УДК 343.9

А. С. Воронков
ФБУ Российский федеральный центр судебной экспертизы
при Министерстве юстиции России, Москва, e-mail: pork12@bk.ru

Д. К. Воронкова
ФГБОУ ВО «Московский государственный технический университет
имени Н.Э. Баумана (национальный исследовательский университет)»,
Москва, e-mail: voronkovadk@bmstu.ru

А. М. Пилипчак
ИнфоТеКС, Москва, e-mail: alexeypilipchak@mail.ru

КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЕ ИССЛЕДОВАНИЕ SIM-КАРТ СРЕДСТВАМИ ПРОГРАММИРУЕМОЙ ПЛАТЫ ARDUINO

Ключевые слова: судебная компьютерно-техническая экспертиза, экспертиза устройств мобильной связи, SIM-карта, аппаратная платформа Arduino.

Сегодня телекоммуникационные и компьютерные технологии находятся на пике своего развития, что позволяет применять их во всех сферах жизнедеятельности человека. Конечно, мобильные устройства не остались в стороне. В настоящее время они используются повсеместно. В связи с их широкой распространённостью происходит и увеличение числа преступлений, которые напрямую связаны с их использованием. Мобильное устройство является типовым объектом судебной компьютерно-технической экспертизы. Важно подчеркнуть, что на мобильном устройстве, представленном на исследование, могут содержаться внешние карты памяти (SD Card) и SIM-карты. В рамках уголовного дела SIM-карта может фигурировать как вещественное доказательство, хранящее в себе криминалистически значимую информацию. Таким образом, и SIM-карта является типовым объектом судебной компьютерно-технической экспертизы. В данной статье рассматривается понятие SIM-карты, ее строение и способы взаимодействия с ней по стандарту для смарт-карт «ISO–7816». Особое внимание в работе уделяется правилам подготовки и исследования SIM-карты. Исследуется возможность получения доступа к информации, хранящейся на SIM-карте, с использованием аппаратной платформы Arduino на конкретном примере получения данных о последнем сообщении. Приводится схема подключения SIM-карты к программируемой плате Arduino Uno и набор команд и параметров, используемых для взаимодействия с SIM-картой.

A. S. Voronkov
Russian Federal Center for Forensic Science under the Ministry of Justice of Russia,
Moscow, e-mail: pork12@bk.ru

D. K. Voronkova
Bauman Moscow State Technical University, Moscow,
e-mail: voronkovadk@bmstu.ru

A. M. Pilipchak
InfoTeCS, Moscow, e-mail: alexeypilipchak@mail.ru

COMPUTER FORENSICS OF SIM-CARDS BY MEANS OF THE PROGRAMMABLE ARDUINO BOARD

Keywords: computer forensic, examination of mobile communication devices, SIM-card, Arduino hardware platform.

Today telecommunications and computer technologies are at the peak of their development, which allows them to be used in all human environments. Mobile devices are not left out. They are currently back. Due to their widespread occurrence and increase in cases of crimes that are associated with their use. A mobile device is a typical punishment for computer forensics. It is important to draw that external memory cards

(SD-cards) and SIM-cards can be obtained for the detection presented in the study. As part of the consideration of cases, the SIM-card may appear as disclosed evidence that contains forensically significant information. Thus, the SIM-card is also a typical computer forensics. This article includes the principle of a SIM-card, its structure and relationship with it according to the standard for smart cards "ISO-7816". Particular attention should be paid to the rules for preparing and examining SIM-cards. The possibility of accessing information stored on a SIM-card using the Arduino hardware platform to detect the transmission of data about the last transmission is being investigated. A diagram of connecting a SIM-card to a programmable Arduino Uno board and a set of commands and parameters related to interaction with a SIM-card is given.

Введение

Компьютеризация – процесс, охватывающий все сферы современной человеческой жизнедеятельности. В настоящее время сложно представить себе хотя бы один элемент общественной жизни, в которой человек обходился бы без использования компьютерной техники.

Согласно статистике МВД России, каждое четвертое преступление совершается с использованием информационно-телекоммуникационных технологий [1]. Увеличение числа компьютерных преступлений, повсеместная компьютеризация и автоматизация процессов обуславливают увеличение количества судебных компьютерно-технических экспертиз (далее – СКТЭ).

СКТЭ основывается на специальных знаниях в сфере электроники, электротехники, информационных систем и процессов, радиотехники и связи, вычислительной техники и автоматизации [2].

Типовыми объектами СКТЭ являются персональные компьютеры, периферийные устройства (принтеры, модемы и т.д.), микросхемы, мобильные телефоны и т.п.

Одним из типовых объектов СКТЭ является и SIM-карта, которая в рамках уголовного дела может фигурировать как вещественное доказательство, хранящее в себе криминалистически значимую информацию.

Значимость данной работы состоит в распространённости SIM-карт как самостоятельных объектов СКТЭ. Особенностями данного типа объектов является возможность их использования мобильными телефонами и иными объектами СКТЭ, оснащенными GSM модулем как средства доступа к сети сотовой связи. Необходимость доступа к вышеназванным сетям и обуславливает наличие SIM-карты в подавляющем большинстве поступающих на исследование мобильных телефонов. При исследовании поступившего на исследование мобильного телефона экспертом тщательно проверяется наличие в «лотках», предназначенных для подключения SIM-карты, соответствующей SIM-карты. Для проверки наличия рассматриваемого объекта эксперт использует соответствующую документацию на мобильный телефон (например, руководство пользователя) и изучает все описанные в ней возможности подключения SIM-карты. В ряде случаев на телефонах может использоваться нестандартное расположение «лотка» для SIM-карты, а также не исключена возможность модификации внутреннего строения телефона с целью скрыть факт подключения SIM-карты и, как следствие, возможность доступа к сети сотовой связи.

К самой SIM-карте в процессе исследования применяются обычные правила исследования информационных компьютерных средств, в частности, описание объекта с фото- и текстовой фиксацией информации, извлечение информации из объекта средствами аппаратно-программных комплексов, анализ извлеченных данных, с целью ответа на поставленные перед экспертом вопросы, составление заключения. Вне зависимости от наличия SIM-карты в списке поступивших на исследование объектов, эксперт в тексте заключения описывает и исследует ее как самостоятельный объект с привязкой к объекту, поступившему на исследование. После привязки объекта исследования к поступившему объекту, SIM-карта может фигурировать в тексте экспертного заключения как самостоятельный объект, и все вопросы, поставленные перед экспертом, подлежат разрешению, в том числе, в отношении этого объекта.

Целью данной работы является получение доступа к криминалистически значимой информации, хранящейся на SIM-карте, средствами программируемой платы Arduino, в целях раскрытия, расследования и предупреждения преступлений.

Материалы и методы исследования

Источниками исследования является научная литература, в которой освещаются вопросы применения компьютерных технологий в судебно-экспертной деятельности,

а также методическая литература, содержащая основные положения производства СКТЭ. Методологическую базу исследования составили общенаучные методы исследования (анализ, синтез), а также эмпирические методы (наблюдение, сравнение, эксперимент и описание).

Результаты исследования и их обсуждение

SIM-карта – это контактная смарт-карта с собственным процессором, способная регистрироваться в мобильной сети. SIM-карта имеет постоянную (энергонезависимую) и оперативную память. Также есть модуль аппаратного шифрования и аппаратный генератор случайных чисел. Процессор SIM-карты работает на частоте до 10 МГц. Постоянная память делится на области: примерно 60% занимают данные оператора, 20% – операционная система, остальное – данные пользователя [3].

С помощью SIM-карты обеспечивается идентификация абонентского устройства, ее доступ к сети связи, а также защита от несанкционированного использования абонентского номера. Идентификация SIM-карты осуществляется с использованием международного идентификационного номера IMSI, однозначно соответствующего пользовательскому (абонентскому) номеру. Международный идентификатор IMSI, наряду с серийным номером телефонного аппарата IMEI задействуется в идентификации пользователя коммутационным оборудованием сети при установлении и поддержании соединения.

На SIM-карте, как самостоятельном объекте исследования, могут храниться электронные следы. В частности, информация, вводимая абонентом, информация, накопленная на носителе при работе в сетях электросвязи, а также иная криминалистически значимая информация. В настоящее время вышеперечисленные данные хранятся в памяти телефонов, однако все эти данные можно хранить и на SIM-карте.

Изучая процедуру получения доступа к информации, хранящейся на SIM-карте, следует упомянуть, что аппаратно-программные комплексы, а также программные продукты, которые применяются в судебно-экспертных учреждениях, являются достаточно дорогостоящими (например, Encase Smartphone Examiner, MOBILedit! Forensic,и т.п.). Однако существуют иные способы и методы получения доступа к такой информации, например, с использованием аппаратной платформы Arduino.

Прежде чем перейти к непосредственному извлечению информации, хранящейся на SIM-карте, считаем целесообразным рассмотреть понятие аппаратной платформы Arduino.

Arduino – это электронная платформа с открытым исходным кодом, основанная на простом в использовании аппаратном и программном обеспечении [4]. Работа такой платформы заключается в считывании входного сигнала и его преобразования в выходной сигнал. С помощью Arduino можно создавать разные устройства для преследования разных целей. В том числе, рассматриваемая аппаратная платформа может использоваться и при исследовании объектов СКТЭ. Конечно, только лишь платформы будет недостаточно, поскольку при отправке какого-либо набора инструкций на микроконтроллер для выполнения определенных действий, необходимо использовать язык программирования «Arduino» и программное обеспечение «Arduino IDE».

Преимуществами Arduino являются дешевизна, кроссплатформенность, а также модульная структура, которая обеспечивает гибкость и аппаратную мощность платформы.

Для снятия данных с SIM-карты необходимо наличие следующих элементов:

1) плата Arduino UNO;

2) терминал, который будет принимать данные с Arduino на компьютер;

3) исследуемая SIM-карта;

Следует отметить, что перед проведением исследования необходимо изучить стандарт ISO-7816, который закрепляет основные положения протокола обмена данными с SIM-картой, а также ряд особенностей, связанных с непосредственной работой SIM-карты [5].

Кроме того, для верного извлечения и изучения информации с SIM-карты нужно знать:

1. Устройство SIM-карты.

2. Значение контактов SIM-карты.

3. Команды, с помощью которых происходит общение SIM-карты с мобильным устройством.

4. Файловую систему SIM-карты.

Необходимо подготовить к проведению исследования, аппаратную часть, подключив SIM-карту к Arduino. Для этого определяется, какие выводы имеет SIM-карта (рис. 1).

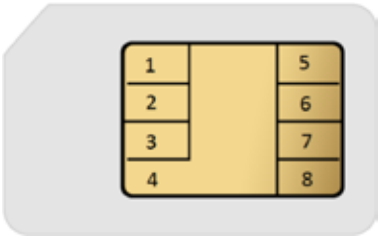

Рис. 1. Распиновка SIM-карты

При установлении подключения между платой Arduino и SIM-картой используются следующие контакты:

1 – неиспользуемый контакт.

2 – I/O – линия последовательного интерфейса ввода/вывода.

3 – VPP – контакт программирования, которое используется при записи служебной информации

4 – GND – «земля»;

6 – CLK – синхросигнал (тактирование);

7 – Reset – контакт сброса;

8 – VCC – питание;

Установление подключения происходит посредством пайки к указанным в стандарте контактам и соединением с выводами платы Arduino по следующей схеме, представленной на рис. 2.

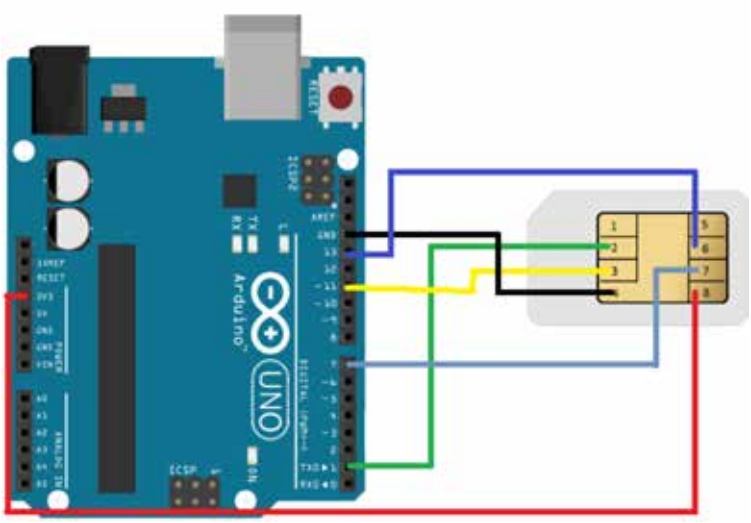

Рис. 2. Подключение SIM–карты к Arduino Uno

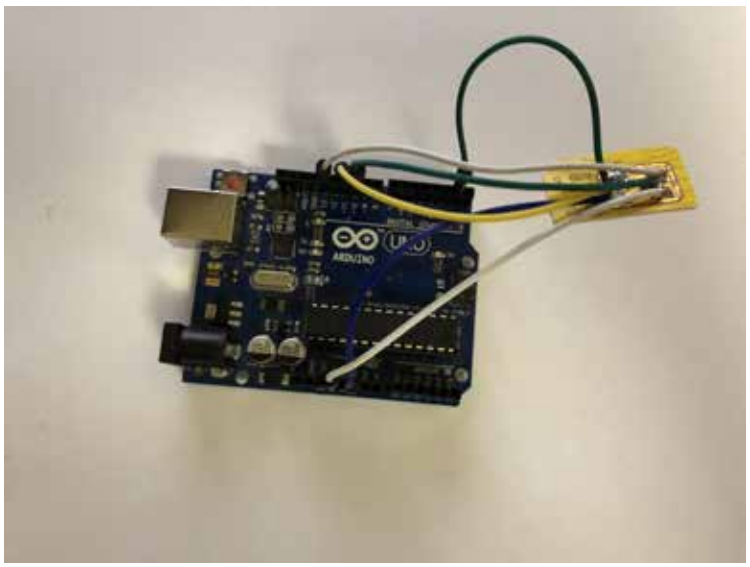

Рис. 3. Внешний вид подключения SIM–карты к Arduino Uno

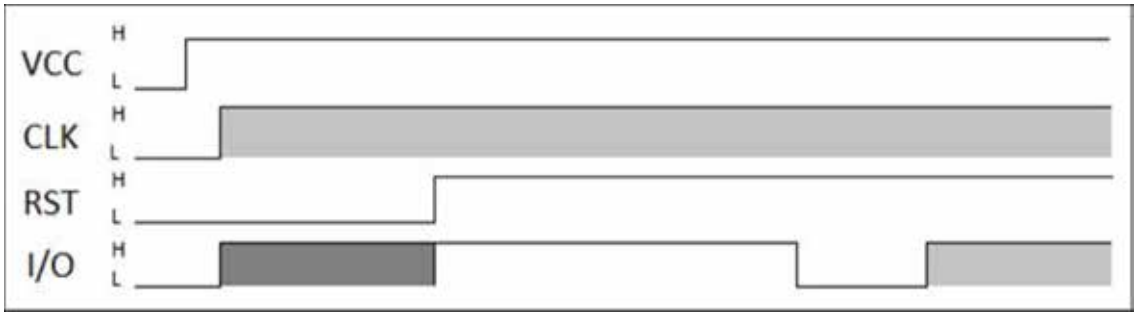

Рис. 4. Временная диаграмма включения SIM–карты

Таблица 1

Пример команд и их кода в шестнадцатеричном виде

Команда	Код инструкции	Параметр инструкции 1	Параметр инструкции 2	Количество байт в данных, передаваемых командой
SELECT	A4	00	00	02
STATUS	F2	00	00	длина
READ RECORD	B2	номер записи	режим	длина
UPDATE RECORD	DC	номер записи	режим	длина

Так как SIM-карта является разновидностью Smart-карт, вся технология снятия будет полностью основываться на стандарте ISO–7816. Обмен данными производится с использованием USART интерфейс со следующими параметрами: скорость передачи = 9600 Бод, частота = 3,5МГц.

Для начала работы с SIM-картой ее требуется «активировать». Для этого необходимо подать на RST низкий уровень, на VCC подать питание, начать «щелкать» синхросигналом CLK с заданной частотой. Через 4000 циклов перехода синхросигнала CLK подать на RST высокий уровень.

После «активации» SIM-карты нужно выставить RST на низкий уровень, затем SIM-карта отправит ATR (Answer–to–Reset) – ответ с информацией о частоте синхронизации, списком поддерживающих протоколов передачи и т.д.

В ATR первый байт (8 бит) говорит о том, какая кодировка применятся SIM-картой (прямая или инверсная). При прямом кодировании первый байт равен 0x3B, при инверсном – 0x3F. Инверсное кодирование означает, что логическая 1 (единица) кодирует в себе логический 0 (ноль) и наоборот.

Когда ATR получен, можно продолжить «общение» с SIM-картой основываясь на подобранной кодировке. Общение происходит при помощи встроенного терминала в программное обеспечение «Arduino IDE», с помощью которого происходит программирование платы «Arduino UNO».

Общение с SIM-картой осуществляется с помощью передаваемых команд. Команды состоят из заголовка команды (4 байта) и тела команды. Пример команд и их соответствующий код можно посмотреть в таблице 1.

Структура памяти SIM- карты состоит из файлов-каталогов и элементарных файлов. В структуре файловой системы имеются:

- корневой файл-каталог – «Master File» («MF»);
- выделенные файлы-каталоги «Dedicated File» («DF»);
- элементарные файлы (записи) «Elementary File» («EF»).

Выделенный файл («DF») – это функциональная группа файлов, состоящая из него самого и всех тех файлов, которые он в себя включает (то есть он состоит из «DF» и его полного «поддерева»). Такой файл состоит только из заголовочной части. Заголовок файла содержит информацию о структуре и атрибутах файла.

Все элементарные файлы состоят из заголовка и части данных файла.

Элементарные файлы различаются по своей структуре. В стандарте «GSM» ис-

пользуется следующие три структуры элементарных файлов:

1. Прозрачный «EF» – имеет структуру заголовка, в котором содержится смещение начала данных файла и общая длина этих данных, а сами данные представляют собой последовательность байт.

2. Линейный фиксированный «EF» – имеет структуру последовательности записей одинаковой (фиксированной) длины. Первой записью является запись номер 1. Длина записи, а также это значение, умноженное на количество записей, указывается в заголовке файла.

3. Циклический «EF» – используется для записей, хранящихся в хронологическом порядке. Когда все пространство записи занято, новые сохраненные данные будут перезаписать самую старую информацию.

Каждый файл имеет идентификатор. Идентификатор файла используется для адресации и идентификации каждого конкретного файла. Такой идентификатор состоит из двух байтов и закодирован в шестнадцатеричной системе счисления.

Первый байт идентификатора указывает на тип файла:

- «3F»: мастер-файл;
- «7F»: выделенный файл;
- «2F»: элементарный файл в основном мастер-файле;
- «6F»: элементарный файл в выделенном файле.

Часть структуры файловой системы SIM-карты представлена в таблице 2.

В качестве эксперимента в ходе написания статьи был получен текст первого SMS–сообщения, которое содержится на SIM-карте. Для этого был отправлен заголовок команды «Select» – A0 A4 00 00 02. После чего необходимо дождаться ответа от SIM-карты (3 байта). После получения ответа было отправлено тело команды – 7F 10 (7F – id файла, 10 – тело файла (каталога) «MF»), далее была отправлена команда A0 A4 00 00 02, 6F 3C – таким образом был совершён переход из корневого каталога в каталог «EF sms». После проведения подготовительных действий по переходу в интересующий нас каталог была отправлена команда «READ RECORD»: A0 B2 01 04 B0.

После получения команды по считыванию указанной записи, SIM-карта отправляет ответ в виде кодированных данных (рис. 5).

Таблица 2

Часть структуры файловой системы SIM-карты

Тип объекта	**Идентификатор объекта**	**Родительский элемент(ы) для объекта**	**Дочерние элементы(ы) для объекта**	**Описание**
MF (Master File)	3F00	-	DF gsm, DF telekom, DF pp-cts, EF iccid, EF elp	Корневой файл-каталог
DF gsm	7F20	MF (Master File)	-	Выделенный файл
DF telekom	7F10	MF (Master File)	DF graphics, EF sms, EF pin, EF and	Выделенный файл
DF pp-cts	7F23	MF (Master File)	-	Выделенный файл
EF iccid	2FF2	MF (Master File)	-	Элементарный файл в основном мастер-файле
EF elp	2F05	MF (Master File)	-	Элементарный файл в основном мастер-файле
DF graphics	5F50	DF telekom	EF img	Выделенный файл
EF sms	6F3C	DF telekom	-	Элементарный файл в выделенном файле
EF pin	6F3B	DF telekom	-	Элементарный файл в выделенном файле
EF and	6F3A	DF telekom	-	Элементарный файл в выделенном файле
EF img	4F20	DF graphics	-	Элементарный файл

Рис. 5. Окно терминала программы «Arduino IDE» полученным сообщением с SIM–карты

Ответ в виде кодированных данных о первом SMS-сообщении выглядит следующим образом:

«B2 07 07 91 97 61 55 63 56 F6 11 FF 09 81 97 71 29 78 56 F6 00 08 FF 0C 04 1F 04 40 04 38 04 32 04 35 04 42 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 90 00».

В представленных данных, отправленных SIM-картой, можно выделить следующие области:

B2 07 – идентификатор начала сообщения;

97 61 55 63 56 F6 – номер получателя 7 916 553 66 56 (младший байт – старший);

97 71 29 78 56 F6 – номер отправителя 7 917 928 76 56;

08 – кодировка (08 – кириллица);

0C – длина сообщения (12 байт);

04 1F 04 40 04 38 04 32 04 35 04 42 – содержимое сообщения: «Привет».

Заключение

В ходе проведенного исследования был проведен эксперимент по извлечению данных с SIM-карты, путем установления «общения» между аппаратной платой Arduino и исследуемой SIM-картой, полученные данные, в точности соответствовали данным реально хранимым на исследуемом носителе информации. Именно это позволяет сделать вывод о возможности применения экспертом вышеописанного метода в качестве альтернативного при исследовании SIM-карты в рамках проведения им судебной компьютерно-технической экспертизы.

Библиографический список

1. Ежемесячный сборник о состоянии преступности в России. [Электронный ресурс]. URL: http://crimestat.ru/analytics (дата обращения: 03.05.2022).

2. Воронкова Д.К., Воронков А.С., Пилипчак А.М. Комплексная судебная компьютерно-техническая и видеотехническая экспертиза. Modern Science. 2019. № 12-1. С. 300-306.

3. Что такое SIM-карта. Секреты вашей симки. [Электронный ресурс]. URL: https://www.iphones.ru/iNotes/sekrety-sim-karty-o-kotoryh-vy-ne-znali-06-16-2019 (дата обращения: 03.05.2022).

4. RUSOLUT – Data Investigation & Recovery Technology. [Электронный ресурс]. URL: https://rusolut.com/ (дата обращения: 03.05.2022).

5. ISO/IEC 7816-9:2017. Identification cards – Integrated circuit cards – Part 9: Commands for card management. [Электронный ресурс]. URL: https://www.iso.org/standard/67802.html (дата обращения: 03.05.2022).