О поиске владельца мобильного телефона

Банин Ю.В., Кизилов Д.М., Намиот Д.Е.

***Аннотация*—Настоящая работа посвящена развитию системы цифровых сертификатов для мобильных устройств. Сертификат является объектом, который подтверждает факт владения мобильным устройством (телефоном). Сертификат содержит идентификацию самого устройства (например, IMEI), которая подтверждается идентификацией владельца в социальной сети. Аккаунт в социальной сети выступает в качестве подписи владельца. Сертификаты создаются владельцами с помощью специального мобильного приложения. А для поиска по накопленной базе сертификатов создано отдельное веб-приложение. Развитию этой модели и посвящена данная работа.**

***Ключевые слова*— сертификат, IMEI, социальная сеть.**

I. Введение

В данной статье представлены результаты двух квалификационных работ, выполненной в лаборатории Открытых Информационных Технологий факультета ВМК МГУ имени М.В. Ломоносова в рамках исследований в области телекоммуникационных сервисов и приложений [1]. Работы были посвящены развитию системы цифровых сертификатов для подтверждения факта владения мобильным устройством (телефоном) [2]. Цифровые сертификаты здесь - это схема, которая позволяет зафиксировать факт владения мобильным телефоном. Владелец телефона с помощью такого сертификата подтверждает (фиксирует) свои права на телефон (на дату создания сертификата, конечно). Все сертификаты собираются в общей базе данных, где заинтересованные пользователи (и/или, что особенно важно, приложения) могут искать информацию. По данным мобильного телефона можно искать информацию о владельце (владельцах), а по данным о владельце, соответственно, искать информацию о мобильных устройствах.

Таким образом, с практической точки зрения, эта схема включает в себя мобильное приложение (где, в первую очередь, и создается сертификат), базу данных (для хранения сертификатов) и веб-интерфейс (веб-портал), который обеспечивает взаимодействие с пользователями (и/или программами) при поиске информации.

Первая полная реализация данной модели была выполнена А.Колосовой [3]. Дальнейшее развитие проекта описано в работах [2][4]. Разработка продолжалась как университетский проект с открытым кодом. В настоящей статье описываются новые элементы, добавленные в модель, а также и в ее реализацию весной 2014 года.

II. Модель цифровых сертификатов

Мобильные телефоны становятся все меньше и дороже, поэтому они часто теряются и становятся объектом посягательства воров. По статистике самым частым видом воровства является кража мобильных телефонов, так как они являются наиболее широко распространенным видом электронной техники среди населения.

Однако вместе с ростом числа краж растет и число способов противодействия им.

Самый распространенный и действенный способ в мире — это блокировка украденного аппарата оператором, используя IMEI. С помощью технических средств, которые имеются у операторов связи, можно локализовать местонахождение включенного телефона с точностью до нескольких сотен метров [5].

Однако, что же делать, если украденное или потерянное мобильное устройство не обладает функциями телефонии, то есть отсутствует IMEI? У всех подобных аппаратов имеются различные идентификационные номера, которые могут быть использованы для нахождения утерянного устройства, мониторинга установок на него некоего приложения, генерации технических средств защиты авторских прав (DRM – digital rights management).

Существует множество идентификаторов мобильного оборудования. В основном, это электронные номера, дающие возможность описать физические параметры мобильного устройства, дающие описание абонента, сетевого оборудования, местоположения. Некоторые номера присваиваются при создании оборудования, другие генерируются при первом включении. Также номера нужны для отчетности в бухгалтерских и иных документах.

В сетях GSM/GPRS/UMTS используются свои идентификаторы. Часть из них являются временными и используются для конфиденциальности и безопасности. Некоторые идентификаторы являются общими для CS (Circuit Switched) и PS (Packet Switched) режимов работы MS (Mobile Station), некоторые нет. Одни

Статья получена 15 июля 2014.

Ю.В. Банин – выпускник программы РКТ факультета ВМК МГУ имени М.В.Ломоносова. (email: yuribanin@mail.ru)

Д.М. Кизилов – выпускник программы РКТ факультета ВМК МГУ имени М.В.Ломоносова. (email: kizilovd@gmail.com)

Д.Е. Намиот – старший научный сотрудник лаборатории ОИТ, факультета ВМК МГУ имени М.В.Ломоносова. (email: dnamiot@gmail.com)

идентификаторы связаны с sim-картами, другие ориентированы на устройство. Ниже (рисунок 1) приведена классификация идентификаторов:

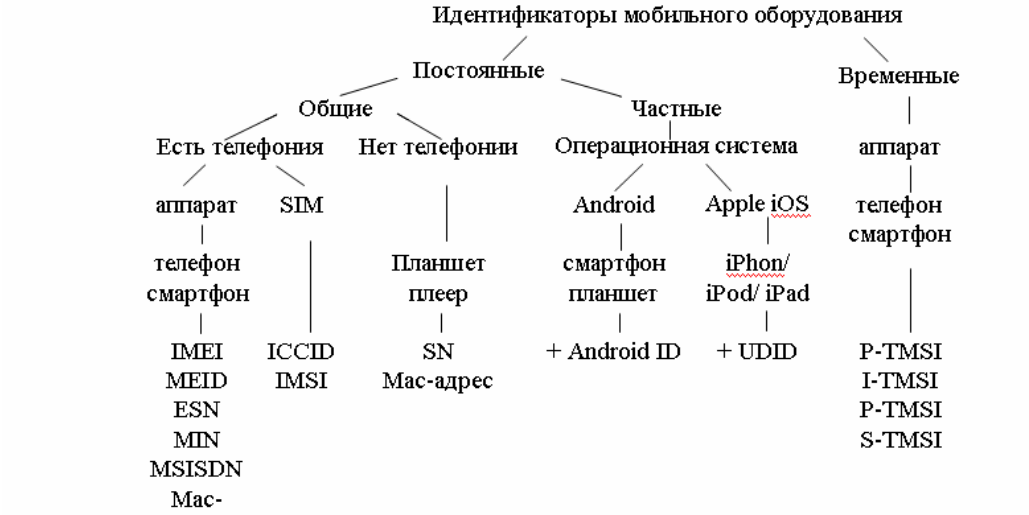

Рисунок 1. Идентификаторы мобильного оборудования

Опишем некоторые из них:

MIN (Mobile Identification Number) – это мобильный идентификационный номер телефон. Этот номер однозначно идентифицирует мобильный телефон, в аналоговой сотовой связи. MIN используется для маршрутизации вызова. Технически – это 34-битное число, разделенное на две половинки. Младшие 10 бит обозначаются MIN2 и отвечают за хранение кода области (area code), оставшиеся 24 бита - личный номер мобильного устройства.

IMEI (International Mobile Equipment Identity) - международный идентификатор мобильного устройства. Используется для телефонов GSM WCDMA IDEN. Функции: идентификация устройства в сети, отслеживание аппарата, блокирование краденого телефона на уровне оператора сотовой связи. IMEI и MIN выбираются не случайным образом и должны соответствовать друг другу.

ESN (Electronic Serial Number) – электронный серийный номер. Используется для телефонов CDMA. Функции: защита от проникновения в сеть нелегальных абонентов.

MEID (Mobile Equipment IDentifier) - мобильный идентификатор оборудования. Определяет физический компонент CDMA оборудования мобильной станции.

MSISDN (Mobile Subscriber Integrated Services Digital Number) — номер мобильного абонента цифровой сети с интеграцией служб. Используется в телефонах GSM, UMTS. Задачи: передача номера телефона назначенному абоненту, получение звонков на телефон. Главный MSISDN номер используется для идентификации абонента при предоставлении большинства услуг. В соответствии с E.164 состоит из трех частей:

кода страны (CC — Country Code),

национального кода направления (NDC — National Destination Code)

номер абонента (SN — subscriber number).

IMSI (International Mobile Subscriber Identity) — международный идентификационный номер мобильного абонента , ассоциированный с каждым пользователем мобильной связи стандарта GSM, UMTS или CDMA. Первые три цифры - это MCC (Mobile Country Code, мобильный код страны). За ним следует MNC (Mobile Network Code, код мобильной сети). Код мобильной сети может содержать две цифры по европейскому стандарту или три по североамериканскому. Все последующие цифры — непосредственно идентификатор пользователя MSIN.

SN (Serial Number) – серийный номер. Это серийный номер изделия, присвоенный на заводе-изготовителе при выпуске

ICCID (Integrated Circuit Card Id) Код содержится на SIM карте и определяется в соответствии со стандартом ITU-T E.118.

Android ID. Поддерживается на устройствах с OS Android. Используется при скачивании приложений с сайтов Google Play, которым необходима идентификация устройства (благодаря нему они знают, что это именно то устройство, которое использовалось при оплате за приложение). Это 64 битный номер, который случайным образом генерируется при первом запуске устройства и остается неизменным далее.

MAC-адрес (Media Access Control) — управление доступом к среде, также Hardware Address Wi-Fi или Bluetooth. Позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу. MAC-адреса формируют на канальном уровне основу сетей, которую используют протоколы более высокого (сетевого) уровня.

UDID (Unique Device Identification Number) - уникальный идентификационный номер устройства с Apple iOS. Используется разработчиками приложений, для рассылки бета-версий программ, усовершенствования и тестирования полученного продукта, а также для защиты от копирования.

Позволяет отслеживать перемещения и профили пользователей [6].

TMSI (Temporary Mobile Subscriber Identity) — временный идентификатор мобильной станции GSM (мобильного телефона). Уникальным образом идентифицирует мобильную станцию (MS). Используется из соображений безопасности, для сокрытия других идентификаторов абонента, а именно, во избежание передачи IMSI через радиоэфир.

P-TMSI (Packet Temporary Mobile Station Identity) – временный идентификатор мобильной станции. Используется для предотвращения передачи в открытом доступе IMSI номера при использовании пакетных сервисов в сети оператора.

Идея цифрового сертификата владения состоит в создании базы данных, где будут храниться записи о связках: идентификация телефона – профиль в социальной сети. Для создания такого сертификата написано мобильное приложение. Оно определяет идентификацию телефона и просит пользователя авторизоваться в социальной сети (Facebook, VK). Эта авторизация как раз и нужна для получения ссылки на публичный профайл пользователя. Для авторизации используется oAuth [7], так что никакая информация о паролях в системе не присутствует по определению.

Использование подтверждения (подписи) в форме авторизации в социальной сети позволяет, во-первых, не создавать отдельной системы регистрации пользователей, а во-вторых, избежать хранения в системе персональных данных. Система хранит, например, ссылку на публичный профиль в Facebook, а имя пользователя (фотографию) может запрашивать для отображения через открытый API социальной сети. Авторизация в социальной сети выступает, в данном случае, как своеобразный сервис Captcha, подтверждающий факт существования пользователя [8].

III. ANDROID ID И IMEI

Это два базовых идентификатора, которые используются в данной системе.

IMEI (International Mobile Equipment Identity) - международный идентификатор мобильного оборудования. Это некоторое число, уникальное для каждого использующего его аппарата. Применяется в сотовых телефонах сетей GSM, WCDMA и IDEN, а также в некоторых спутниковых телефонах [9].

IMEI присваивается телефону во время изготовления на заводе. Он служит для идентификации устройства в сети, хранится в прошивке аппарата и не имеет постоянного отношения к абоненту. Телефонам, поддерживающим одновременную работу с двумя SIM-картами, присваивается два номера IMEI.

Как правило, IMEI указывается в четырёх местах:

1) в самом аппарате. В большинстве случаев его можно вывести на экран набором **#06#* на клавиатуре, но этот способ применим не ко всем устройствам. Например, если в iPhone, использующем сеть AT&T, отобразится номер MEID, а в iPhone, использующем сеть Verizon - пользователь услышит следующее: «Номер, который вы набрали, не существует»;

- под аккумуляторной батареей;
- на упаковке аппарата;
- в гарантийном талоне.

IMEI играет роль серийного номера аппарата и передаётся в эфир при авторизации в сети. Также IMEI используется для слежения за аппаратами и блокирования краденых телефонов на уровне оператора сотовой связи, что не позволяет в дальнейшем использовать такой аппарат в сети этого оператора, однако не мешает его использованию в других сетях. Опорная сеть GSM хранит IMEI в EIR (Equipment Identity Register — регистр идентификации оборудования). По сути, IMEI это аналог MAC-адреса. У операторов есть возможность отслеживать ворованные и иные серые аппараты по IMEI и блокировать доступ к сети, для чего и служит EIR. Данный регистр содержит перечень IMEI мобильных телефонов, доступ которым запрещён в сеть, или они находятся под наблюдением. Теоретически, все данные об украденных мобильных телефонах должны распространяться по EIR всех сетей в мире через некоторый корневой (центральный) EIR. Очевидно, тем не менее, что в ряде стран эта возможность не поддерживается. Данные в EIR не обновляются в режиме реального времени, что делает его применение ограниченным. В России EIR пока не используется.

IMEI (14 десятичных цифр плюс контрольная цифра) содержит информацию о происхождении, модели и серийном номере устройства. Первые 6 цифр составляют модель и место происхождения устройства, и известны как TAC (Type Approval Code). Остальная часть - это определяемый производителем серийный номер аппарата, с высчитанной по алгоритму Луна контрольной цифрой в конце [10].

Например, код IMEI - *35-209900-176148-1* и код IMEISV - *35-209900-176148-23*:

- Первые 6 цифр «35-2099» - TAC (Type Approval Code) - первые 2 цифры утвержденный код типового образца назначается сериям мобильных телефонов после тестирования. Это официально зарегистрированный код RBI. RBI всегда десятичен, то есть он меньше чем 0xA0, что позволяет легко отличать IMEI от MEID, начало которого равно или больше, чем 0xA0. «35» - код британского совета по согласованию телекоммуникаций (BABT). Далее «2099» - модель телефона Alcatel One Touch 332;

- FAC (Final Assembly Code) - это код окончательно собранного изделия. Добавляется для идентификации производителя. Код «00» - значит, что телефон был сделан во время переходного периода, когда FAC был упразднён (во время существования FAC, использовались следующие коды: 67 — США, 19 или 40 — Великобритания, 78 или 20 — Германия, 10 или 70 — Финляндия, 30 — Корея, 80 — Китай, 04 — Вьетнам);

- SNR (SerialNumber) - «176148» — серийный номер аппарата;

- CD (Check Digit) «1» — контрольное число;

IMEI нового стиля выглядит немного по-другому: 49-015420-323751 (Nokia 3110 classic) и имеют 8-значный TAC (49-015420).

Новый идентификатор подвижного оборудования MEID, работающий в CDMA сетях, использует тот же базовый формат, что и IMEI.

IMEI имеется не во всех телефонах. На данный момент он присутствует на всех GSM и UMTS мобильных телефонах Европы, Азии, Африки, Австралии и Америки. AT&T & T-Mobile являются набольшими операторами мобильной связи, которые используют GSM повсеместно с номерами IMEI. Но также и увеличивается количество региональных операторов, которые переходят на GSM, к ним относятся Wireless, Highland Cellular, Dobson Cellular. Телефоны компаний Verizon and Sprint обычно не имеют номеров IMEI, вместо них они используют номера MEID, если только они не используют сдвоенную модель для использования заграницей. Большинство предоплаченных и бесконтактных телефонов в Америке не имеют своих IMEI номеров, то же самое относится и к одноразовым телефонам в Европе, Азии и Африке.

Граждане Южно-Африканской Республики, согласно закону, должны сообщить о краже телефона своему оператору и полиции. Телефон будет занесен в черный список и заблокирован для всех операторов мобильной связи, чтобы предотвратить его использование в нелегальных целях. Возвращенный телефон можно убрать из черного списка, представив оператору доказательства того, что телефон возвращен владельцу.

В некоторых странах, например, в Латвии, Великобритании, Республике Беларусь изменение IMEI является уголовно наказуемым деянием. Имеется, также прецедент попытки уголовного преследования за изменение IMEI в России.

В режиме он-лайн проверить IMEI аппарата и получить информацию о нем можно, например, некоторых ресурсах [11].

IMEISV (International Mobile Terminal Identity и Software Version number) состоит из 16 цифр и обеспечивает уникальную идентификацию каждого мобильного телефона и соответствие версии программного обеспечения, инсталлированного в мобильный телефон, разрешенной оператором. От версии программного обеспечения зависят услуги, доступные для мобильного аппарата, а также способность выполнить речевое кодирование, и поэтому данный параметр весьма важен.

Производители постоянно совершенствуют методы защиты программного обеспечения аппарата от изменения IMEI [12]. В ряде современных аппаратов IMEI хранится в OTP (One-time programmable-однократно программируемой) зоне памяти и не может быть изменен программными средствами, но, не смотря на это, существуют способы смены IMEI.

Технические аспекты смены IMEI зависят от модели аппарата. В одних моделях (большинство старых телефонов и аппараты азиатско-китайского производства) смена IMEI производиться достаточно легко – достаточно специальной программы и кабеля телефон-компьютер. В других моделях для полной смены IMEI необходимо заменить на новые часть электронных компонентов телефона (микросхемы процессора, флэш-памяти, либо контроллера), после чего заново запрограммировать флэш-память аппарата. Некоторые модели допускают «неполную» смену IMEI, при которой модифицируют программное обеспечение телефона (устанавливают патч к прошивке) таким образом, чтобы оно передавало на базовую станцию нужный номер IMEI, а не тот, который запрограммирован в аппаратных средствах телефона. При «неполной» смене IMEI исходное значение IMEI будет восстановлено после обновления программного обеспечения телефона.

Android ID – это 64 битный номер, который случайным образом генерируется при первом запуске устройства и остается неизменным далее. У устройств с операционной системой более ранних версий, чем 2.2 (“Froyo”) он может не определяться.

Android ID является уникальным ID для каждого устройства. Он используется при скачивании приложений с сайтов Google Play, которым необходимо идентификация устройства (благодаря нему они знают, что это именно то устройство, которое использовалось при оплате за приложение). Android ID генерируется единожды при загрузке устройства. Android ID генератор реализован в ROM при загрузке, и таким образом каждое устройство, которое было перепрошито, получает уникальный ID. Посмотреть или поменять Android ID можно программным способом, например, существующими для этого приложениями.

IV. Создание сертификатов

Для этого служит мобильное приложение (рисунок 2).

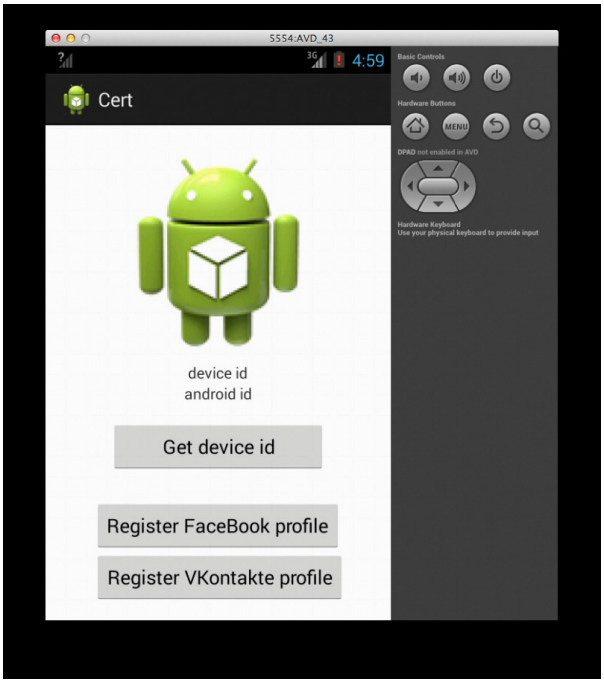

Рисунок 2. Создание сертификатов

Приложение определяет идентификацию телефона:

```
   import android.app.Activity;
   import android.os.Bundle;
   import
android.provider.Settings.Secure;
   import android.widget.Toast;

   public class ShowDeviceInfo extends
Activity {
         /** Called when the activity is
first created. */
   @Override
         public void onCreate(Bundle
savedInstanceState) {

super.onCreate(savedInstanceState);
   setContentView(R.layout.main);
               String deviceId =
Secure.getString(this.getContentResolver
(),
           Secure.ANDROID_ID);
         Toast.makeText(this, deviceId,
Toast.LENGTH_SHORT).show();
   }
   }
```

и предлагает авторизоваться в социальной сети (рисунок 3):

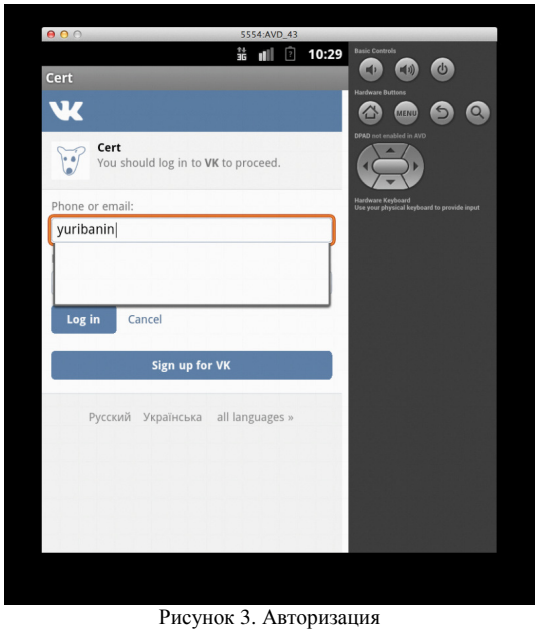

Рисунок 3. Авторизация

С помощью REST API полученные данные передаются серверному приложению, которое и записывает информацию в базу данных. Пользователь получает подтверждение (рисунок 4).

V. Веб-портал для системы сертификатов.

В настоящем разделе описывается переработанная веб-система для модели цифровых сертификатов.

Для реализации серверной части модели цифровых сертификатов был выбран язык программирования Java и среда разработки NetBeans.

В качестве сервера приложений был выбран Apache Tomcat (версия 7.0.41.0). Также есть возможность развертывания приложения на сервере GlassFish Server 4.0.

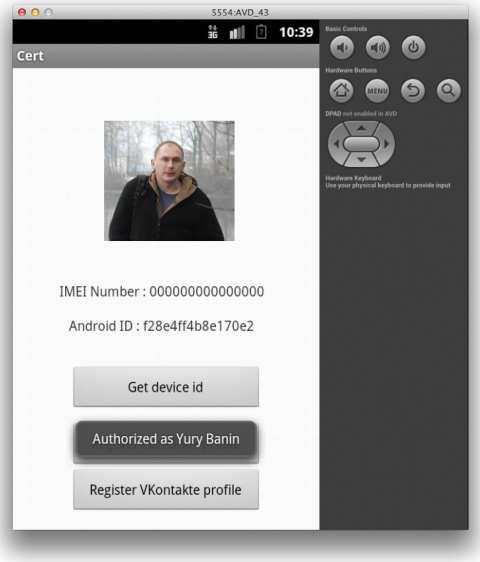

Рисунок 4. Подтверждение авторизации

Для возможности интеграции с различными базами данных было принято решение использовать библиотеку Hibernate (4.2.2).

Для функционирования приложения предполагалось разработать структуру модели сервлетов серверной части, управляющих базой данных и клиентским представлением сайта в рамках модели MVC.

В частности, было принято решение отделить клиентскую часть приложения, представленную JSP со статической html/css разметкой и динамическим взаимодействием web-интерфейса, основанного на javascript библиотеках и плагинах, от серверной части, включающей сервлеты, доступные с клиентской стороны посредством технологии Ajax. При этом для обмена данными предполагалось использовать формат JSON.

Для реализации кросс-браузерного интерфейса, с адаптивным дизайном для устройств с различным разрешением экрана (мобильные телефоны, планшеты), было решено использовать фреймворк Bootstrap 3.0. Этот фреймворк также реализует 12-колоночную структуру разметки.

Для представления данных из базы данных на web-странице и реализации удобного интерфейса поиска по ним был выбран jquery плагин DataTables 1.10, интегрированный с фреймворком Bootstrap.

Предполагалось реализовать интерфейс взаимодействия между базой данных и сервлетами модели серверной части посредством библиотек Hibernate, которые могли бы обрабатывать запросы, поступающие от плагина DataTables.

Программное API для получения информации из базы данных решено было реализовать в виде сервлета, которому на вход подается либо идентификатор, проверяемый в базе данных, либо url профиля в социальной сети. Ответ должен возвращаться в JSON формате, и содержать, в зависимости от запроса, найденную информацию в базе данных.

Система поддерживает создание QR-кодов для сертификатов. Это реализовано посредством Google сервиса Google Charts, который возвращает .png файл QR, содержащий url, передаваемый текстом в запросе. При переходе по этому url пользователь попадает на страницу web-интерфейса, отображающую запись из базы данных для устройства. Идея здесь состоит в том, чтобы физически представить сертификат в виде наклейки для телефона.

На рисунке 5 представлен интерфейс для поиска информации

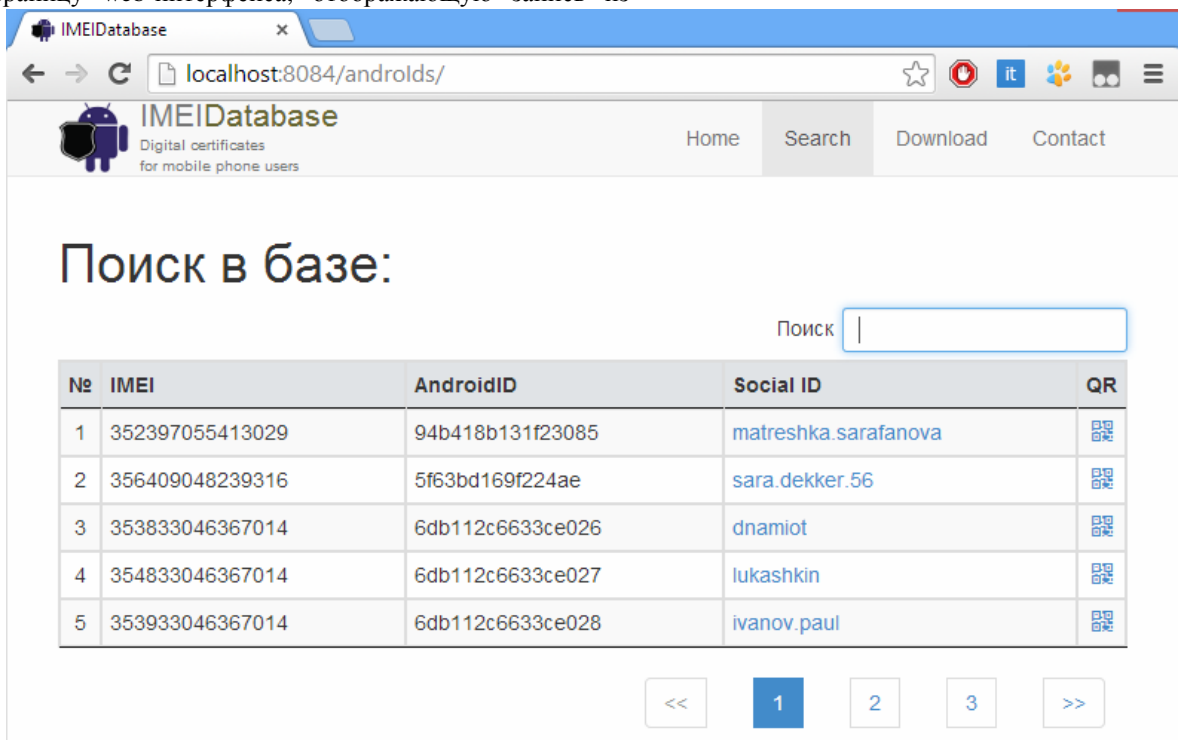

Рисунок 5. Поиск информации

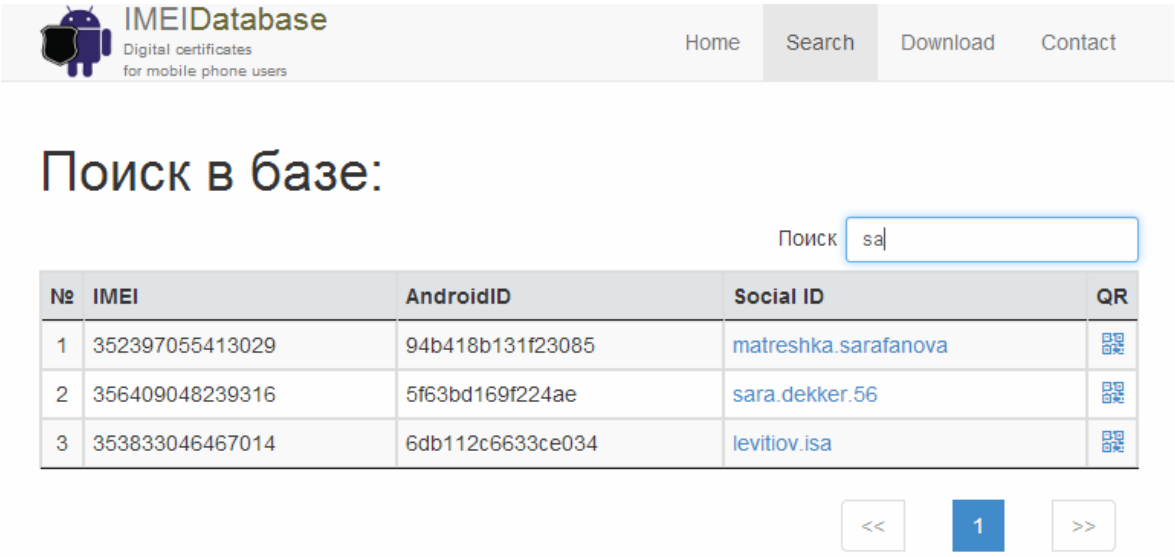

Рисунок 6. Полнотекстовый поиск

Здесь вставлен объект DataTables который имеет вид таблицы, содержащей записи, отображаемые из базы данных системы цифровых сертификатов. Информация по записям распределена в колонках таблицы:

IMEI – содержит IMEI устройства, при его наличии.

AndroidID – содержит AndroiID

Social ID – представлена ссылкой на профиль в Facebook, которым подписано идентифицированное устройство

QR – кнопка, с помощью которой можно распечатать QR-код, содержащий ссылку на сайт с записью для данного устройства.

Возможен полнотекстовый поиск (рисунок 6).

Благодаря интеграции DataTables с Bootstrap есть возможность адаптировать отображение таблицы к разрешению устройства, с которого пользователь получает доступ к сайту. Например, на рисунке 7 показано отображение той же таблицы поиска на мобильном устройстве.

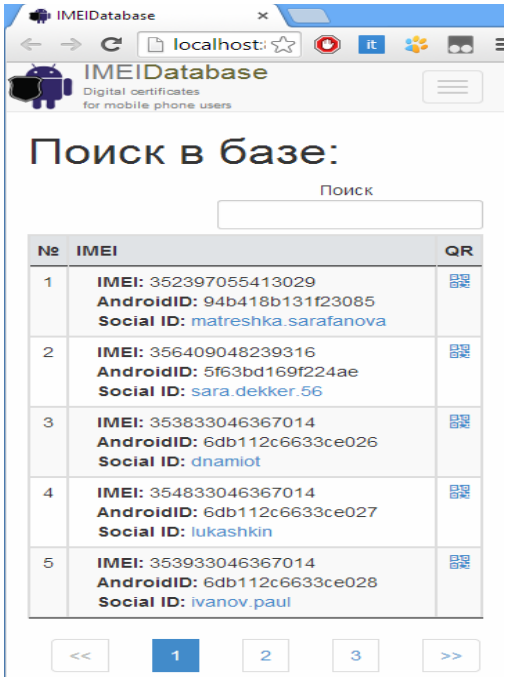

Рисунок 7. Поиск на мобильном устройстве

VI. API СИСТЕМЫ ЦИФРОВЫХ СЕРТИФИКАТОВ

Для получения информации из открытой базы данных системы цифровых сертификатов было реализовано программное API. Запрос направляется к сервлету *GetAndroidUserDetails*, при этом на входе сервлет принимает параметр для поиска. Возможные параметры:

imei – поиск по IMEI

andrid – поиск по AndroidId

socialId – поиск по уникальной составляющей url профиля социальной сети

all – полнотекстовый поиск по трем выше перечисленным полям

Пример запроса:

```
GetAndroidUserDetails?imei=353833046367014
```

В ответ на запрос возвращается строка, содержащая объект в JSON формате:

```
{"res": 1,
"obj": {
        "DT_RowId": 1,
        "createdOn": "18.05.2014",
        "IMEI": "352397055413029",
        "AndroidID":
"94b418b131f23085",
        "authenticatorsList": [
{
                "DT_RowId": 1,
                "createdOn":
"18.05.2014",
                "socialIdUrl":
"http://www.facebook.com/matreshka.saraf
anova",
                "userName":
"matreshka.sarafanova",
                "netAuthentication":
"facebook" }
  ]
      }
  }
```

Здесь свойство res – содержит количество возвращенных записей, оно больше 1 для запросов с полнотекстовым поиском, при этом возвращается массив объектов, соответствующих записям в базе данных.

Поскольку в разное время, одно и тоже мобильное устройство может быть подписано несколькими профилями одной социально сети, либо одновременно профилями разных социальных сетей – объект содержит список профилей *authenticatorsList*, которыми подписано устройство. Этот список также представляет собой массив объектов.

API – это важный элемент данной экосистемы. Идея состоит в том, что авторизация с помощью аккаунта в социальных сетях в настоящее время используется во многих мобильных приложениях. Следовательно, после авторизации пользователя в приложении можно получить ссылку на его профайл. С помощью API сертификатов, приложение может определить идентификатор телефона в базе данных и сравнить его с реальным. Таким образом, можно организовать дополнительную проверку – а со своего ли телефона авторизуется данный пользователь? Это может быть использовано, например, в финансовых системах или приложениях типа Geo Messages [13].

БИБЛИОГРАФИЯ

[1] Гурьев Д.Е., Намиот Д.Е., Шнепс М.А. О телекоммуникационных сервисах //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 4. – С. 13-17.

[2] Намиот Д. Е., Колосова А. И. Об определении владельцев мобильного телефона //International Journal of Open Information Technologies. – 2013. – Т. 1. – №. 8. – С. 26-31.

[3] Колосова А., Намиот Д. Цифровые сертификаты для владельцев мобильных телефонов //International Journal of Open Information Technologies. – 2013. – Т. 1. – №. 4. – С. 7-11.

[4] Namiot D., Sneps-Sneppe M. On Database for Mobile Phones Ownership. Proceedings of the 15th Conference of Open Innovations Association FRUCT, Saint-Petersburg, Russia. Publisher: ITMO university publisher house, ISSN 2305-7254, ISBN 978-5-7577-0463-0

[5] Гончаров М. С., Шатохин П. А. Разработка компьютеризированной подсистемы учета и анализа преступлений, связанных с кражей мобильных телефонов. – 2010. http://ea.donntu.edu.ua/handle/123456789/9182

[6] Hoog A., Strzempka K. iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices. – Elsevier, 2011

[7] Hardt D. The OAuth 2.0 authorization framework. – 2012.

[8] Namiot, Dmitry, and Manfred Sneps-Sneppe. "Customized check-in procedures." Smart Spaces and Next Generation Wired/Wireless Networking. Springer Berlin Heidelberg, 2011. 160-164.

[9] Enck W., OcteauD., McDaniel P.,Chaudhuri S. A Study of Android Application Security //USENIX Security Symposium. – 2011

[10] Майер Р. Android 2. Программирование приложений для планшетных компьютеров и смартфонов. – Litres, 2013.

[11] IMEI http://xsms.com.ua/phone/imei/ Retrieved: Jul, 2014

[12] Нестеров В., Пушкарев О. Вопросы безопасной передачи данных при использовании GSM канала //Беспроводные технологии. – 2008. – №. 13

[13] Namiot, D., & Sneps-Sneppe, M. (2013, April). Peer to Peer Location Sharing. In ICDT 2013, The Eighth International Conference on Digital Telecommunications (pp. 20-25).

On search for the owner of a mobile phone

Banin Y.V., Kizilov D.M , Namiot D.E.

Abstract— **This paper is devoted to the development of digital certificates for mobile devices. The certificate is an object that confirms ownership of the mobile device (phone). The certificate contains the identification of the device (e.g., IMEI) and the identification of the owner in some social network. A user's account on the social network acts as the holder's signature. Certificates are created by a special mobile application. And a special web portal with REST API could be used for the search. The latest development of this model is the subject of this paper.**

Keywords— **certificate, IMEI, social network.**