the same direction, and the second bogi has started to move in another direction. In other words there has occurred turnout incut. In order to check operation of a turnout, various modes of its operation were simulated. Also experimental transits of tram cars were carried out. The obtained data has allowed to draw up a conclusion that the cause of the first tram coming-off from rails was a technical malfunction switch and coincidence of certain circumstances. That is, on the one hand, automatic moving of point switch occurred only for tram movement to the left. On the other hand, the reason of the first tram descent from a railway was that the driver of the second tram has passed entrance harp during the moment when the first tram still was in a pass stage of switch. In article the algorithm of the specialist actions in a similar situation during carrying out of investigatory experiment is resulted and the list of questions solved at carrying out of switch researches, which works in an automatic mode at the moment of traffic accident occurrence is stated.

Keywords: tram car, traffic accident with trams participation, railway line, switch.

УДК 343.148.6:004+621.39

Ю. С. Харабуга, старший науковий співробітник Львівського НДІСЕ

ОСОБЛИВОСТІ КОМП'ЮТЕРНО-ТЕХНІЧНОГО ДОСЛІДЖЕННЯ ІНФОРМАЦІЇ В ПАМ'ЯТІ SIM, USIM ТА R-UIM-КАРТ

Наведено теоретичну та практичну інформацію про особливості дослідження вмісту елементарних файлів SIM, USIM і R-UIM-карт, відомості про які відсутні в чинній редакції методики 10.9.10 «Методика комп'ютерно-технічного дослідження інформації в пам'яті SIM-карток».

Ключові слова: комп'ютерно-технічні дослідження, інформація, елементарний файл, R-UIM, SIM, USIM-карти.

У грудні 2006 р. 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 складала не більше 63 % від загальної чисельності населення, тобто на той час мобільний телефон був фактично в кожних двох із трьох українців[1]. Подібне зростання рівня проникнення стільникового зв'язку в Україні призвело до того, що під час розслідування майже кожної кримінальної справи слідство стикається з питанням дослідження інформації, що міститься в пам'яті мобільних телефонів, уключаючи змінні модулі ідентифікації абонентів стільникового зв'язку. У деяких випадках слідчі обмежуються лише оглядом мобільного телефону та змінного модуля ідентифікації абонента стільникового зв'язку, але часом, особливо в разі вилучення змінного модуля окремо, призначається відповідна судова експертиза.

Існує три типи модулів ідентифікації абонентів стільникового зв'язку: SIM-карти для мереж стандарту GSM, R-UIM-карти для мереж стандарту CDMA та USIM-карти для мереж стандартів UMTS і LTE. Специфічні особ-

[1] Обзор рынка GSM-операторов Украины за декабрь 2006 года. URL: http://media.mabila.ua/ru/articles/operts_review_12_07 (дата звернення: 19.06.2017).

ливості SIM та USIM-карт (фізичні характеристики, логічна модель, функції) регулюються стандартами 3rd Generation Partnership Project (3GPP). Оскільки команда підтримки 3GPP знаходиться в Європейському інституті телекомунікаційних стандартів (ETSI), стандарти 3GPP нині більш відомі як стандарти ETSI. Специфічні особливості R-UIM-карт регулюються стандартами 3rd Generation Partnership Project 2 (3GPP2).

Базовим стандартом для SIM-карт є стандарт ETSI TS 100 977 (3GPP TS 11.11), що більш відомий за своєю початковою назвою GSM 11.11, яку він мав до версії 8.4.0. Цей стандарт визначає інтерфейс між модулем ідентифікації абонента (SIM) і мобільним обладнанням (ME), а також аспекти внутрішньої організації SIM-карти, що належать до її експлуатації в мережі GSM. Протягом деякого часу стандарт ETSI TS 100 977 змінювався. Останньою версію стандарту ETSI TS 100 977 є версія 8.14.0, яка була прийнята у 2007 р.[1]

Ієрархічна структура SIM-карти відповідає ієрархічній структурі смарт-карти стандарту ISO/IEC 7816-4 та складається з трьох типів файлів: головного файлу (MF), призначеного файлу (DF) та елементарного файлу (EF). Для адресації або ідентифікації кожного конкретного файлу використовується ідентифікатор файлу, який складається з двох байтів і має бути закодований у шістнадцятковому форматі. Перший байт ідентифікатора визначає тип файлу (таблиця).

Таблиця

Типи файлів згідно зі стандартом ETSI TS 100 977

Значення 1-го байта файлу	Тип файлу
3F	Головний файл (MF)
2F	EF у головному файлі
7F	DF 1-го рівня
6F	EF у DF 1-го рівня
5F	DF 2-го рівня
4F	EF у DF 2-го рівня

Згідно з методикою 10.9.10 «Методика комп'ютерно-технічного дослідження інформації в пам'яті SIM-карток»[2] комп'ютерно-технічне дослідження інформації в пам'яті SIM-карт полягає в дослідженні вмісту таких елементарних файлів:

[1] ETSI TS 100 977 V8.14.0 (2007-06). URL: http://www.etsi.org/deliver/etsi_ts/100900_100999/100977/08.14.00_60/ts_100977v081400p.pdf (дата звернення: 09.06.2017).

[2] Комп'ютерно-технічне дослідження інформації в пам'яті SIM-карток: звіт про НДР (заключ.)/Львів. НДІСЕ; викон. Ю. С. Харабуга. № ДР 0111U000946. Львів, 2012. 51 с.

— EF_{ICCID} (ідентифікатор 3F00/2FE2) – ідентифікаційний номер карти;
— EF_{IMSI} (ідентифікатор 3F00/7F20/6F07) – міжнародний ідентифікатор абонента мобільного зв'язку;
— EF_{MSISDN} (ідентифікатор 3F00/7F10/6F40) – міжнародний абонентський телефонний номер;
— EF_{ADN} (ідентифікатор 3F00/7F10/6F3A) – телефонна книга;
— EF_{SMS} (ідентифікатор 3F00/7F10/6F3C) – інформація про текстові повідомлення (SMS);
— EF_{LND} (ідентифікатор 3F00/7F10/6F44) – інформація про останні набрані номери.

Як показала експертна практика, у разі, коли на SIM-карті відсутні позначення щодо оператора стільникового зв'язку або замість назви оператора наведений невідомий експерту логотип, доцільно проводити дослідження вмісту елементарного файлу $EF_{SPN.}$ (ідентифікатор 3F00/7F20/6F46), у якому зберігається назва оператора стільникового зв'язку. На відміну від більшості інших елементарних файлів, уміст елементарних файлів EF_{ICCID} та EF_{SPN} можна прочитати із SIM-карти без уведення PIN-коду. Наприклад, у 2007 р. як один із об'єктів комп'ютерно-технічної експертизи у Львівський НДІСЕ надійшла заблокована на PIN-код SIM-карта білого кольору. Згідно з ідентифікаційним номером карти, що починався з цифр 8937201, ця SIM-карта належала оператору мобільного зв'язку Estonian Mobile Telecom. Разом із тим в елементарному файлі EF_{SPN} замість позначення цього оператора містився напис TravelSiM.ua, тобто фактично об'єктом дослідження була туристична SIM-карта TravelSiM.

Для дослідження вмісту елементарних файлів SIM-карти доцільно використовувати програмні засоби, призначені виключено для дослідження інформації в пам'яті змінних модулів ідентифікації абонентів стільникового зв'язку: SIMCon, Dekart SIM Explorer та ін. Що стосується програмних засобів, основним призначенням яких є дослідження інформації в пам'яті мобільних телефонів, смартфонів і планшетів, то ці засоби доцільно використовувати виключно як допоміжні. Наприклад, на відміну від програми SIMCon, програма MOBILedit Forensic дозволяє фіксувати результати дослідження в різноманітних форматах, зокрема XLS і XML. Водночас ця програма не дозволяє отримувати докладну інформацію щодо SMS-повідомлень та інших даних, тобто позбавлена багатьох можливостей програми SIMCon. Що ж стосується програми Dekart SIM Explorer, то її доцільно використовувати для поглибленого аналізу інформації в пам'яті USIM і R-UIM-карт.

До 2017 р. USIM-карти практично не зустрічалися в експертній практиці. Це було пов'язано з тим, що до 2015 р. єдиним оператором стільникового зв'язку стандарту UMTS був оператор ТриМоб, кількість абонентів якого була надто низькою порівняно з абонентами зв'язку стандарту GSM. Ситуація почала змінюватися після того, як усі три українські оператори зв'язку стандарту GSM придбали ліцензії на зв'язок стандарту UMTS і почали готуватися для впровадження 4G-зв'язку.

У травні 2016 р. оператор мобільного зв'язку Lifecell повідомив про доступність LTE-роумінгу в 7 країнах[1]. Станом на травень 2017 р. послуга LTE-роумінг від Lifecell діє вже у 27 країнах. Скористатися LTE-роумінгом може будь-який абонент Lifecell, що попередньо здійснив в одному з офіційних магазинів заміну SIM-карти на USIM-карту, необхідну для підключення до мереж четвертого покоління[2]. У грудні 2016 р. оператор мобільного зв'язку Vodafone Україна повідомив, що повністю перейшов на закупівлю USIM-карт[3]. Отже, станом на травень 2017 р. лише оператор мобільного зв'язку Київстар продовжує використовувати виключно SIM-карти.

Головна відмінність USIM-карти від SIM-карти є використання в SIM-карті призначеного файлу додатків (ADF). Крім того, USIM-карта має додаткові призначені файли, зокрема призначений файл $DF_{PHONEBOOK}$ (ідентифікатор 3F00/7F10/5F3A), у якому у вигляді набору елементарних файлів зберігається телефонна книжка користувача. Якщо в SIM-карті в елементарному файлі EF_{ADN} може зберігатися лише назва контакту та номер телефону, то в USIM-карті завдяки впровадженню додаткових елементарних файлів у $DF_{PHONEBOOK}$, крім назви контакту та основного номера телефону може зберігатися додатковий номер телефону, e-mail та інша додаткова інформація, а самі контакти можуть об'єднуватися в групи.

Відомості про елементарні файли $DF_{PHONEBOOK}$ зберігаються в елементарному файлі EF_{PBR} (ідентифікатор 3F00/7F10/5F3A/4F30). Як у SIM-карті, відомості про назву контакту та номер телефону зберігаються в елементарному файлі EF_{ADN} (ідентифікатор 3F00/7F10/5F3A/4F3A). Що ж стосується елементарних файлів EF_{ANR} та EF_{EMAIL}, у яких зберігається додатковий номер телефону та e-mail, то згідно зі стандартом 3GPP TS 31.102[4] ці елементарні файли можуть мати різні ідентифікатори в різних операторів. Наприклад, в USIM-карті оператора ТриМоб елементарні файли EF_{ANR} та EF_{EMAIL} мають локальні ідентифікатори 4F03 та 4F07, в USIM-карті оператора Vodafone Україна – локальні ідентифікатори 4F00 і 4F06, а в USIM-карті оператора Lifecell елементарні файли EF_{ANR} та EF_{EMAIL} узагалі не використовуються. Такий різнобій призводить до того, що програмний засіб SIMCon 1.2 не може аналізувати вміст елементарних файлів EF_{ANR} та EF_{EMAIL}, а програмний засіб Dekart SIM Explorer 1.4 надає доступ до вмісту елементарних файлів EF_{ANR} та EF_{EMAIL} лише після проведення повного сканування вмісту USIM-карти, що займає понад 15 хв замість 15 с у режимі звичайного сканування.

[1] Lifecell запустив LTE-роумінг у семи країнах. URL: https://www. rbc.ua/ukr/lnews/lifecell-zapustil-lte-rouming-semi-stranah-1463991056.html (дата звернення: 09.06.2017).

[2] Послуга «LTE-роумінг». URL: https://www.lifecell.ua/uk/mobilnij-zvyazok/roaming/lte-roaming/ (дата звернення: 09.06.2017).

[3] Vodafone Україна перейшла на USIM-карти з підтримкою 4G. URL: http://tehnot.com/ua/vodafone-ukraina-pereshla-na-usim-karty-s-podderzhkoj-4g/ (дата звернення: 09.06.2017).

[4] ETSI TS 131 102 V13.4.0. URL: http://www.etsi.org/deliver/etsi_ts/ 131100_131199/131102/13.04.00_60/ ts_131102v130400p.pdf (дата звернення: 09.06.2017).

Отже, на початку дослідження призначеного файлу $DF_{PHONEBOOK}$ USIM-карти експерт за допомогою вмісту EF_{PBR} має встановити склад елементарних файлів, що входять до складу $DF_{PHONEBOOK}$, їх ідентифікатори, а після цього встановлювати додаткову інформацію стосовно контактів, що містяться в елементарному файлі EF_{ADN}.

Не менше складнощів виникає при дослідженні інформації в пам'яті R-UIM-карт. Справа в тім, що згідно зі стандартом 3GPP2 C.S0023[1] в пам'яті R-UIM-карти елементарний файл EF_{SMS}, у якому зберігаються SMS-повідомлення, знаходиться в призначеному файлі DF_{CDMA} (ідентифікатор 3F00/7F25) замість $DF_{TELECOM}$ (ідентифікатор 3F00/7F10). Саме тому в R-UIM-картах оператора стільникового зв'язку CDMA Ukraine в призначеному файлі $DF_{TELECOM}$ зберігається лише елементарний файл EF_{ADN}. Отже, якщо експерт при встановленні вмісту SMS-повідомлень у пам'яті R-UIM-карти обмежиться спробою дослідження елементарного файлу 3F00/7F10/6F3C, то він припуститься експертної помилки.

Для встановлення вмісту елементарного файлу 3F00/7F25/6F3C за допомогою програмного засобу Dekart SIM Explorer 1.4 необхідно провести повне сканування вмісту R-UIM-карти. Оскільки ця версія зазначеного програмного засобу не передбачає розшифрування вмісту елементарного файлу 3F00/7F25/6F3C, установлення змісту SMS у пам'яті R-UIM-карти потрібно проводити за таким алгоритмом:

— експерт проводить повне сканування вмісту R-UIM-карти та зберігає результати сканування в .sim файл;

— в отриманому .sim файлі експерт за допомогою текстового в розділі [0x7F25] знаходить три текстових рядка, що відповідають елементарному файлу 0x6F3C, і переносить їх у кінець розділу [0x7F10];

— після переносу рядків у розділ [0x7F10] експерт змінює число після букв EF на початку кожного рядка так, аби нове число було наступним щодо попередньої групи рядків (наприклад, стрічка EF27 на початку кожного з трьох рядків змінюється на EF13, якщо попередня група рядків у розділі [0x7F10] починається з комбінації символів EF12);

— збережений файл знову відкривається програмою Dekart SIM Explorer 1.4, після чого встановлюється зміст SMS-повідомлень, наявних в елементарному файлі EF_{SMS}.

Як відомо, стандарт для SMS-повідомлень передбачає можливість відправлення сегментованих повідомлень. Оскільки програма програмного засобу Dekart SIM Explorer 1.4 не розшифровує подібну інформацію, що зберігається в заголовку даних користувача (User Data Header), при дослідженні вмісту сегментованих повідомлень за допомогою цього програмного засобу експерт має самостійно встановлювати, із скількох сегментів мало складатися повідомлення та яким сегментом є досліджуваний сегмент. Зазвичай це адреси 0x20 (кількість сегментів) і 0x21 (номер поточного сегмента) від початку конкретного запису в EF_{SMS}.

[1] 3GPP2 C.S0023-D v2.0. URL: http://www.3gpp2.org/Public_html/Specs/C.S0023-D_v2.0_R-UIM_20111231.pdf (дата звернення: 09.06.2017).

Під час дослідження R-UIM-карт оператора Vodafone Україна (МТС Україна) необхідно звернути увагу, що вони призначені лише для використання в USB-модемах і не розраховані на прийом SMS-повідомлень, тому немає потреби проводити повне сканування даних R-UIM-карт.

Нарешті, як показала експертна практика, певні проблеми можуть також виникати при ідентифікації R-UIM-карт, оскільки оператори CDMA-зв'язку CDMA Ukraine та Інтертелеком в ідентифікаційному номері карти замість міжнародного телефонного коду України 380 указують мобільний код країни (MCC) 255. Урахування цієї та іншої наведеної інформації щодо вмісту окремих елементарних файлів допоможе уникнути експертних помилок під час комп'ютерно-технічного дослідження інформації в пам'яті SIM, USIM і R-UIM-карт.

ОСОБЕННОСТИ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОГО ИССЛЕДОВАНИЯ ИНФОРМАЦИИ В ПАМЯТИ SIM, USIM И R-UIM-КАРТ

Харабуга Ю. С.

Приведены теоретическая и практическая информации об особенностях исследования содержимого элементарных файлов SIM, USIM и R-UIM-карт, сведения о которых отсутствуют в действующей редакции методики 10.9.10 «Методика компьютерно-технического исследования информации в памяти SIM-карточек».

Ключевые слова: компьютерно-технические исследования, информация, элементарный файл, R-UIM, SIM, USIM-карты.

FEATURES OF COMPUTER TECHNICAL RESEARCH OF THE INFORMATION IN THE MEMORY OF SIM, USIM AND R-UIM-CARDS

Harabuga Yu. S.

The paper considers the features of expert research of elementary files contents of SIM, USIM and R-UIM-cards, the information on which is absent in the current edition of technique 10.9.10 «Technique of computer technical research of information in the memory of SIM-cards». Effective standards which regulate the structure of files in SIM, USIM and R-UIM-cards, are specified. For today there are three types of identification modules of cellular communication customers: SIM-cards for networks of standard GSM, R-UIM-cards for networks of standard CDMA and USIM-cards for networks of standards UMTS and LTE. The hierarchical structure of a SIM-card corresponds to the hierarchical structure of a smart card of standard ISO/IEC 7816-4 and consists from three types of files: the main file (MF), the intended file (DF) and an elementary file (EF). For addressing or identification of each concrete file the identifier of a file is used which consists of two bytes. The first byte of the identifier defines file type. The attention is paid to the elementary file EF_{SPN} in which the name of a cellular communication operator is stored. The theoretical and practical information concerning research of the content of the intended file $DF_{PHONEBOOK}$ is presented in which the telephone book of an USIM-card is stored. It's specified that elementary file EF_{SMS} is stored in the memory of a R-UIM-card in other intended file in comparison with SIM and USIM-cards. The research algorithm of contents

EF_{SMS} file in memory of a R-UIM-card is offered. The attention that in identification number of a R-UIM-card some Ukrainian CDMA-operators specify a mobile code of the country 255 instead of the international telephone code of Ukraine 380, is paid. Keeping in mind the presented information will help to avoid expert errors during computer technical research of the information in the memory of SIM, USIM and R-UIM-cards.

Keywords: computer technical researches, information, elementary file, R-UIM, SIM, USIM-cards.

УДК 343.98

Р. Н. Гусейнов, судовий експерт Харківського НДІСЕ

АЛГОРИТМ ВИЗНАЧЕННЯ КАТЕГОРІЇ ОБ'ЄКТА ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ ЗА ТЕХНОГЕННОЮ НЕБЕЗПЕКОЮ

Розглянуто основні етапи при проведенні ідентифікації потенційно небезпечних об'єктів і об'єктів підвищеної небезпеки, що дозволить систематизувати процес дослідження та прискорити проведення судових експертиз і експертних досліджень стосовно визначення категорії об'єкта господарської діяльності за техногенною небезпекою.

Ключові слова: потенційно небезпечний об'єкт, об'єкт підвищеної небезпеки, небезпечна речовина, порогова маса, джерело небезпеки, надзвичайна ситуація.

Функціонування на території України численних об'єктів господарської діяльності, де наявні джерела та чинники небезпеки, підвищує ймовірність виникнення аварій чи катастроф, які можуть загрожувати життю й здоров'ю людей, погіршенню стану природного середовища та великими матеріальними збитками. Однією зі складових зменшення ризику надзвичайних ситуацій (НС) на цих об'єктах є проведення аналізу їх структури та характеру функціонування з метою виявлення потенційних джерел небезпеки, які за певних обставин можуть ініціювати (викликати реальну загрозу) виникнення НС.

Для досягнення цього необхідно провести дослідження з визначення категорії об'єкта господарської діяльності за техногенною небезпекою, що складається з двох етапів:

— проведення ідентифікації потенційно небезпечного об'єкта (ПНО);

— проведення ідентифікації об'єкта підвищеної небезпеки (ОПН).

Результати проведених досліджень нададуть змогу розробити на об'єктах господарської діяльності встановленої категорії за техногенною небезпекою відповідні заходи щодо попередження НС, мінімізації ризику їх виникнення та підготовки до реагування на них.

Слід зазначити те, що при проведенні таких досліджень виникає низка питань, оскільки ця процедура є складною та трудомісткою. Багато труднощів виникає при ідентифікації великих об'єктів.