Об определении владельцев мобильного телефона.

Намиот Д.Е., Колосова А.И.

***Аннотация*—Данная работа посвящена задаче подтверждения факта владения мобильным телефоном. В статье рассматривается модель цифровых сертификатов для мобильных устройств. В этой модели каждый мобильный пользователь может создать уникальную цифровую метку для своего телефона и подписать ее с помощью ссылки на свой профиль в социальной сети. После этого появляется возможность искать данные по накопленной базе цифровых сертификатов. Поиск может осуществляться как по идентификации мобильного телефона, так и по атрибутам профиля социальной сети или сетей.**

***Ключевые слова*—сертификат, IMEI, Android.**

I. Введение

В работе рассматривается модель цифровых сертификатов для мобильных устройств, впервые описанная авторами в работе [1].

Проблема хищений мобильных телефонов остро стоит во всем мире. Как правило, у каждого владельца мобильного телефона хранится достаточное количество важной информации, которую может быть тяжело и которая не предназначена для сторонних пользователей. Как-то – список контактов, фотографии и др., в зависимости от сложности устройства. Поэтому нахождение утерянных аппаратов, равно как и противодействие их использованию, является важной задачей.

В данной работе рассматриваются мобильные устройства с операционной системой Android – смартфоны и др. Это, в большей степени, практический выбор, обусловленный удобством программирования. Рассматриваемая модель может быть применена и к другим мобильным операционным системам.

У всех мобильных аппаратов имеются различные идентификационные номера. Именно эти уникальные идентификаторы и могут быть использованы для нахождения утерянных телефонов, мониторинга установок некоего приложения, генерации технических средств защиты авторских прав (DRM – digital rights management). Например, мобильные операторы, при наличии определенного оборудования могут полностью или частично прекратить обслуживать украденный телефон, перенаправлять SMS-сообщения с него на другой телефон. Или отследить его место нахождения по GPS [2]. В России подобная практика не так распространена, как в некоторых других странах, однако и у нас есть случаи нахождения украденных телефонов по IMEI номеру.

Предлагаемая модель рассматривает два основных аспекта:

-разработка методики идентификации мобильных аппаратов;

-разработка системы регистрации идентификационных номеров, а также принципов работы с регистрационной базой.

II. Основные существующие методы идентификации мобильных телефонов

A. IMEI

IMEI (International Mobile Equipment Identity) - число (обычно 15-разрядное в десятичном представлении), уникальное для каждого использующего его аппарата. Применяется в сотовых телефонах сетей GSM, WCDMA и IDEN а также в некоторых спутниковых телефонах [3].

IMEI присваивается телефону во время изготовления на заводе. Он служит для идентификации устройства в сети и хранится в прошивке аппарата. Как правило, IMEI указывается в четырёх местах: в самом аппарате (в большинстве случаев его можно вывести на экран набором *#06# на клавиатуре), под аккумуляторной батареей, на упаковке и 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.

В отличие от ESN и MEID, используемых в CDMA и прочих сетях, IMEI используется только для идентификации устройства и не имеет постоянного отношения к абоненту. Вместо него используется номер IMSI, хранящийся на SIM-карте, которую можно вставить в практически любой другой аппарат. Однако существуют специальные системы, позволяющие

Статья получена 5 сентября 2013.

Намиот Дмитрий Евгеньевич – кандидат физико-математических наук, старший научный сотрудник лаборатории Открытых Информационных Технологий факультета Вычислительной Математики и Кибернетики Московского государственного университета им. Ломоносова.

Колосова Алена Игоревна – выпускница факультета Вычислительной Математики и Кибернетики Московского государственного университета им. Ломоносова.

одному телефону использовать только одну определённую SIM-карту.

Модель и происхождение телефона описываются первыми 8 цифрами IMEI (так называемый TAC). Оставшаяся часть — серийный номер с контрольным числом в конце. Телефонам, поддерживающим одновременную работу с двумя SIM-картами, присваивается два номера IMEI [4].

Производители постоянно совершенствуют методы защиты программного обеспечения аппарата от изменения IMEI. В современных аппаратах IMEI хранится в однократно программируемой зоне памяти и не может быть изменен программными средствами [5].

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 [6].

B. MEID

MEID (Mobile Equipment IDentifier) – глобальный уникальный идентификатор подвижного оборудования, работающий в сетях CDMA, использует тот же базовый формат, что и IMEI [7].

C. IMSI

MSI (International Mobile Subscriber Identity) - международный идентификатор мобильного абонента (индивидуальный номер абонента), ассоциированный с каждым пользователем мобильной связи стандарта GSM, UMTS или CDMA. При регистрации в сети аппарат абонента передаёт IMSI, по которому происходит его идентификация. Во избежание перехвата, этот номер посылается через сеть настолько редко, насколько это возможно — в тех случаях, когда это возможно, вместо него посылается случайно сгенерированный TMSI [8].

В системе GSM идентификатор содержится на SIM-карте в элементарном файле (EF), имеющем идентификатор 6F07. Формат хранения IMSI на SIM-карте описан ETSI в спецификации GSM 11.11. Кроме того, IMSI используется любой мобильной сетью, соединенной с другими сетями (в частности с CDMA или EVDO) таким же образом, как и в GSM сетях. Этот номер связан либо непосредственно с телефоном, либо с R-UIM картой (аналогом SIM карты GSM в системе CDMA) [9].

Длина IMSI, как правило, составляет 15 цифр, но может быть короче. Например: 250-07-XXXXXXXXXX. Первые три цифры это MCC (Mobile Country Code, мобильный код страны). В примере 250 - Россия. За ним следует MNC (Mobile Network Code, код мобильной сети). 07 из примера - СМАРТС. Код мобильной сети может содержать две цифры по европейскому стандарту или три по североамериканскому. Все последующие цифры — непосредственно идентификатор пользователя MSIN (Mobile Subscriber Identification Number) [10].

D. Serial number

Серийный номер можно определить у устройств, не обладающих сервисом телефонии начиная с операционной системы Android 2.3 (“Gingerbread”) и у некоторых телефонов [11].

E. 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 [11].

F. Mac-Address

MAC-адрес (от англ. Media Access Control — управление доступом к среде, также Hardware Address) — это уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей. Большинство сетевых протоколов канального уровня используют одно из трёх пространств MAC-адресов, управляемых IEEE: MAC-48, EUI-48 и EUI-64. Адреса в каждом из пространств теоретически должны быть глобально уникальными. Не все протоколы используют MAC-адреса, и не все протоколы, использующие MAC-адреса, нуждаются в подобной уникальности этих адресов [12].

В широковещательных сетях (таких, как сети на основе Ethernet) MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу. Таким образом, MAC-адреса формируют основу сетей на канальном уровне, которую используют протоколы более высокого (сетевого) уровня. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы (например, ARP и RARP в сетях IPv4 и NDP в сетях на основе IPv6) [12].

Адреса вроде MAC-48 наиболее распространены; они используются в таких технологиях, как Ethernet, Token ring, FDDI, WiMAX и др. Они состоят из 48 бит, таким образом, адресное пространство MAC-48 насчитывает 248 (или 281 474 976 710 656) адресов. Согласно подсчётам IEEE, этого запаса адресов хватит по меньшей мере до 2100 года [12].

EUI-48 от MAC-48 отличается лишь семантически: в то время как MAC-48 используется для сетевого оборудования, EUI-48 применяется для других типов аппаратного и программного обеспечения.

Идентификаторы EUI-64 состоят из 64 бит и используются в FireWire, а также в IPv6 в качестве младших 64 бит сетевого адреса узла.

Можно также получить MAC-адрес Wi-Fi или Bluetooth оборудования устройства, однако не рекомендуется использовать его в качестве уникального идентификационного номера, так как не все мобильные устройства имеют Wi-Fi. Если Wi-Fi модуль есть, он должен быть обязательно включен, иначе MAC-адрес не определится. Кроме того, MAC-адрес устройства можно изменить программным путем [12].

III. Модель цифровых сертификатов

Идея цифровых сертификатов состоит в создании открытой базы данных, где каждый владелец мобильного телефона мог бы сохранить идентифицирующие признаки своего аппарата, заверив (подписав) их ссылкой на собственный профиль в социальной сети. Идея использования ссылки на профайл состоит в том, что в этом случае база данных избегает проблем, связанных с хранением персональной информации. В таком случае ее просто нет. Вся персональная информация остается в социальной сети. В базе данных сертификатов хранится только открытая ссылка на соответствующий профиль.

Соответственно этому, реализация такой модели должна включать в себя мобильное приложение для создания сертификата, базу данных для хранения сертификатов и интерфейс к базе данных для поиска. Важный момент, что такой интерфейс должен включать в себя и программный API.

Владелец телефонного аппарата может бесплатно, по собственной инициативе, добавить сертификат для своего телефона в общую базу. База сертификатов публично доступна. Следовательно, сильно упрощается процесс проверки владельца телефона. А это, в свою очередь, сможет остановить какой-то значимый процент мобильных абонентов от пользования телефоном, который попал к ним не совсем законным способом. Кроме того, такая база может оказаться подспорьем для официального следствия.

Таким образом, общая идея данной модели состоит не в отслеживании потерянного (похищенного) телефона, а во введении возможности проверки владельца телефона в момент использования телефона. При этом, в первую очередь, имеется в виду использование смартфонов в сети Интернет. Самая простая модель использования: приложение во время авторизации пользователя в социальной сети может проверить, кому принадлежит данный телефон.

Естественно, что ничто не препятствует и операторам связи использовать ту же самую открытую базу данных для проверки владельцев в момент совершения звонков и отправки SMS.

В данной работе качестве уникального идентификатора используются IMEI номер и Android ID. Это позволяет увеличить надежность идентификация Android устройства. На практике, не у всех устройств определяются оба эти номера, но хотя бы один из них определяется практически всегда. Мобильные операторы для взаимодействия с телефоном используют IMEI номер.

Мобильное приложение разработано на *Java*, в среде *Eclipse*. Так как именно для этой среды существует официальный плагин *Android Developer Tools* (ADT), который предоставляет профессиональную среду разработки Android-приложений. Для определения IMEI номера и Android ID воспользовались классами *TelephonyManager* и *Settings*. Для определения ссылки на страницу пользователя в Facebook воспользовались некоторыми функциями Facebook SDK. В результате, при нажатии на кнопку регистрации, пользователь перенаправляется в окно авторизации в Facebook. Иными словами, используется стандартная схема авторизации с помощью Facebook в сторонних приложениях.

Взаимодействие с удаленной базой данных осуществлено на PHP с использованием JSON, в отдельном классе *JSONParser*, с помощью функций из класса *org.apache.http*.

В качестве удаленной базы данных используется MySQL. Основная таблица содержит 4 столбца: ID, IMEI, AndroidID и Link. Взаимодействие с ней сделано таким образом, чтобы было невозможно добавить строку с каким-то определенным IMEI-номером или Android ID более одного раза.

Записи могут только добавляться в базу данных, операций удаления и редактирования нет. Таким образом, база данных представляет собой журнал регистраций, который позволяет проследить всю историю владения.

Для того, чтобы информировать пользователя об успешной отправке запроса с телефона в базу данных, и успешной авторизации в Facebook, добавлено соответствующее всплывающее сообщение (*Toast*) и функция добавления фото из профайла пользователя с его личной страницы. На рисунке 1 представлен общий вид после авторизации, получившегося в итоге приложения на Android-эмуляторе. А на рисунке 2 – вид окна авторизации в Facebook.

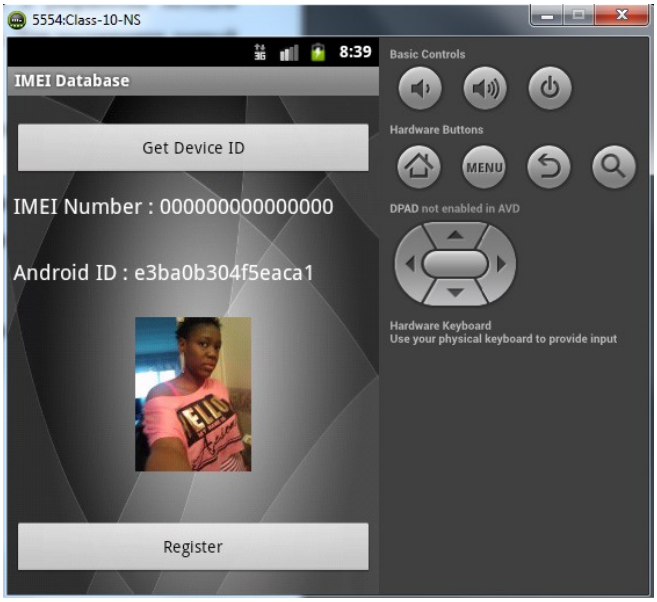

Рис. 1. Приложение после авторизации.

Для того чтобы просматривать удаленную базу данных приложения авторами был сделан сайт *http://fr30706.tw1.ru/*.

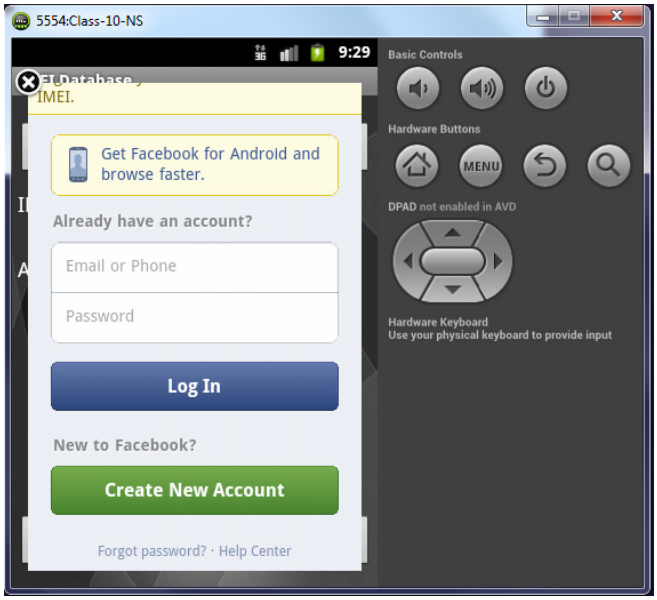

Рис. 2. Окно авторизации в Facebook.

На рисунке 3 представлен вид главной страницы сайта. На этом сайте по вкладке «Search» можно перейти на страницу с функциональностью поиска по получившейся IMEI-базе данных. Взаимодействие сайта с базой данных реализовано на PHP. Искать записи в базе данных можно по любому из трех полей: по IMEI номеру, по Android ID, или же по ссылке на личную страницу в Facebook. На рисунке 4 представлен вид страницы поиска.

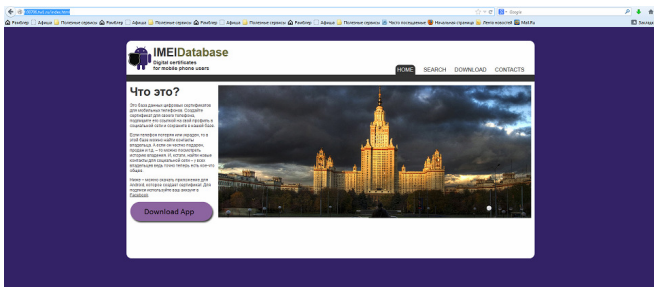

Рис. 3. Главная страница сайта проекта.

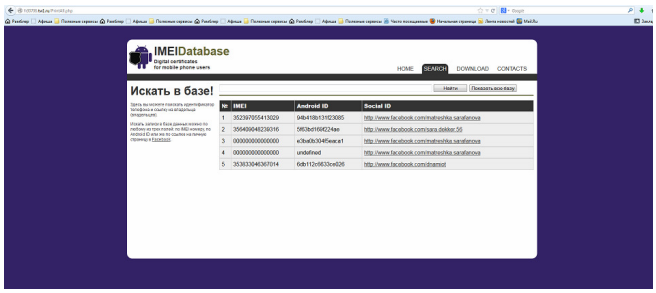

Рис. 4. Страница поиска по базе данных.

Также на этом сайте можно скачать последнюю версию приложения для аппаратов с операционной системой Android.

Дизайн сайта разработан с поддержкой технологии Responsive Design. Это обеспечивает хорошее отображение сайта, а также удобство работы, как на стандартных компьютерных мониторах, так и на маленьких экранах смартфонов. Таким образом, у сайта реализованы 2 разные разметки.

На рисунке 5 представлен вид страницы поиска на экране смартфона. А на рисунке 6 – сравнительный вид страницы «DOWNLOAD» на экране монитора и на Android-эмуляторе.

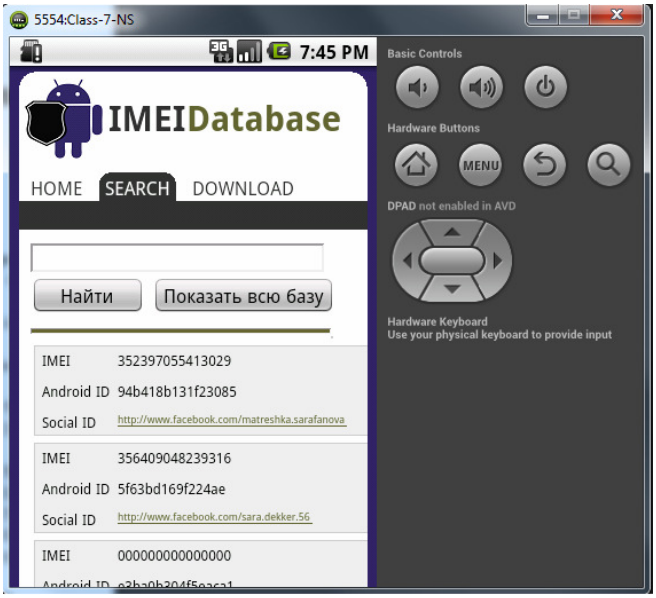

Рис. 5. Страница поиска на экране смартфона.

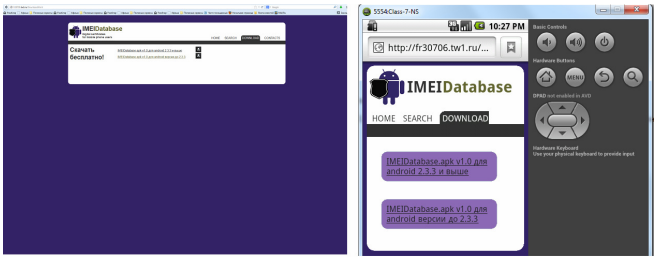

Рис. 6. Страница «DOWNLOAD» на разных экранах.

IV. Дальнейшие разработки

Можно указать следующие направления развития проекта. Во-первых, можно предложить пользователям физическое изготовление сертификатов. Это может быть реализовано в виде печати наклейки с QR-кодом, которая содержит URL для страницы с результатами поиска данного сертификата в базе данных. Получается некоторая аналогия контекстно-зависимого QR-кода [13].

Другим возможным направлением работы является развитие программного API к базе данных. В этом случае, искать подтверждения владения можно будет программно. Например, приложения типа Geo Messages [14] или WATN [15,16] смогут также проверять законность владения телефоном отправителя сообщений.

Проверка факта владения телефоном может оказаться полезной, например, для финансовых приложений. Рассмотрим, например, следующий модельный пример авторизации приложения в Facebook. В данном случае пример относится к веб-приложениям, но схема для мобильных приложений будут такой же.

```
FB.login(function(response) {
   if (response.authResponse) {
     console.log('Welcome!  Fetching
your information.... ');
     FB.api('/me', function(response) {
       console.log('Good to see you, ' +
response.name + '.');

// здесь может быть добавлен код для
// проверки владельца
// Это действительно response.name ?

     });
   } else {
     console.log('User cancelled login
or did not fully authorize.');
   }
 });
```

Подобного рода авторизация с дополнительной проверкой может служить хорошим дополнением к модифицированным системам отметок о присутствии [17] или приложениям для рассылки локальных сообщений [18]. В обоих случаях добавляется новый уровень проверки мобильных пользователей.

Идея здесь заключается в том, что авторизация с помощью социальных сетей становится (стала) одним из самых полярных инструментов для авторизации пользователей в сторонних приложениях. Тот же самый Facebook Login, например, может использоваться в массе приложений и не связанных непосредственно с самой социальной сетью Facebook. Сторонние мобильные приложения эксплуатируют тот факт, что у произвольного пользователя почти наверняка уже есть регистрация в данной социальной сети. А проверка факта владения как раз и привязана к этой самой сети. Мобильное приложение, авторизуя пользователя с помощью Facebook, сможет проверить и факт обладания данным пользователем (владельцем аккаунта) телефоном, с которого проходит авторизация.

Развитие проекта входит в число приоритетных работ лаборатории ОИТ [19]. Собственно говоря, возврат к этой теме после работы [1] как раз и продиктован желанием очертить все возможности проекта (в том числе и не вошедшие в оригинальную работу) и, возможно, привлечь к нему внимание заинтересованных лиц.

V. Заключение

Разработана и реализована модель цифровых сертификатов для владельцев мобильных устройств. С помощью этой системы пользователь может создать сертификат для своего мобильного телефона, подписать его ссылкой на свой профиль в социальной сети и сохранить в базе данных.

Если телефон потерян или украден, то в этой базе можно найти контакты владельца. Программный API для поиска позволит встраивать процедуру проверки в мобильные сервисы. А для случая корректной смены владельца, сервис позволяет создать подобие некоторой специализированной социальной сети – все владельцы данного устройства.

Библиография

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

[2] Sonia C. V., Aswatha A. R. SAPt: A Stolen Android Phone Tracking Application.

[3] Gosden, P., Allen, A., McDonald, D., & Montemurro, M. (2013). A Uniform Resource Name Namespace for the GSM Association (GSMA) and the International Mobile station Equipment Identity (IMEI).

[4] GSM Association Non Confidential Official Document IMEI Allocation and Approval Guidelines Version 6.0 (27th July 2011) (http://www.gsma.com/newsroom/wp-content/uploads/2012/03/ts0660tacallocationprocessapproved.pdf).

[5] В. Шалькевич, А. Макаревич «Противодействие теневому обороту мобильных телефонов уголовно правовыми мерами», Журнал «Законность и правопорядок», No 3(7)/2008, стр. 36-40.

[6] http://www.legislation.gov.uk/ukpga/2002/31/section/1.

[7] Atarius R. A Uniform Resource Name Namespace for the Device Identity and the Mobile Equipment Identity (MEID). – 2013.

[8] Matsumoto, S., & Sakurai, K. (2013, January). A proposal for the privacy leakage verification tool for Android application developers. In Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication (p. 54). ACM.

[9] Fred Gaechter "Chairman of IMSI Oversight Committee" (IOC)(GSMNA Doc 036/02) (http://www.ifast.org/files/IFAST22_015_GSMNALetter.pdf).

[10] Abdalla, I., & Venkatesan, S. (2013, April). Scalable addressing of M2M terminals in 4G cellular wireless networks. In Wireless Telecommunications Symposium (WTS), 2013 (pp. 1-6). IEEE.

[11] http://developer.samsung.com/android/technical-docs/How-to-retrieve-the-Device-Unique-ID-from-android-device.

[12] IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture (IEEE Std 802®-2001 (R2007)(Revision of IEEE Std 802-1990).

[13] Namiot, D., Sneps-Sneppe, M., & Skokov, O. (2013). Context-aware QR-codes. arXiv preprint arXiv:1307.7597.

[14] Namiot, D. “Geo messages”, In Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on (pp. 14-19). IEEE. DOI: 10.1109/ICUMT.2010.5676665

[15] Dmitry Namiot and Manfred Sneps-Sneppe. "Where Are They Now–Safe Location Sharing." Internet of Things, Smart Spaces, and Next Generation Networking. Springer Berlin Heidelberg, 2012. 63-74. DOI: 10.1007/978-3-642-32686-8_6

[16] Alla Qoussini, Yousef Daradkeh and Dmitry Namiot. "Location Sharing Without Central Server", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3, March 2013, pp. 138-144

[17] Dmitry Namiot and Manfred Sneps-Sneppe. "Customized check-in procedures." Smart Spaces and Next Generation Wired/Wireless Networking. Springer Berlin Heidelberg, 2011. 160-164. DOI: 10.1007/978-3-642-22875-9_14

[18] Dmitry Namiot and Manfred Sneps-Sneppe. "Local messages for smartphones". Future Internet Communications (CFIC), 2013 Conference on (pp. 1-6). IEEE. DOI: 10.1109/CFIC.2013.6566322.

[19] Намиот, Д., & Сухомлин, В. (2013). О проектах лаборатории ОИТ. International Journal of Open Information Technologies, 1(5), 18-21.

Checking of mobile phone owner

D.Namiot, A.Kolosova

***Abstract* — this paper is devoted to the problem of confirmation of the ownership of a mobile phone. In this paper we present a model of digital certificates to mobile devices. In this model, each mobile user can create a unique numeric label for own phone and sign it with a link to own profile on the social network. After that it is possible to search the data stored on the digital certificates data base. We can search this database by phone's ID, as well as by owner's attributes in social networks.**

***Keywords*—certificate, IMEI, Android.**