УДК 343.983

Ю.С. Харабуга, ст. науков. співробітник

Львівський НДІ судових експертиз

КОМП'ЮТЕРНО-ТЕХНІЧНЕ ДОСЛІДЖЕННЯ МОБІЛЬНИХ ТЕЛЕФОНІВ, СМАРТФОНІВ ТА SIM-КАРТ

Розглянуто межі компетенції експерта, можливі небезпеки щодо втрати інформації та запропоновано послідовність дій експерта при комп'ютерно-технічному дослідженні мобільних телефонів, смартфонів та SIM-карт.

У грудні 2006 року загальна кількість абонентів мобільного зв'язку в Україні стала більшою за чисельність населення. При цьому, за оцінками аналітиків, реальна кількість діючих абонентів мобільного зв'язку становила не більше 63% від загальної чисельності населення, тобто на той час мобільний телефон був фактично у кожних двох з трьох українців [1]. Подібний ріст рівня проникнення стільникового зв'язку в Україні привів до того, що під час розслідування майже кожного кримінального провадження слідство стикається з питанням дослідження інформації, що міститься в пам'яті мобільних телефонів та смартфонів, включаючи SIM-картки.

Відповідно до Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень, затверджених наказом Міністерства юстиції України від 8 жовтня 1998 р. № 53/5 (у редакції наказу Міністерства юстиції України від 26 грудня 2012 р. № 1950/5; далі — Науково-методичних рекомендацій), основними завданнями експертизи телекомунікаційних систем та засобів (далі — ЕТСЗ) є:

- визначення характеристик та параметрів телекомунікаційних систем та засобів;
- встановлення фактів та способів передачі (отримання) інформації в телекомунікаційних системах;
- встановлення фактів та способів доступу до систем, ресурсів та інформації у сфері телекомунікацій;
- визначення якості надання телекомунікаційних послуг на рівні їх споживання;
- встановлення конфігурації та робочого стану телекомунікаційних систем та засобів;
- встановлення типу, марки, моделі та інших класифікаційних категорій телекомунікаційних систем та засобів;

– дослідження алгоритмів обробки інформації та її захисту у сфері телекомунікацій.

Оскільки мобільні телефони та смартфони становлять собою різновид терміналу стільникового зв'язку (далі — ТСЗ), а SIM-карти — необхідний компонент для функціонування ТСЗ в якості телекомунікаційного засобу, їх дослідження передусім є завданням ЕТСЗ. Разом з цим необхідно враховувати, що мобільний телефон та сматрфон є спеціалізованим комп'ютером з відповідним програмним забезпеченням. Вони виконують низку функцій, починаючи з функцій звичайного цифрового органайзера та закінчуючи функціями молодшої моделі персонального комп'ютера (робота з електронною поштою, перегляд текстових або мультимедійних файлів тощо) [2]. Багато моделей мобільних телефонів оснащено слотом для карти пам'яті та/або можна підключити до комп'ютеру як звичайний зовнішній накопичувач інформації з файловою системою FAT.

У свою чергу, SIM-карта становить різновид смарт-карти стандарту ISO/IEC 7816 [3].

Відповідно до вказаних Науково-методичних рекомендацій, основними завданнями експертизи комп'ютерної техніки і програмних продуктів є:

– встановлення робочого стану комп'ютерно-технічних засобів;
– встановлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;
– виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;
– встановлення відповідності програмних продуктів певним версіям чи вимогам на його розробку.

Таким чином, якщо розглядати мобільний телефон, смартфон та SIM-карту як спеціалізовані комп'ютерно-технічні засоби та/або спеціалізовані комп'ютерні носії, їх дослідження можна за певних умов проводити виключно у межах комп'ютерно-технічної експертизи (далі — КТЕ).

При підключенні ТСЗ до комп'ютера за допомогою дата-кабелю або бездротового з'єднання експерт шляхом використання спеціалізованого програмно-апаратного забезпечення може дослідити інформацію в пам'яті мобільного телефону про: останні набрані номери; одержані та пропущені дзвінки; надіслані, одержані та збережені повідомлення (SMS, MMS, електронна пошта); телефонну книгу, нотатки тощо; звукові, графічні, відео й інші файли.

У пам'яті SIM-карти може зберігатися телефонна книга, SMS та інша текстова інформація. При цьому, безумовно, одним із завдань комп'ютерно-технічної експертизи є дослідження знищеної інформації в пам'яті мобільного телефону, смартфону та SIM-карти.

З іншого боку, за межі компетенції експерта виходить питання походження інформації в пам'яті мобільного ТСЗ (внаслідок мобільного зв'язку, внаслідок відео-, звуко- або фотозйомки), яке потребує комплексного дослідження за участю експертів інших видів судової експертизи (ЕТСЗ, відеозвукозапису, фототехнічної). Аналогічно комплексного дослідження потребує встановлення походження інформації в пам'яті SIM-карти. Також за межі компетенції експерта з КТЕ виходять деякі спірні випадки встановлення типу, марки, моделі, версії прошивки, перевірка робочого стану та технічних характеристик ТСЗ [2].

На початку комп'ютерно-технічного дослідження експерт має з'ясувати, яку саме інформацію необхідно дослідити. Якщо питання сформульовано нечітко або неоднозначно (допускає різні за змістом тлумачення), експерт шляхом клопотання з'ясовує, яку саме інформацію необхідно дослідити, після чого вирішує питання у новій редакції відповідно до відповіді на клопотання. У випадку відсутності відповіді на клопотання протягом встановленого законодавством терміну, експерт повідомляє про неможливість надання відповіді на питання або може у порядку експертної ініціативи провести дослідження щодо того або іншого виду інформації, що міститься у пам'яті мобільного телефону.

Дослідження відео та звукової інформації, яка утворена за допомогою мікрофону та відеокамери ТСЗ, має проводитись за участю експерта з технічного дослідження матеріалів та засобів відеозвукозапису за умови, що поставлене завдання передбачає вирішення питань про здійснення запису представленим ТСЗ та відсутністю у запису змін.

Дослідження графічної інформації, яка утворена за допомогою фотокамери телефону, має проводитись за участю експерта з фототехнічного дослідження за умови, що поставлене завдання передбачає вирішення питань про здійснення запису представленим ТСЗ та відсутністю у запису змін.

Дослідження інформації, яка могла утворитись у ТСЗ або SIM-карті у наслідок мобільного або іншого зв'язку, має проводитись за участю експерта з ЕТСЗ за умови, що поставлене завдання передбачає вирішення питань про походження інформації внаслідок мобільного або іншого зв'язку.

У випадку, якщо у експертній установі відсутні експерти відповідних експертних спеціальностей, експерт з комп'ютерно-технічного дослідження проводить необхідні дослідження відповідно до своєї компетенції (зазначає факт наявності зазначених файлів та наводить їх атрибути), про що зазначає про це у висновку експертизи [3; 4].

При проведенні комп'ютерно-технічного дослідження слід використовувати засоби, що однозначно вірно можуть працювати з даним ТСЗ. Такими засобами можуть бути:

– спеціалізовані пристрої (програматори), що випускаються виробником самого стільникового терміналу;
– спеціалізовані пристрої, що призначені для судово-експертних (криміналістичних) досліджень стільникових терміналів та сертифіковані виробником досліджуваного пристрою на предмет вірної взаємодії та коректної роботи у рамках судових досліджень;
– програмне забезпечення та дата-кабелі, що призначені для підключення стільникового терміналу до ПК та вироблені або сертифіковані виробником стільникового терміналу.

Кожний із перелічених засобів має як свої переваги, так і свої недоліки. Так, спеціалізовані програматори часто потребують випаювання мікросхеми, що не завжди зручно. Спеціалізовані пристрої для судових досліджень терміналів зазвичай можуть працювати лише з обмеженою серією моделей терміналів та мають високу вартість, але забезпечують повну гарантованість результатів дослідження. Програмне забезпечення не може гарантувати незмінності досліджуваної інформації на терміналі, але є легко доступним, майже завжди — безплатне та надає ті ж вірні результати.

Також слід відмітити, що пристрої та програмне забезпечення, що надаються виробником досліджуваного терміналу, можуть обмежувати доступ до деяких системних областей пам'яті, що можуть містити важливі для експертного дослідження дані. У такому випадку можливо використання методу "фізичного дампу". При використанні даного методу необхідно за допомогою програматору чи іншого пристрою, що може виконувати функції зчитування пам'яті з контролерів, отримати бінарний образ усієї області пам'яті, який буде в подальшому піддаватися дослідженню [5].

У випадку використання програмного забезпечення, що не сертифіковане виробником досліджуваного пристрою або не спеціалізованим програмним забезпеченням для судово-експертних (криміналістичних) досліджень, експерт має перевірити достовірність отриманих

результатів дослідження шляхом візуального огляду згідно відповідних пунктів меню ТСЗ. Наприклад, при використанні програмного засобу "LogoManager Pro Suite" експерт має звернути увагу, що даний засіб не завжди повністю надає всі відомості про SMS, а також не показує номер телефону у телефонній книжці, якщо абонентом йому не присвоєний певний символ або набір символів. У зв'язку з цим, використання подібних програмних засобів у експертній практиці має проводитись лише у виняткових ситуаціях із врахуванням зазначених недоліків.

Перед початком дослідження експерт має перевести ТЗС у режим "політ" (відключення від стільникової мережі), якщо цій режим передбачено у ТСЗ. Так експерт запобігає внесення змін щодо вхідних дзвінків та повідомлень.

При підключенні ТСЗ до комп'ютера експерт повинен при можливості використовувати дата-кабель. Використання Bluetooth-з'єднання можливо лише у випадках, коли підключити ТСЗ до комп'ютеру за допомогою дата- кабелю неможливо. Небажаність використання Bluetooth-з'єднання при дослідженні обумовлено наступними причинами:

– Bluetooth-з'єднання неможливо у режимі "політ" (у випадку відсутності "клітки Фарадея" на ТСЗ можуть поступати вхідних дзвінки та повідомлення);
– при Bluetooth-з'єднанні вносяться зміни у пам'ять ТСЗ.

При дослідженні інформації щодо записів у телефонній книзі ТСЗ, експерт при можливості має зазначити, який тип номеру телефону (загальний, мобільний, домашній тощо) присвоєно тому чи іншому номеру телефону. Разом з цим, у виняткових випадках можна обмежуватись лише загальним наведенням відомостей: яка цифрова, текстова або графічна інформація закріплена за тим чи іншим контактом. Якщо програмній засіб дозволяє проводити аналіз щодо належності того чи іншого контакту до певної групи абонентів, створеної користувачем у телефонній книжці ТСЗ, експерт має наводити відповідні відомості.

При дослідженні вхідних повідомлень експерт може обмежуватись фіксацією основних відомостей про повідомлення (номер або ідентифікатор відправника повідомлення, дата/час відправлення, текст або зображення, що міститься у повідомленні). Інша службова інформація наводиться при необхідності у випадку проведення комплексної експертизи за участю експерта з дослідження телекомунікаційних засобів. Також бажано зазначати, чи має повідомлення статус "прочитане", чи ні.

Дослідження інформації у пам'яті SIM-картки та картки пам'яті бажано проводити за допомогою спеціалізованих пристроїв (смарт-картрідер для SIM-карти та картрідер для картки пам'яті), оскільки таким чином забезпечується безпосередній доступ до носія інформації та з'являється можливість дослідити видалену та іншу інформацію, яку неможливо дослідити під час знаходження у корпусі ТСЗ [4].

SIM-картки можуть надходити на дослідження окремо або у складі смартфонів, мобільних телефонах та інших подібних пристроїв. Оскільки у смартфонах та мобільних телефонах SIM-картка зазвичай міститься під акумуляторної батарею, експерт має врахувати небезпеку втрати даних щодо поточних показів системного календаря та годинника ТСЗ, у складі якого вона поступила.

Перед оглядом меню ТСЗ для встановлення поточних показів системного календаря та годинника експерт має переконатися, що акумуляторна батарея має достатній заряд. У випадку, якщо телефон не вмикається, експерт має спробувати її зарядити, не виймаючи з корпусу телефону, за допомогою відповідного зарядного пристрою.

Якщо у подальшому доступ до меню телефону заблокований PIN-кодом SIM-картки або кодом захисту мобільного телефону, експерт має перевірити, чим саме пристрій заблоковано: SIM-карткою або безпосередньо ТСЗ. Для цього проводиться аналіз інформації у пам'яті SIM-картки за допомогою пристрою читання смарт-карток та спеціалізованого програмного забезпечення. У випадку, якщо SIM-картка заблокована на PIN-код, експерт може спробувати ввести стандартний PIN-код (1111 для "Київстар" та 0000 для МТС) за умови відсутності попередніх спроб введення коду. У випадку, якщо такі спроби вже були, експерт направляє відповідне клопотання про надання додаткових матеріалів.

У випадку, якщо відкриття задньої стінки корпусу ТСЗ з метою доступу до SIM-картки та акумуляторної батареї є складним для експерта, він має ідентифікувати ТСЗ за зовнішнім виглядом, після чого скористатися інструкцію користувача, яка зазвичай міститься на інтернет-сайті виробника мобільного телефону.

До інформації у в пам'яті SIM-картки, що підлягає дослідженню у межах комп'ютерно-технічної експертизи, належить відомості про останні набрані номери, текстові повідомлення (SMS), вміст телефонних книг, відомості про закріплений за SIM-карткою телефонний номер абонента. Також у випадку, якщо на поверхні SIM-картки за-

тертий її серійний номер, експерт може визначити його експертним шляхом — він зберігається у її пам'яті.

При дослідженні інформації про останні набрані номери експерт наводить зміст файлу EF_LND, у тому числі (у випадку наявності) відповідні ідентифікатори, що містяться у файлі EF_LND поряд з номерами телефонів.

При дослідженні текстових повідомлень, інформація про які міститься у файлі EF_SMS, експерт може обмежуватись фіксацією основних відомостей про повідомлення (номер або ідентифікатор відправника повідомлення, дата/час відправлення, текст або зображення, що міститься у повідомленні). Якщо у SIM-карті міститься лише фрагмент (фрагменти) SMS-повідомлення, необхідно зазначити, який саме фрагмент (фрагменти) та скільки всього фрагментів містило SMS-повідомлення. Інша службова інформація наводиться при необхідності у випадку проведення комплексної експертизи за участю експерта з дослідження телекомунікаційних засобів. Бажано зазначати статус повідомлення: "видалене", "прочитане" тощо.

При дослідженні телефонної книги SIM-карти експерт зазначає значення ідентифікаторів та відповідних номерів телефону, відомості про які містяться у файлі EF_ADN.

При дослідженні інформації відносно закріпленого за SIM-карткою абонентського телефонного номеру, експерт наводить інформацію, яка міститься у файлі, але зазначає, що дана інформація могла бути змінена користувачем SIM-карти [3].

При дослідженні SMS-повідомлень та записів у телефонній книзі експерт має враховувати, що оператор мобільного зв'язку може внести відповідну інформацію ще до реалізації SIM-картки кінцевому користувачу. У зв'язку з цим вирішення питань, пов'язаних із походженням інформації у SIM-картці, має проводитись виключно при проведенні комплексної експертизи за участю експерта з дослідження телекомунікаційних засобів.

Список використаної літератури

1. Обзор рынка GSM-операторов Украины за декабрь 2006 года [Электронный ресурс]. — Режим доступа: http://media.mabila.ua/ru/articles/ operts_review_12_07.
2. *Харабуга Ю.С., Білий С.Б.* Дослідження мобільних телефонів і смарт-карт до них у межах комп'ютерно-технічної експертизи / Ю.С. Харабуга, С.Б. Білий // Теорія та практика судової експертизи і криміналістики: зб. наук. праць. Вип. 9. — Х.: Право, 2009. — С. 454–458.

3. Комп'ютерно-технічне дослідження інформації в пам'яті SIM-карток: Звіт з НДР (заключний) / ЛНДІСЕ; кер. Ю.С. Харабуга. — Львів, 2012. — 51 с. — № держреєстрації 0111U000946.
4. Дослідження інформації в пам'яті терміналів стільникового зв'язку (у межах комп'ютерно-технічної експертизи): Звіт з НДР (заключний) / ЛНДІСЕ; кер. Ю.С. Харабуга. — Львів, 2011. — 65 с. — № держреєстрації 0110U002599.
5. Методичні рекомендації дослідження мережевих технологій та пристроїв: Звіт з НДР (заключний) / ХНДІСЕ; кер. О.В. Чишкала. — Х., 2012. — 107 с. — № держреєстрації 0110U001409.

Резюме

Рассмотрены границы компетенции эксперта, возможные опасности потери информации, а также предложена последовательность действий эксперта при компьютерно-техническом исследовании мобильных телефонов, смартфонов и SIM-карт.

Summary

It was considered the competence of the expert, the dangers of loss of information and it was suggested sequence as an expert in computer and technical research of mobile phones and SIM-cards.

УДК 343.98:332

О.І. Буратевич, зав. лабораторії

Київський НДІ судових експертиз

ЩОДО НЕОБХІДНОСТІ ЗАПРОВАДЖЕННЯ НОВОЇ ЕКСПЕРТНОЇ СПЕЦІАЛЬНОСТІ З ПИТАНЬ ЗЕМЛЕУСТРОЮ

Пропонується встановити наступні вимоги до фахівців, які мають намір отримати кваліфікацію судового експерта за спеціальністю "Дослідження з питань землеустрою": вища землевпорядна освіта; досвід роботи у сфері землеустрою, землевпорядкування та кадастру — не менше 1 року.

Відповідно до останніх змін, внесених Наказом Міністерства юстиції України від 26.12.2012 р. № 1950/5 до Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої Наказом Міністерства юстиції України 08.10.1998 р. № 53/5 (далі — Інструкція), до інженерно-технічних видів експертиз окрім будівельно-технічної експертизи віднесені оціночно-будівельна, земельно-технічна та оціночно-земельна.

Також, Наказом Міністерства юстиції України від 26.12.2012 р. № 1950/5 внесені суттєві зміни до Науково-методичних рекоменда-