи, потребують детального опису в тексті методики, охоплюючи максимальну кількість всіх можливих варіантів вилучення інформації, а також, що не є менш важливим, розробка не одного, а декількох підходів до дослідження та вилучення інформації в залежності від запитань, які поставлені перед судовим експертом.

Виходячи із вищезазначеного, створення методики буде потребувати багато часу, що також можна вважати ризиком, адже є висока вірогідність, що буде втрачено актуальність методики ще на етапі її написання, у зв'язку з чим, необхідно буде частіше змінювати або доповнювати цю методику у майбутньому, можливо вже після її опублікування. Також для більш якісного процесу створення методики необхідно провести аудит програмного та апаратного забезпечення, яке мається у розпорядженні судових експертів комп'ютерно-технічної експертизи у експертних підрозділах України, що також потребує значних витрат часу, а також узагальнення, поглиблений аналіз та робота з напрацюваннями, у тому числі взаємодія з іншими Експертними установам України.

Література

1. Методика ДНДЕКЦ МВС України: Комп'ютерно-технічна експертиза (загальна частина): / [уклад. К.М. Ковальов, С.М. Корнійко, В.О. Княждвірський]. К.: ДНДЕКЦ МВС України, 2007. 24 с.
2. Методика ДНДЕКЦ МВС України: Проведення комп'ютерно-технічних досліджень носіїв цифрової інформації / [уклад. С.М. Корнійко, С.В. Поцелуй]. К.: ДНДЕКЦ МВС України, 2009. 27 с.
3. Дослідження мобільних пристроїв під керуванням операційної системи Android: методичні рекомендації / [уклад. В.А. Поліщук]. К.: ДНДЕКЦ МВС України, 2017. 22 с.