УДК 343.132+343.98

Віталій Геннадійович КОЛЕСНИК,
завідувач відділу комп'ютерно-технічних та телекомунікаційних досліджень Харківського науково-дослідного експертно-криміналістичного центру МВС України

ПРОБЛЕМНІ ПИТАННЯ ЗБЕРЕЖЕННЯ, ФІКСАЦІЇ ТА ДОСЛІДЖЕННЯ ІНФОРМАЦІЇ В СУЧАСНИХ МОБІЛЬНИХ ТЕЛЕФОНАХ

Сучасне життя сьогодні неможливо уявити без мобільних телефонів. Будь-яка діяльність, комунікація, спілкування, планування роботи і дозвілля, так чи інакше будуть відображені у телефоні сучасної людини. Доступність на ринку та надзвичайне поширення мобільних пристроїв зробили мобільний телефон незмінним супутником людини. Широке різноманіття функцій та сервісів у мобільному телефоні, такі як фотографування, відеозапис, аудіозапис, фіксація географічних координат та переміщень, можливість миттєво обмінюватися у різноманітних програмах-месенджерах текстовими та голосовими повідомленнями, документами, графічними зображеннями, можливість здійснювати миттєве керування фінансами та робити грошові перекази, призводить до накопичування у пам'яті телефону значної кількості інформації, яка має суттєве, а іноді й вирішальне значення для з'ясування обставин та доказування в процесі досудового розслідування.

Очевидно, що виробники телефонів та розробники їх операційних систем приділяють значну увагу захисту даних користувача. Окрім коду розблокування телефону, захист даних у телефонах наразі забезпечується (в залежності від року випуску та моделі телефону): режимом Secure Startup, засобами повного дискового шифрування Full Disk Encryption (FDE), а на останніх моделях – засобами пофайлового шифрування File Based Encryption (FBE). Окрім того, з кожним роком ускладнюється доступ до завантажувача та звужується вікно можливостей для його модифікації. Переписка у месенджерах вже не заноситься до резервної копії, тому її можливо вилучити лише з повної дешифрованої фізичної копії пам'яті телефону, зробити яку є можливим далеко не з усіх моделей, присутніх на ринку. Навіть найсучаснішими техніко-криміналістични-

ми засобами не є можливим здійснити вилучення інформації з усіх без винятку моделей мобільних телефонів [1].

Таким чином, головним засобом отримати доступ до інформації з метою хоча б її візуального огляду, наразі є визначення слідчим паролю розблокування, який підозрюваний повідомляти, зазвичай, відмовляється. Окрім паролю, сучасні телефони також можливо розблокувати сканером відбитка пальця та системою розпізнавання обличчя, однак вони надають лише умовний доступ та не є повноцінною заміною визначеному паролю блокування.

Постійний розвиток засобів захисту у сучасних телефонах, та недостатня обізнаність слідчих та оперативних співробітників у особливостях їх функціонування, помилки під час вилучення пристроїв, призводять до негативних наслідків, що виражаються у втраті як можливості доступу до інформації у телефонах, так і до втрати самої інформації в цілому. До найбільш типових помилок при вилученні та упакуванні телефону слід віднести:

1. Не вмикання автономного режиму («режиму польоту») або незабезпечення його захисту від зовнішнього впливу через мережу мобільного оператора та мережі бездротового зв'язку. У разі залишення телефону у мережі, можливе його віддалене блокування та навіть стирання (скидання, очищення) користувачем через мережу Інтернет [2].

2. Вимикання телефону без його попереднього огляду. Якщо телефон вдасться розблокувати, до його вимкнення доцільно робити вибіркові фото або відеозаписи виявлених окремих відомостей, оскільки після вимкнення телефону доступ до них може бути втрачений назавжди [3].

3. Витягання SIM-карти прямо на ввімкненому телефоні, що призводить до його автоматичного перезавантаження та втрати можливості розблокування відбитком пальця або системою розпізнавання обличчя.

4. Втрата можливості дослідження телефону після його розблокування відбитком пальця або системою розпізнавання обличчя.

Як зазначається у міжнародних інструкціях для правоохоронних органів, на місці події доцільно використовувати лише два основних алгоритми дій правоохоронця по збереженню інформації у телефоні.

Перший – ввімкнення «режиму польоту» без витягання SIM-карти з одночасним постійним підтримуванням стану зарядженості батареї

(під'єднання power bank) та упакуванням телефону у пакет, блокуючий радіохвилі (т.з. «пакет Фарадея») [4, с. 153].

Другий алгоритм витікає з першого та виконується у разі можливості розблокування особою телефону відбитком пальця або системою розпізнавання обличчя – розблокований телефон переводиться у «режим польоту», після чого у його налаштуваннях дисплею та меню налаштувань безпеки встановлюються параметри: «Вимикання екрану» – «ніколи», «Блокування екрану/режим очікування» – «ніколи», яскравість екрану виставляється в мінімум з метою збільшення строку збереження заряду батареї, телефон під'єднується до зовнішнього носія живлення (power bank) та упаковується у пакет, блокуючий радіохвилі. Таким чином, екран телефону не буде гаснути, телефон буде знаходитись постійно у розблокованому стані та може вільно оглядатись до розряджання всіх джерел живлення. Вимкнути біометричний захист у сучасних телефонах неможливо, оскільки при спробі його вимкнення телефон запитає числовий пароль розблокування.

Вказаний другий спосіб наразі є найбільш ефективним, його застосовують навіть для розблокування телефону потерпілого при вбивстві, використовуючи палець чи обличчя вбитого прямо на місці події, звичайно із дотриманням усіх процесуальних та протокольних процедур. Діючи невідкладно, доки телефон не заблокований, існує можливість синхронізувати переписку з месенджерів та деякі інші відомості з телефону на комп'ютер.

Як ми можемо спостерігати на практиці, спираючись на стан мобільних телефонів, що находять на експертизу, переважної більшості слідчих та оперативних співробітників (окрім спеціальних технічних управлінь) вищевказані алгоритми не відомі, а заняття та підвищення кваліфікації на цю тему з ними майже не проводяться, що за підсумком призводить до непоодиноких випадків втрати важливої доказової інформації.

Список бібліографічних посилань

1. Afonin O. Challenges in Computer and Mobile Forensics: What to Expect in 2020 // Elcomsoft. Blog. 20.12.2019. URL: https://blog.elcomsoft.com/2019/12/challenges-in-computer-and-mobile-forensics-what-to-expect-in-2020/ (дата звернення: 28.04.2020).
2. Извлечение данных из устройств под управлением iOS. Физический и логический методы // Elcomsoft : сайт. https://www.elcomsoft.ru/presentations/ios_acquisition_ru.pdf (дата звернення: 30.04.2020).

3. Распространённые ошибки в мобильной криминалистике // Elcomsoft. Blog. 05.02.2020. URL: https://blog.elcomsoft.com/ru/2020/02/rasprostranyonnye-oshibki-v-mobilnoj-kriminalistike/ (дата звернення: 30.04.2020).
4. Sammons J. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Elsevier Inc, 2012. 208 p.
5. Reiber L. Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation. McGraw-Hill Education, 2015. 480 p.

Одержано 30.04.2020