

УДК 654.072.5

Проблемные вопросы внедрения национального центрального реестра идентификации мобильного оборудования

Никитин Д. А.

Постановка проблемы: центральный реестр идентификации мобильного оборудования внедрён уже в ряде стран, в том числе в нескольких странах бывшего СССР. В настоящее время проекты по выработке требований, особенностей реализации и по запуску таких систем идут в России, Узбекистане, Таджикистане и других странах. Такие проекты являются сложными (не только в упомянутых странах) и, как правило, длительными. При этом публикаций, всесторонне рассматривающих применение таких систем, на русском языке практически нет. **Целью работы** является рассмотрение проблемных вопросов, с которыми могут столкнуться все участники проекта при внедрении в стране центрального реестра идентификации оборудования. **Используемые методы:** системный анализ информации, полученной в ходе участия в разработке требований, как к национальным, так и к реестрам идентификации оборудования, так и к реестрам идентификации оборудования в сети отдельного сотового оператора, в проработке сценариев их функционирования в различных условиях, а также информации, полученной при подготовке и реализации таких проектов. **Новизна:** приводится структурная схема национального центрального реестра идентификации мобильного оборудования. Выделены наиболее существенные проблемные вопросы, возникающие при внедрении реестра, которые классифицированы по типам: концептуальные, организационные (в том числе юридические), экономические и технические. Для концептуальных проблемных вопросов описано, как их решение влияет на структуру и принципы функционирования реестра, а также на сам процесс реализации проекта. Для организационных, экономических и технических проблемных вопросов предложены варианты их решения. **Практическая значимость:** представленный анализ поможет заказчику подобной системы заранее учесть все самые сложные моменты и выработать непротиворечивое техническое задание, а также запланировать адекватные сроки исполнения проекта. Для сотовых операторов статья интересна тем, что содержит требования к их сетям, которые возникают при внедрении в стране центрального реестра идентификации мобильного оборудования.

Ключевые слова: центральный реестр идентификации оборудования, Central EIR, CEIR, Equipment identity registry, EIR, IMEI, IMSI, MSISDN, GSMA, IMEI DB, дубликаты IMEI, CheckIMEI, IMEI check, блокировка услуг связи, регистрация в сотовой сети.

Введение

Центральный реестр идентификации мобильного оборудования (Central Equipment Identity Register) предназначен для борьбы с такими явлениями как кражи мобильных устройств, неконтролируемый/незаконный ввоз мобильных устройств, использование контрафактных мобильных устройств, уход от налогообложения при импорте мобильных устройств. Основным механизмом борьбы является полная или частичная блокировка услуг связи при использовании

Библиографическая ссылка на статью:

Никитин Д. А. Проблемные вопросы внедрения национального центрального реестра идентификации мобильного оборудования // Системы управления, связи и безопасности. 2019. № 2. С. 28-53. DOI: 10.24411/2410-9916-2019-10202

Reference for citation:

Nikitin D. A. Significant issues of introduction of a central register for mobile equipment identification in a country. *Systems of Control, Communication and Security*, 2019, no. 2, pp. 28-53. DOI: 10.24411/2410-9916-2019-10202 (in Russian).

мобильного устройства, которое по той или иной причине считается нелегальным. Препятствовать использованию краденных или контрафактных устройств может каждый оператор сотовой связи в отдельности, используя узел EIR (Equipment Identity Register) в своей сети. Но тогда для него возникает риск оттока абонентов в другие сети, где такая работа не проводится. Поэтому блокировка услуг связи начинает применяться, как правило, тогда, когда появляется центральный реестр, интегрированный со всеми или почти всеми мобильными сетями в стране. Дополнительно, с точки зрения государства, внедрение подобной системы даёт следующее: во-первых, появляется возможность введения новых налогов или пошлин, во-вторых, для спецслужб и правоохранительных органов появляется возможность точечной блокировки работы мобильного устройства во всех сетях страны без использования специального оборудования.

Несмотря на такой перечень предполагаемых положительных эффектов, центральные реестры, которые успешно решают поставленные задачи, внедрены в небольшом количестве стран. При этом реализация таких внедрений, как правило, имеет существенные различия, а введение в эксплуатацию характеризуется длительными сроками подготовительных и пуско-наладочных работ. Например, в Казахстане обязательную регистрацию устройств в единой базе идентификационных кодов планировали запустить с 1 июля 2017 года [1], но по факту это пришлось перенести на 2019 год [2].

Прежде всего, центральные реестры эффективно применяются для снижения уровня краж мобильных устройств и получения дополнительной налоговой прибыли [3, 4], а вот остальные его возможности реализуются не всегда в полной мере. Так происходит, в том числе, и из-за ряда проблемных аспектов реализации такого проекта. Возникающие проблемы можно классифицировать следующим образом:

- 1) концептуальные;
- 2) организационные (в том числе юридические);
- 3) экономические;
- 4) технические.

Сначала введём основные понятия и дадим краткую характеристику применения центрального реестра идентификации мобильного оборудования, а затем подробно рассмотрим каждую группу проблем.

GSM (Global System for Mobile Communications) – глобальный стандарт цифровой мобильной сотовой связи с разделением каналов по времени и частоте.

CDMA (Code Division Multiple Access) – технология радиосвязи, в которой используется множественный доступ с кодовым разделением каналов.

GSMA (GSM Association, Ассоциация GSM) – международная ассоциация, объединяющая лицензированных сотовых операторов, работающих в стандарте GSM (полные члены), и производителей различного оборудования, связанного с GSM-сетями (операторского, абонентского и др.) – ассоциированные члены. Занимается развитием экосистемы GSM, в том числе разработкой стандартов.

SIM-карта (Subscriber Identification Module) – модуль идентификации абонента, применяемый в мобильной связи стандарта GSM.

IMEI (International Mobile Equipment Identity) – идентификатор мобильного оборудования, уникальный для каждого устройства [5]. Принципы выделения IMEI определены Ассоциацией GSM [6, 7]. Согласно им IMEI должен быть уникален для каждого устройства, и менять его не допускается. По сути, этот номер назначается каждому радиомодулю, работающему в сотовых сетях стандартов 2G/3G/4G. Например, если устройство может работать одновременно с двумя SIM-картами, то оно имеет два идентификатора IMEI.

TAC (Type Allocation Code) – первые 8 цифр идентификатора IMEI, из которых первые 2 цифры указывают уполномоченный орган, который выделил данный TAC-код, а следующие 6 цифр – уникальный идентификатор модели устройства. Когда TAC-код выделен и выдан производителю, он должен использовать его для формирования IMEI устройств только одной модели. Однако иногда это правило нарушается.

EIR (Equipment Identification Register, реестр идентификации оборудования) – узел сотовой сети оператора, к которому совершает запрос коммутационное оборудование оператора, как минимум при каждой регистрации и перерегистрации каждого мобильного устройства в сети. Коммутатор передаёт IMEI устройства и ждёт от EIR ответ, регистрировать это устройство в сети или нет. Для сокращённой записи данного запроса введём обозначение – CheckIMEI. Запрос CheckIMEI может выполняться и чаще, например, при каждом звонке, либо не реже, чем через 4 ч. Это зависит от возможностей и настройки коммутационного оборудования.

CEIR (Central EIR, центральный реестр идентификации оборудования) – база данных, интегрированная с узлами EIR операторов одной страны, и содержащая списки IMEI, которые синхронизируются на все EIR. Обычно системой CEIR управляет регулятор услуг связи или уполномоченная им организация.

IMEI DB (IMEI Database) – база данных, аналогичная CEIR, но принадлежащая Ассоциации GSM. CEIR любой страны или EIR любого оператора может интегрироваться с IMEI DB, чтобы обмениваться чёрным списком [8]. Так, появляется возможность блокировать регистрацию устройств, украденных в другой стране.

IMSI (International Mobile Subscriber Identity) – международный идентификатор мобильного абонента (индивидуальный номер абонента), ассоциированный с каждым пользователем мобильной связи [5]. Содержится в SIM-карте.

MSISDN (Mobile Station Integrated Services Digital Number) – в мобильной связи сопоставленный SIM-карте телефонный номер абонента. Используется для идентификации абонента при предоставлении большинства услуг [5]. На SIM-карте не содержится.

Чёрные, белые и серые списки – списки, на основании которых EIR формирует ответ коммутационному оборудованию на запрос CheckIMEI. В классическом варианте это списки IMEI, но ниже будет показано, что для реализации необходимой функциональности может потребоваться и поддержка списков IMSI или MSISDN, а также списков кортежей этих идентификаторов (IMEI-

IMSI, IMEI-IMSI-MSISDN, либо IMSI-MSISDN). На запрос CheckIMEI система EIR может дать один из трёх ответов: whitelisted, greylisted и blacklisted. Whitelisted (белый список) – регистрация разрешена. Blacklisted (чёрный список) – регистрация запрещена. Реакция на greylisted зависит от поддержки этой функции со стороны коммутационного оборудования. Серые списки поддерживаются и в IMEI DB [9], однако фактически этот функционал не используется (обмен с CEIR выполняется только чёрными списками). Так как в каждой стране своё понимание серого списка, то такие списки используются внутри страны, то есть они содержатся на уровне EIR и/или CEIR и не передаются в IMEI DB.

Коммутационное оборудование – основные узлы сигнальной сети сотового оператора. Для 2G-сети это обычно MSC (Mobile Switching Centre, центр коммутации мобильной сети), совмещённый с VLR (Visitors Location Registry), базой данных, содержащей информацию обо всех абонентах, находящихся в зоне действия конкретного MSC. Для 3G-сети это обычно SGSN (Serving GPRS Support Node, узел обслуживания абонентов GPRS). Для 4G-сети это обычно MME (Mobility Management Entity, узел управления мобильностью). MSC выполняют сигнальный обмен по протоколу MAP (Mobile Application Part) стека ОКС-7 (общеканальная система сигнализации №7). Узел MME выполняют сигнальный обмен по протоколу S13 (расширение протокола Diameter). SGSN встречаются как работающие по протоколу MAP, так и по протоколу Diameter.

HLR (Home Location Register) – база данных в сети сотового оператора, содержащая информацию обо всех собственных абонентах этого оператора. Применяется в сетях 2G и 3G.

HSS (Home Subscriber Server) – аналог HLR в сети 4G.

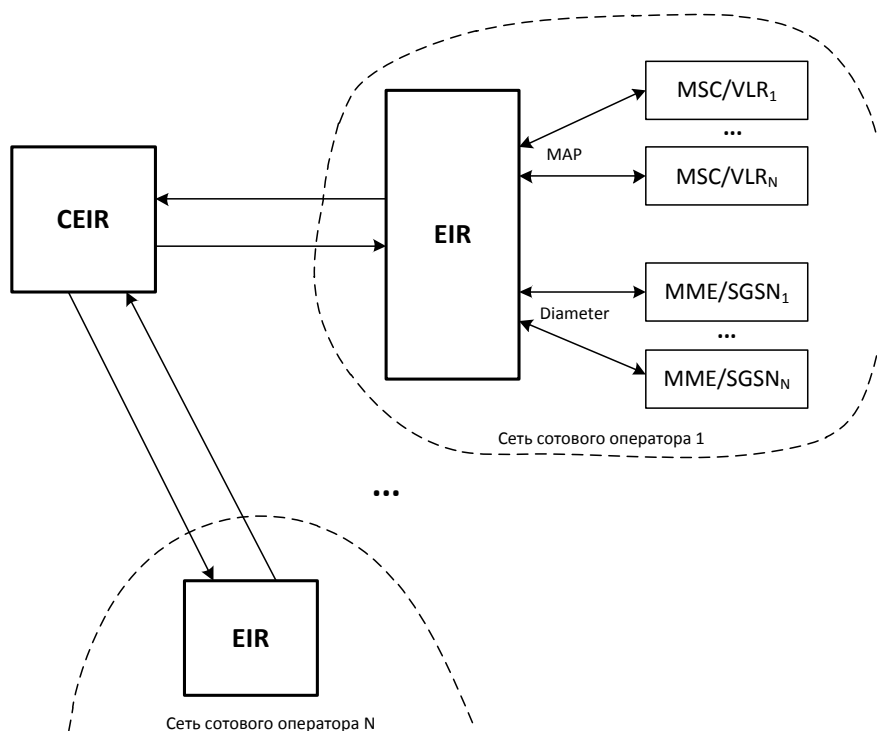


Рис. 1. Схема с минимальным набором компонентов, необходимых для работы центрального реестра с возможностью блокировки регистрации в сети

На рис. 1 приводится минимальная структурная схема компонентов, вовлечённых в работу центрального реестра идентификации мобильного оборудования. По мере расширения задач, которые должен решать центральный реестр (это рассматривается ниже), количество вовлечённых систем может значительно увеличиться (рис. 2).

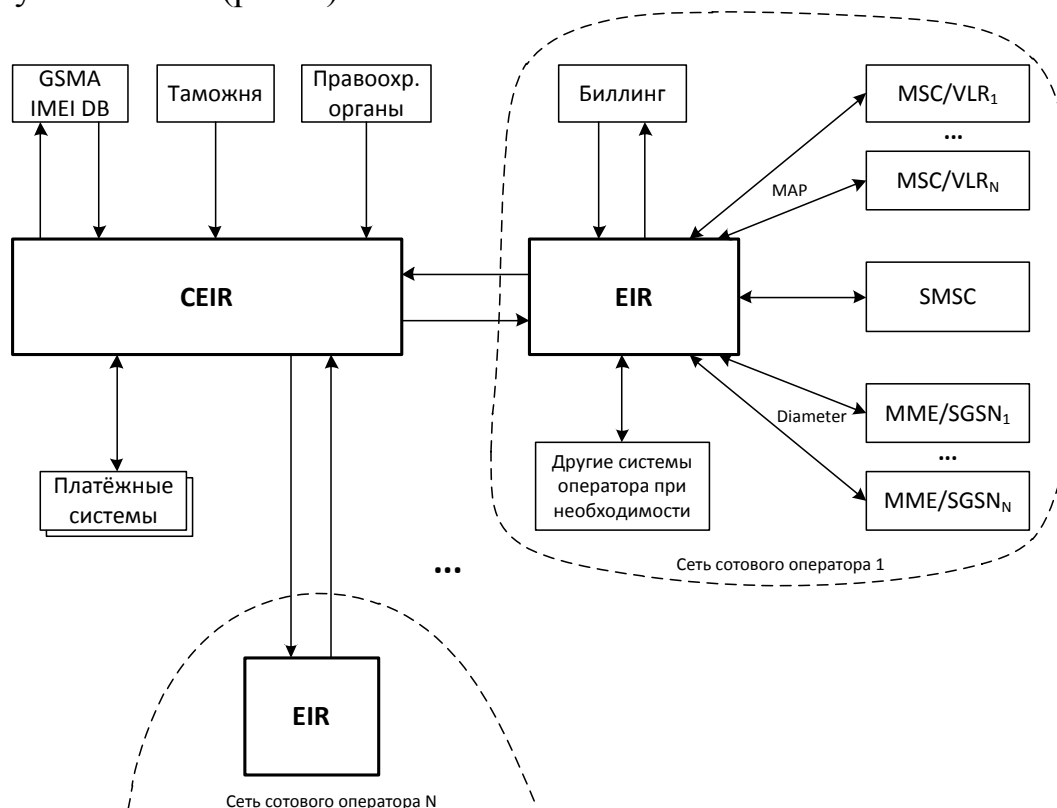


Рис. 2. Расширенная схема компонентов, вовлечённых в работу центрального реестра мобильного оборудования

Концептуальные моменты в разработке проекта

В данном разделе кратко характеризуются различные проблемные вопросы проекта по внедрению в стране центрального реестра идентификации оборудования, решение по которым может сильно повлиять на его структуру и принципы функционирования.

Первый концептуальный момент, который должен определить заказчик проекта – какие основные задачи должно решать внедрение системы, каким основным целям она должна следовать. В качестве основных можно выделить следующие цели:

- 1) повышение уровня предупреждения и раскрытия хищений мобильных устройств;
- 2) создание препятствий для нелегального ввоза мобильных устройств и их использования;
- 3) сокращение использования контрафактных абонентских устройств;
- 4) контроль уполномоченными органами государства использования абонентами средств мобильной связи.

Повышение уровня предупреждения хищений мобильных устройств считается основной целью внедрения центрального реестра. Поэтому он в очень

редких случаях не нацелен на решение этой проблемы. Другие две цели достигаются гораздо более сложными мероприятиями, поэтому они являются более дискуссионными. При выборе каждой из них заказчику следует определиться, насколько жёстко и принципиально планируется решать эти задачи. От выбранного варианта в дальнейшем будет зависеть много нюансов во всех остальных аспектах проектирования и внедрения центрального реестра – как технических, так и организационных.

Следующим важным аспектом создания центрального реестра является определение необходимости его интеграции с всемирным реестром CEIR (IMEI DB). Взаимодействие с IMEI DB состоит из двух независимых частей – обмен чёрным списком и получение списка выделенных ТАС [10, 11]. Если CEIR используется только для борьбы с кражами, то достаточно только обмена с чёрным списком (при этом возможны варианты: только импорт, только экспорт, двухсторонний обмен), либо можно вообще не интегрироваться с IMEI DB. Если CEIR используется также и для борьбы с контрафактом, либо для какого-то более глубокого анализа всего массива IMEI в стране, то необходимо также получение списка выделенных ТАС. Кроме собственно ТАС от GSMA поступает небольшой набор параметров к ним (наименование производителя, наименование модели, тип устройства и т.п.). Следует заметить, что интеграция с чёрным списком бесплатна, а получение списка ТАС – платная услуга.

Третий концептуальный момент состоит в следующем. Довольно распространена ситуация, когда в стране присутствуют сети различных стандартов – 2G, 3G, 4G, CDMA. Также распространена ситуация, когда у одного оператора есть сети более чем одного стандарта. Для того чтобы CEIR эффективно реализовал свои функции, он должен контролировать процесс регистрации во всех этих сетях. Таким образом, перечень типов сетей, которые требуется контролировать, определяет перечень коммутационного оборудования, с которым потребуется интегрировать EIR каждого оператора связи. При этом сети стандартов CDMA имеют некоторые отличительные особенности. В этих сетях есть аналогичная процедура проверки идентификатора абонентского устройства, и есть аналогичный узел EIR. Однако идентификатор устройств в сетях CDMA отличается по формату от IMEI (он называется MEID, Mobile Equipment Identifier). Нужно решить, будет CEIR влиять только на 2G/3G/4G-сети (например), или на все типы сетей. Если CDMA-сети тоже должны контролироваться центральным реестром, то разработчику потребуется это учесть, как минимум в алгоритме анализа идентификаторов и в структуре базы данных. Кроме того, MEID не содержится в IMEI DB. Их выделением и администрированием базы данных занимается другая организация [12]. Учитывая это, иногда прибегают к следующему решению: если сети CDMA в стране небольшие, и количество абонентов CDMA незначительно по сравнению с остальными сетями, то CDMA-сети не включают в проект. Обосновано это тем, что небольшие сети другого стандарта не могут составить сильную конкуренцию GSM-сетям, и значительной миграции абонентов из GSM в CDMA не произойдёт, даже из-за возможных неудобств от внедрения центрального реестра.

Далее, заказчик может учесть, что все устройства, использующие сотовую связь, можно поделить не только по поддерживаемым стандартам (GSM, CDMA и т.п.), но и по другим признакам. Для данного проекта может иметь значение деление на типы устройств, а именно: обычные мобильные телефоны, смартфоны, модемы, планшеты с SIM-модулем, IoT-устройства и другие. Можно накладывать ограничения в зависимости от типа устройства. Например, какие-то устройства всегда пускать в мобильную сеть. Если есть такая задача, то нужно определить возможность классификации устройств во время поступления CheckIMEI. Приведём примеры выполнения такой классификации.

- Можно использовать тип устройства, который содержится в IMEI DB для каждого ТАС-кода.
- В Казахстане было решено освободить от регистрации в реестре SIM-модули национальной системы экстренных вызовов при авариях и катастрофах (ЭВАК), которые устанавливаются в автомобилях. Оказалось, что их можно легко отличить по префиксу IMSI, так как для них используются только SIM-карты с определёнными сериями IMSI, которые для других целей не используются.

Другим проблемным вопросом для разработки архитектуры и всех сценариев работы центрального реестра является распределение зон ответственности между CEIR и EIR. Как правило, решение по данному вопросу получается не из выбора наиболее подходящего технического решения, а из конфликта интересов следующих участников проекта:

- 1) регулятор услуг связи хочет контролировать выполнение функций EIR, и как можно больше хочет знать о состоянии рынка услуг сотовой связи в стране;
- 2) сотовые операторы, во-первых, не желают передавать третьей стороне персональные данные своих абонентов и раскрывать важные показатели своей сети, а во-вторых, они могут иметь опасения, что вмешательство чужой системы в процесс регистрации абонентов в сети может ухудшить доступность услуг связи.

Наиболее сильно это повлияет на два следующих технических вопроса.

1. Какими данными, и в каком режиме, будут обмениваться CEIR и EIR каждого оператора?
2. Какой из этих узлов более интеллектуальный (реализует всю более сложную логику)? Например, сложными частями логики можно назвать реализацию серых списков и решение вопросов с дубликатами IMEI (см. ниже в обсуждении технических аспектов). Если это реализуется полностью на узлах EIR, то с них на CEIR, скорее всего, не потребуется передавать ряд данных.

Также распределение зон ответственности связано с юридическими и экономическими сторонами проекта, а именно: кому принадлежат EIR, на чьи средства они приобретаются или дорабатываются.

До разработки архитектуры заказчику необходимо зафиксировать, какие дополнительные сценарии или услуги должны быть реализованы с помощью CEIR.

Приведём примеры.

1. Будет ли реализована поддержка VIP-абонентов, которым можно регистрироваться с любыми устройствами?
2. Будет ли существовать привязка устройств к абонентам как услуга. Можно ли привязывать несколько устройств к одному абоненту? Можно ли привязывать одно устройство более чем к одному абоненту?
3. Какие услуги должны предоставляться центральным реестром абонентам и государственным службам? Например, дополнительные проверки на таможне при ввозе устройств:
 - а) проверка модели и внешнего вида;
 - б) проверка соответствия радиодиапазонов, поддерживаемых устройством, и разрешённых радиодиапазонов в стране.
4. Предполагается ли введение каких-то платежей? Если да, то должна ли информация об этом поступать в CEIR и как-то им обрабатываться?

Успешность и скорость реализации проекта может сильно зависеть от того, кто является инициатором проекта. Это может быть какое-то министерство, иной государственный орган, или даже местный производитель устройств, желающий защититься от импорта дешёвых контрафактных устройств. Чаще всего без поддержки государства такой проект реализовать невозможно, так как изменения, связанные с внедрением реестра, которые могут появиться в условиях оказания услуг сотовой связи, скорее всего, потребуют законодательной поддержки.

Бывает, заказчиком ставится условие, что поставщик CEIR должен быть компанией из этой же страны. Разумеется, не в каждой стране есть компания, уже производящая CEIR, либо имеющая достаточно компетенций для этого. Следствием этого становится то, что поставщик всё равно зарубежный, а в списке участников проекта появляется некий посредник – местная компания. Хорошо, если эта же компания выполняет некую полезную нагрузку (поставка оборудования, хостинг, услуги интегратора), но так бывает не всегда.

Организационные сложности

Сложности данного характера возникают из-за большого числа сторон проекта, куда могут входить: различные государственные органы и подразделения (законодательная власть, таможня, правоохранительные органы, интернет-порталы органов власти, включая электронное правительство, и т.д.), операторы сотовой связи, будущий оператор CEIR, поставщик CEIR, интегратор(ы), производители мобильных устройств, крупные ритейлеры и импортёры мобильных устройств.

У каждого сотового оператора уже может быть EIR, в том числе выполняющий дополнительные функции. В этом случае потребуется его как-то совместить с новыми сценариями работы. Чаще всего для оператора это означает, что потребуется либо доработка имеющегося EIR, либо его замена на новое решение от другого поставщика. На это требуется время. Поэтому необходимо

как можно раньше зафиксировать с операторами требования к их EIR, и возможно к другим их системам.

Также потребуется разделить зоны ответственности между государством (регулятором услуг связи, оператором системы CEIR) и операторами сотовой связи. Как минимум может быть четыре варианта.

1. CEIR имеет выносы в сети операторов, которые являются частью CEIR. Они управляются только со стороны регулятора. Коммутаторы оператора интегрируются с этим выносом, а если в сети оператора уже есть EIR, то вынос CEIR проксирует на него все запросы CheckIMEI, на которые он отвечает разрешением (whitelisted).
2. Коммутаторы интегрируются с операторским EIR, который по каждому CheckIMEI делает запрос на вынос (все списки и логика, определяющая, что ответить коммутатору, находятся на выносе CEIR).
3. EIR в сетях операторов принадлежат операторам и управляются ими, кроме списков, которые синхронизируются с CEIR.
4. Выносов и EIR нет. Все запросы CheckIMEI передаются из сетей операторов на центральный реестр оборудования, а он на них отвечает. Такой вариант, скорее всего, вероятен только в маленькой стране.

Далее в ходе разработки сценариев работы новой системы следует определиться, где и как будет происходить взаимодействие с абонентами. Кроме удалённого взаимодействия, SMS-уведомлений и действий на веб-портале, скорее всего, потребуется и непосредственное обслуживание физических лиц или представителей юридических лиц. Заказчику необходимо решить:

- 1) какие услуги будут оказываться в точках обслуживания (например, регистрация устройства, привязка устройства к конкретному физическому лицу, отвязка устройства и др.);
- 2) какие необходимые условия или ограничения для оказания услуг (например, в Турции для регистрации нового мобильного устройства необходимо иметь вид на жительство, и при этом можно зарегистрировать не более одного устройства за 2 года);
- 3) в каких местах будут оказываться услуги (например, офисы сотовых операторов, офисы оператора CEIR, офисы почты);
- 4) какова стоимость услуг;
- 5) в случае если, за услуги требуется оплата, возникает целый ряд вопросов, связанных с приёмом и обработкой платежей.

Решения, принятые по этим вопросам, станут отправной точкой для проработки изменений, которые должны быть внесены в рабочие места служащих в точках обслуживания, и для проработки программных интерфейсов, которые CEIR должен предоставлять информационным системам на этих рабочих местах. На доработку рабочих мест и обучение персонала, опять же, требуется заложить некоторое время.

Разумеется, все эти нововведения требуют внесения изменений в нормативно-правовые акты. Как минимум это требуется для обоснования сбора новых платежей и пошлин с населения и импортёров, для регламентирования процедуры регистрации, для регламентирования внесения устройств в чёрный

список и удаления из него, и для того, чтобы обязать операторов на регулярной основе передавать данные из своих систем во внешнюю систему. Перечень того, что, как минимум, необходимо добавить в нормативно-правовые акты, если этого не было ранее:

- 1) определение абонентского устройства;
- 2) определение IMEI;
- 3) определение центрального реестра IMEI;
- 4) о том, какая организация является оператором центрального реестра IMEI;
- 5) о том, что изменение идентификатора абонентского устройства запрещено;
- 6) о том, какие устройства подлежат регистрации;
- 7) порядок регистрации устройства физическим лицом;
- 8) порядок регистрации устройства юридическим лицом – импортёром;
- 9) порядок регистрации устройства юридическим лицом – производителем;
- 10) порядок внесения в чёрный список и исключения из него физическим лицом;
- 11) порядок внесения в чёрный список и исключения из него правоохранными органами;
- 12) определения, какие IMEI являются допустимыми к использованию и какие запрещены (в том числе определение уникального IMEI);
- 13) определение частичной блокировки (если таковую планируется сделать);
- 14) расширить обязанности операторов (что они должны передавать в CEIR, с какой задержкой и периодичностью).
- 15) о том, что регистрация устройства является платной (или бесплатной). Возможно, указать ограничение стоимости или конкретную стоимость.

Дополнительно может потребоваться:

- 16) указание ответственности за смену IMEI;
- 17) документация на новую интерактивную государственную услугу (портал проверки IMEI и регистрации устройств).

Иногда противниками проекта может стать кто-то из крупных участников рынка: сотовый оператор, производитель или ритейлер мобильных устройств. Производитель, который не является ассоциированным членом GSMA, не обязан следовать официальным документам Ассоциации, а значит, не обязан исполнять правила по выделению и несменяемости IMEI. Например, членом GSMA не является компания Apple [13]. Для ритейлеров наличие центрального реестра оборудования может помешать серому импорту устройств. Операторов такая схема может не устраивать, так как с ней появляется или значительно усиливается внешний контроль за абонентской базой и, скорее всего, потребуется на постоянной основе передавать регулятору данные абонентов. При наличии крупных и активных оппонентов проекта, возможно, придётся сильно изменить или отказаться от части сценариев работы системы.

Экономические факторы

Кроме собственно стоимости новой системы, её внедрения и сопровождения, есть ряд других экономических факторов проекта, которые могут повлечь дополнительные расходы. Рассмотрим основные экономические факторы.

1. С запуском CEIR могут появляться новые обязательные платежи (например, при покупке или регистрации устройства, при ввозе устройства из-за границы, при передаче устройства другому абоненту) и новые ограничения (например, ограничение на ввоз мобильных устройств из-за границы). Все эти нововведения по понятным причинам могут вызывать недовольство абонентов. Стоит их планировать, учитывая, что они будут затрагивать большую часть населения страны, и, скорее всего, всю активную часть населения. Способы смягчения данного фактора могут быть следующими.
 - А. Не вводить оплату сразу. Сначала ввести бесплатную регистрацию, а когда пользователи разберутся с организационными вопросами и научатся регистрировать устройства, то вводить плату за эту услугу.
 - В. Как до ввода оплат, так и периодически после неё, анализировать финансовую сторону проекта и отношение к нему в обществе, чтобы скорректировать тарифную политику. Например, можно освободить от оплаты какую-то часть устройств: устройства местных производителей, самые дешёвые устройства, устройства, не предназначенные для личного пользования (GSM-модули, устройства IoT (Internet of Things) и т.п.).
 - С. Постараться сделать так, чтобы большая часть устройств регистрировалась не физическими, а юридическими лицами. В первую очередь импортёрами и производителями этих устройств. В этом случае обычный человек, купивший в магазине телефон, который уже внесён в реестр, будет освобождён от процедуры регистрации.
2. Как правило, в стране может быть много контрафактных аппаратов, в том числе много аппаратов с неуникальным или нулевым IMEI, либо с IMEI, который не был выделен удостоверяющим центром GSMA. Согласно оценке [14], объем контрафактных мобильных устройств на глобальном рынке составляет 15-20%. Есть страны, где их порядка 10%. Есть страны, где их количество превышает 40%. То есть, если предполагается использовать CEIR для борьбы с контрафактом, и просто ввести блокировку всех таких устройств, это может создать сильную социальную напряжённость вследствие экономических потерь у большой массы как физических, так и юридических лиц. Это и необходимость покупки новых устройств связи и возможный ущерб вследствие внезапного пропадания услуг связи. Способов смягчения данного фактора два.
 - А. Преждевременно предупредить всё население страны о предстоящих ограничениях и предоставить им простой сервис по определе-

нию легальности мобильных устройств. Чтобы у каждого пользователя была возможность заблаговременно проверить свои устройства и заменить нелегальные устройства легальными.

- В. Запустить CEIR сначала в режиме наблюдения, когда он получает все события регистрации, но чёрные и серые списки не наполняются, блокировки не производятся. CEIR должен работать в этом режиме некоторый период (предположительно от месяца до года) и сохранить все встретившиеся за это время пары IMEI-MSISDN. При включении в штатный режим работы CEIR все эти пары вносятся в белый список (так называемый «список амнистии»). Таким образом, если кто-то использовал контрафактное устройство до включения проверки IMEI, он сможет использовать его далее (с этим же номером), но при передаче его другому абоненту устройство регистрироваться в мобильных сетях страны не будет.

Чаще всего используют именно второй способ. Упростить его путём внесения в белый список только IMEI, а не пар IMEI-MSISDN, нельзя по понятным причинам. Во-первых, производители контрафактных устройств вполне могут прошивать целые партии своих устройств одним IMEI. Если внести один такой IMEI в белый список, будет разрешена регистрация сразу всем таким устройствам. Во-вторых, для какой-то части устройств возможна такая операция как перепрошивка IMEI, хоть она и нелегальна с точки зрения GSMA. Если станет известно, что какой-то IMEI является белым для CEIR, в стране тут же появится нелегальный бизнес по «разблокировке сотовых телефонов». То есть важно иметь на CEIR (и соответственно, на EIR в сетях всех операторов страны) именно реализацию белых списков IMEI-MSISDN.

Исходя из вышесказанного, в общий список работ и затрат по проекту необходимо включить работу по публичному разъяснению причин, сути и положительных сторон нововведений. Как правило, расходы по этой части ложатся на плечи государства.

Далее рассмотрим экономические факторы внедрения CEIR, возникающие для операторов связи.

1. Если выбран вариант разделения ответственности, когда системы EIR в сетях операторов принадлежат им (а вероятнее всего так и будет), то может оказаться, что имевшийся EIR у оператора обладает довольно ограниченным функционалом. А для реализации проекта требуется поддержка такого функционала, который у него отсутствует. (Например, нужна поддержка не только списков IMEI, но и списков IMEI-MSISDN, а базовые версии EIR этого не поддерживают). Также, если EIR в сети оператора использовался фиктивным образом (то есть чёрные списки в нём реально не наполнялись), то может встать вопрос о его производительности в условиях реального использования, когда списков много, и они большие. На объём работы EIR влияет не только размер абонентской базы оператора, но и размеры списков, по которым должна проверяться каждая регистрация, количество этих списков и др. Много моментов, которые могут потребовать расширенной

функциональности, описано ниже в разделе описания технических аспектов. Из вышесказанного вытекает, что оператору может понадобиться обновление или замена EIR на более производительный и/или более функциональный вариант.

2. Также может понадобиться доработка/обновление части коммутационного оборудования, которое отправляет на EIR запросы на проверку оборудования. Сюда входят MSC/VLR, SGSN, MME. Опишем сначала суть проблемы для оборудования, работающего с EIR по протоколу MAP. Спецификацией протокола MAP чётко описан только базовый вариант запроса CheckIMEI, который содержит только IMEI. IMSI и MSISDN могут содержаться только в запросе CheckIMEI Extended, поддержка которого не является обязательной, а формат не специфицирован. Таким образом, конкретный коммутационный узел может вообще не поддерживать передачу IMSI и MSISDN в запросе на проверку оборудования, либо поддерживает, но это платная опция, а также его конкретный формат может не поддерживаться на стороне EIR (что приводит к необходимости доработки EIR или этого узла). Для коммутационного оборудования, работающего по протоколу Diameter, проблема аналогична – в запросе ME-Identity-Check-Request обязательна передача IMEI, а параметры IMSI и MSISDN являются опциональными.

Что будет, если часть коммутационных узлов в стране не поддерживает передачу IMSI в запросе проверки оборудования? Это значит, что в зоне действия этого узла функции CEIR не будут выполняться. В лучшем случае они будут выполняться не полностью. По одному IMEI можно проверить только его наличие в чёрном или белом списке IMEI, но, как будет показано ниже, большая часть логики CEIR требует и проверки IMSI.

Если в стране есть местные производители мобильных устройств, работающих в сетях 2G/3G/4G, то внедрение CEIR может коснуться и их. Основной риск в экономической плоскости состоит в том, что если какой-то производитель не соблюдал рекомендации GSMA по использованию IMEI, а CEIR будет выполнять соответствующие проверки, то возникнут проблемы с легальностью оборудования этого производителя. Проблемы могут возникнуть независимо от того, где непосредственно выполняется производство – внутри страны или на какой-то зарубежной фабрике. Типичная ситуация: местный «производитель» заказывает производство партии телефонов под своим брендом в Китае, и никак не контролирует прошивку идентификаторов IMEI в них. В итоге на фабрике во все устройства прошивают одинаковый IMEI, причём ТАС может быть от произвольной модели, для которой в IMEI DB значится некое китайское название. Если анализировать эти устройства просто по его IMEI (а CEIR именно так и делает), то все они – контрафакт.

Таким образом, запуск блокировки контрафакта может негативно, и при этом значительно, повлиять на бизнес отдельных производителей мобильных устройств. Если этого в планах нет, то проблема может быть решена двумя путями.

1. В EIR и CEIR вводится функционал белых списков исключений для такого не совсем правильного оборудования. Проблема в том, что заранее неизвестен масштаб проблемы. Сколько таких производителей, сколько они уже продали устройств внутри страны, достаточно ли будет списка исключений по ТАС или требуются и исключения по IMEI, каковы будут размеры списков – исчерпывающие ответы на все эти вопросы поставщику систем CEIR/EIR, отдельному оператору или органам власти самостоятельно не собрать. Данная информация должна исходить от самих производителей, а значит, они должны быть заранее проинформированы о данном проекте и его возможных последствиях.
2. Более правильное решение состоит в следующем комплексе шагов:
 - а) такие производители заранее переходят на прошивку корректных IMEI в свои устройства;
 - б) для тех устройств с некорректными или дублированными IMEI, которые уже были проданы, проблема решается использованием «списка амнистии», который описан выше в этом разделе.

Технические аспекты

Имеется целый ряд технических аспектов, которые могут усложнить качественную реализацию системы CEIR. Список, представленный ниже, не претендует на полноту.

Многосимочные аппараты. Как указывалось выше, в многосимочных аппаратах собственным IMEI обладает каждый отдельный модуль связи, в который вставляется SIM-карта. Значит, если какой-то IMEI такого аппарата подлежит блокировке (например, по причине кражи), то необходимо поместить в чёрный список и другие IMEI этого аппарата. Иначе можно будет переставить SIM-карту в другой слот и пользоваться телефоном дальше.

Также информация о многосимочности устройства может понадобиться, если решено при внесении в реестр брать плату не за IMEI, а за устройство.

Поэтому в БД CEIR желательно:

- 1) иметь информацию, сколько всего IMEI имеет это устройство;
- 2) иметь конкретные IMEI каждого многосимочного устройства.

Это сделать непросто. Проще всего сбор такой информации реализовать для вновь ввозимых/производимых устройств: при их добавлении в БД CEIR сразу вносить IMEI одного устройства, указывая их связь. Для устройств, которые уже находятся в обороте, простого и эффективного способа не существует. Скорее всего, удастся постепенно заполнять такую информацию только в случаях, когда абоненты предъявляют в пункте обслуживания само устройство или документы на него.

Привязка устройства к абоненту. Если было решено, что каждое устройство должно быть привязано к конкретному абоненту, то, как минимум, БД CEIR должна содержать список пар IMEI-IMSI. Из-за особенностей привязки, накладываемых законодательно ограничений, и возникающих при этом сценариев обслуживания абонентов может понадобиться хранение в системе CEIR

дополнительных сведений (например, профиль абонента или карточка устройства).

MultiSIM. В данном случае подразумевается не клонирование SIM-карт и не технология записи нескольких профилей (в том числе, разных операторов) на одну SIM-карту. Имеется в виду наличие в сетях отдельных операторов услуг, в рамках которых может одновременно использоваться несколько SIM-карт с одним MSISDN, но с разными IMSI, либо наоборот. Все особенности таких услуг и их реализации предусмотреть невозможно, однако потенциально они могут создать проблемы – или для их пользователей, или для реализации запрета регистрации мобильных устройств. Поэтому для учёта этих особенностей на этапе обсуждения проекта все операторы страны, сети которых будут взаимодействовать с CEIR, должны предоставить сведения о таких услугах в их сетях, либо о наличии планов по их внедрению.

Дубликаты IMEI. Дубликаты IMEI появляются в следующих случаях.

1. Когда недобросовестный производитель не имеет договорных отношений с удостоверяющим центром GSMA или хочет сэкономить количество выданных ему IMEI, он может при создании партии устройств «прошить» в них одинаковые IMEI или использовать для этого ранее использованные IMEI. Это противоречит принципам выделения и использования IMEI [6, 7].
2. Владелец устройства сознательно прибегает к операции «перепрошивки IMEI». Это также противоречит принципам GSMA, и в некоторых странах эта операция преследуется по закону. Разумеется, при смене IMEI он меняется на произвольное значение, в том числе оно может совпадать с IMEI другого существующего устройства, либо вообще не входить в диапазоны разрешённых значений IMEI.
3. Каким-то образом у абонентов могут оказаться устройства с тестовыми IMEI. Они предназначены для устройств, на которых производитель хочет что-то протестировать ещё до их вывода на рынок. Такие IMEI выдаются более мелкими сериями, и для них соответствие определённым моделям не устанавливается. Важное требование GSMA к таким IMEI: в сети не должно находиться более одного устройства с каждым из них. Тем не менее, такие случаи встречаются. Возможно также, что перепрошивка такими IMEI производится в авторизованных сервисных центрах каких-то производителей, во время ремонта, а потом их не всегда перепрошивают исходным значением перед возвратом клиентам.

Таким образом, если в сети присутствуют два или более устройств с одинаковым IMEI, чаще всего только одно из них является произведённым, введённым и проданным на законных основаниях, а остальные являются или контрафактом, или устройством с изменённым IMEI (чаще всего так делают для сокрытия кражи устройства). Поэтому, если одной из целей перед CEIR ставится сокращение контрафактных устройств в стране, то он должен уметь выявлять дублированные IMEI.

Рассмотрим проблемы, возникающие при выявлении дубликатов IMEI и определении, какое из устройств подлинное, а какое контрафактное. EIR, как и CEIR, не имеет информации о состоянии устройства в каждый момент. Запросы на EIR поступают как минимум при регистрации и перерегистрации устройства в сети, и возможно в какие-то моменты между ними в зависимости от настроек коммутационного оборудования. Допустим, на EIR поступил запрос CheckIMEI, содержащий IMEI1 и IMSI1, при этом в БД CEIR уже содержится пара IMEI1-IMSI2. Как определить – это дублированный IMEI, или просто в одном устройстве сменили SIM-карту с IMSI2 на SIM-карту с IMSI1? Возможны разные варианты выяснения этой информации, каждый со своими недостатками.

1. Имея интеграцию с сигнальной сетью, EIR может совершать запросы в сеть, в ответе которых содержатся и IMEI и IMSI. Такими запросами являются MAP-PROVIDE-SUBSCRIBER-INFO (PSI) и MAP-ANY-TIME-INTERROGATION (ATI). То есть при получении CheckIMEI, содержащего некие IMEI и IMSI, система должна совершить запросы по всем другим IMSI, которые встречались с этим же IMEI, чтобы проверить, в сети ли они, и с каким IMEI сейчас используются. Перечислим недостатки метода.
 - A. Параметр IMEI в ответах на запросы PSI и ATI не является обязательным полем.
 - B. Вообще, EIR – это изначально пассивный узел сети, который не делает активных запросов в сигнальную сеть, а с введением таких запросов он становится активным узлом и при этом может заметно возрасти нагрузка на сигнальную сеть. Если выбирать такой способ, то следует рассчитать вероятную интенсивность таких запросов и, возможно, проработать меры по её снижению.
 - C. В БД CEIR могут иметься пары с этим же IMEI, в которых IMSI принадлежит другой сети, отличной от поступившего в данный момент запроса. Значит, нужно проверить и их. Запросы PSI и ATI в чужую сеть (по чужому IMSI) почти стопроцентно не будут пропущены. Значит, событие регистрации должно быть передано с EIR на CEIR, а он, определив наличие других пар с таким же IMEI, должен передать на соответствующие EIR команду проверить заданные IMSI. Потом все результаты проверок должны быть где-то собраны, скорее всего, на CEIR, и проанализированы.
 - D. У каждого оператора может быть более одного типа сети. А значит, кроме сетей 2G, может потребоваться проверять и в сетях 3G и 4G. Diameter-протоколы, которые предоставляют коммутационные узлы сетей 3G/4G, имеют аналог запроса PSI, однако в ответах на него нет обязательного поля IMEI.
2. Вместо стандартных запросов в сигнальную сеть, которые возвращают много дополнительной информации, которая для обнаружения дубликатов не требуется, можно задействовать прямой интерфейс с узлом HLR, который всегда возвращал бы статус IMSI (в сети или нет) и

IMEI (если IMSI в данный момент зарегистрирован в сети). Такой интерфейс называется MML (Man-Machine Language), и его возможности отличаются для HLR разных производителей. Перечислим недостатки метода.

- А. Нужно, чтобы каждый оператор предоставил доступ к такому интерфейсу со стороны EIR. Разные HLR могут иметь разный формат протокола. Поставщику EIR нужно будет добавить поддержку соответствующего формата MML.
 - В. Нагрузка на сигнальную сеть не повысится, но возрастёт нагрузка на HLR.
 - С. Аналогично варианту с запросами в сигнальную сеть, здесь требуется для каждого события иметь возможность совершать запросы и в другие сети. То есть задействуются EIR других сетей и CEIR.
3. Периодический анализ событий постфактум (например, посуточно). При каждом поступающем событии не выполняется никаких действий по определению дубликатов, а вместо этого все события регистрации передаются в БД CEIR, где периодически выполняется их анализ, в ходе которого выявляются дублированные IMEI, появившиеся со времени предыдущего анализа. Перечислим недостатки метода.
- А. Накопление и регулярный анализ большого объёма данных может повысить требования к выделяемым ресурсам под CEIR.
 - В. Обнаружение каждого дублированного IMEI откладывается во времени.

Учитывая сложность учёта всех особенностей протоколов и коммутационного оборудования, более приемлемым представляется последний из описанных вариантов обнаружения дубликатов IMEI. Накапливать в БД CEIR все события регистрации, дополненные временной меткой, не составляет труда – интеграции для этого уже есть, а эти данные могут пригодиться и для решения других полезных задач. Кроме того, не составляет труда дополнить каждое событие регистрации идентификатором сетевого узла, с которого оно пришло, а это тоже может пригодиться при анализе.

Обсудим далее, что должно происходить, если обнаружено наличие двух или более дубликатов IMEI в сетях сотовых операторов страны. Кто из этих абонентов использует подлинное устройство, а кто контрафакт – заранее неизвестно. Если исходить из того, что у CEIR есть только IMEI, набор IMSI, возможно есть MSISDN к каждому IMSI, то решать задачу далее только техническими средствами невозможно. Необходимо применять организационные меры, подкреплённые нормативно-правовыми актами. Наиболее вероятен следующий сценарий.

- 1. На каждое устройство с неуникальным IMEI доставляется уведомление о том, что владельцу необходимо подтвердить подлинность устройства в течение определённого срока, иначе оно будет заблокировано.
- 2. Для подтверждения желающие предъявляют само устройство и документы на него, и конечно SIM-карту, с которой оно используется.

3. В белый список CEIR вносится пара IMEI с IMSI предъявленной SIM-карты (или с MSISDN абонента).
4. В чёрный список вносится IMEI, как скомпрометированный.
5. Впоследствии, все другие SIM-карты не смогут зарегистрироваться в сети с данным IMEI – CEIR их будет блокировать.

Данный сценарий может иметь множество вариаций, желательно их предусмотреть на этапе проработки всего проекта. Осложняющим обстоятельством является то, что устройство может поддерживать только передачу данных (например, 4G-модем). Тогда классическое SMS (короткое сообщение) на него не доставить. Эта проблема может разрешаться как техническими, так и организационными методами. Например, вместо блокировки таких устройств можно их HTTP-запросы перенаправлять на веб-страницу с необходимой информацией.

Можно добавить, что удобным дополнительным средством при верификации устройства может быть БД параметров мобильных устройств, содержащая, в том числе, ТАС-коды и изображение устройства. Она может использоваться как при ручной проверке (сотрудник оператора или органов государственной власти сверяет внешний вид устройства), так и при выполнении автоматических проверок (например, если в 3G-сети регистрируется устройство, которое согласно его IMEI поддерживает только 2G, значит это не подлинный IMEI).

Вопросы информационной безопасности. В отличие от большинства систем, которые тесно взаимодействуют с коммутационными узлами оператора, CEIR находится не внутри сети оператора, а где-то на независимой площадке, и при этом должен иметь доступ в сети всех операторов страны. Это порождает ряд задач информационной безопасности – как на стороне CEIR, так и на стороне каждого оператора связи. Осложняющим фактором является то, что в составе CEIR, скорее всего, будет портал, общедоступный через интернет.

Также стоит добавить, что производителем CEIR, вероятнее всего, является компания, являющаяся производителем систем EIR. То есть, это компания, специализирующаяся на решениях, которые устанавливаются внутри защищённой сети оператора и чаще всего не имеют прямого доступа в интернет. Особенностью инсталляции таких систем является то, что при этом вопросы хостинга и большую часть вопросов ИБ решают специалисты сотовых операторов. Из-за этого необходимых компетенций для выбора правильного хостинга и решения всех необходимых вопросов по информационной безопасности у такой компании-поставщика может просто не хватать. Поэтому необходимым условием успешной реализации проекта может стать участие интегратора или привлечённых специалистов с необходимым опытом.

Площадка CEIR и площадки каждого EIR должны быть связаны, как минимум, для синхронизации списков. В зависимости от реализации системы набор передаваемых данных может отличаться, а кроме того в соответствии с законодательством страны какая-то их часть может быть классифицирована как персональные данные. Для повышения защищённости передачи данных желательно организовать связь между площадками участников проекта не через ин-

тернет-каналы, а через выделенные каналы. Поскольку проект, скорее всего, будет государственным, логично, если такие каналы предоставит государственный оператор, владеющий магистральными каналами. Также желательно сразу предусмотреть резервирование каналов.

Получение и использование MSISDN. Обсудим сначала, в каких случаях и зачем нужны MSISDN, а затем рассмотрим, как их получать. MSISDN необходим в следующих случаях.

1. Если в сценариях работы CEIR есть отправка SMS-уведомлений абонентам, то, скорее всего, система будет выполнять это по SMPP-соединениям (short message peer-to-peer protocol). А в этом случае необходим номер MSISDN получателя.
2. Если будет реализовываться сценарий добровольной привязки телефона к абоненту, то там, где это будет производиться (в офисах обслуживания или через веб-портал), абоненты будут указывать именно MSISDN, так как про существование IMSI большинство не знает.
3. Аналогично предыдущему пункту привязка телефонов к абонентам происходит в процессе выявления и уменьшения количества дубликатов IMEI, как это описано выше в этой статье. Можно привязывать IMEI к IMSI, но эта логика даст сбой при смене абонентом SIM-карты (MSISDN остаётся прежним, а IMSI изменяется). Лучше привязывать к IMEI к MSISDN.
4. Если CEIR будет осуществлять какую-то информационную поддержку органам власти (например, возможность посмотреть историю устройств, используемых абонентом), то MSISDN тут гораздо удобнее, чем IMSI.
5. Представим ситуацию, когда абонент обращается в правоохранительные органы с заявлением о краже устройства. IMEI он не помнит, об IMSI даже не знает. Что он знает точно – свой номер (MSISDN), время, когда его SIM-карта ещё точно была в телефоне, внешний вид телефона, и, возможно, сможет вспомнить название модели. Чтобы определить IMEI и добавить его в чёрный список, сотрудник правоохранительных органов может найти в БД CEIR, с какими IMEI и когда встречался данный MSISDN. Затем, если есть сомнения, то по производителю и модели телефона, которые тоже может выдать CEIR, уточнить у абонента устройство. Как видим, MSISDN в данном случае необходим, а также желательно иметь в составе CEIR базу данных с изображениями устройств, о которой уже упоминалось выше.

Таким образом, как в момент обработки событий регистрации с сотовых сетях, так и в отдельных сценариях обслуживания абонентов, может быть необходим номер абонента (MSISDN), который привязан к SIM-карте (IMSI), которая вставлена в конкретное мобильное устройство (IMEI).

Далее обсудим, в чём сложность сбора в БД триплетов идентификаторов IMEI-IMSI-MSISDN. Запросы проверки IMEI поступают по двух протоколам – MAP (запросы CheckIMEI) и Diameter (запросы ME-Identity-Check-Request). И MAP-узлы и Diameter-узлы могут в запросе передавать либо весь триплет, либо

только пару IMEI-IMSI. К сожалению, передачу полного триплета идентификаторов поддерживают далеко не все такие узлы (по опыту это поддерживает около половины коммутационных узлов). Однако даже если на коммутационном узле включён режим добавления полей IMSI и MSISDN в запрос проверки IMEI, всё равно какая-то часть запросов от него может приходить либо с IMEI-IMSI, либо вообще только с IMEI. Предлагается с такими событиями регистрации поступать следующим образом.

1. Если запрос содержит IMEI-IMSI и в БД уже есть триплет, содержащий эти значения, то считается, что событие относится к нему же (вероятность появления SIM-карты с таким же IMSI, но другим MSISDN исчезающе мала).
2. События, содержащие только IMEI, предлагается либо игнорировать (отвечать на них всегда whitelisted), либо проверять только по спискам IMEI. Доля таких запросов для каждого отдельного коммутационного узла редко превышает 1%, и обычно меньше 0,2%. Полностью избавиться от таких событий невозможно. К ним, например, относятся экстренные вызовы (emergency call), при которых разрешается позвонить вообще без SIM-карты в телефоне.
3. Если запрос содержит новое уникальное сочетание IMEI-IMSI, получить соответствующий MSISDN можно, имея соответствие этого конкретного IMSI с конкретным MSISDN. Возможны следующие способы связывания MSISDN и IMSI.

А. Пара IMSI-MSISDN – это, сочетание, которое хранится в различных базах данных оператора, описывающее SIM-карту абонента. SIM-карты выпускаются и уничтожаются не так часто. Можно, чтобы каждый оператор организовал в своих бизнес-процессах выгрузку новых сочетаний IMSI-MSISDN (новых выпущенных SIM-карт), желательно до их реальной продажи, а также передачу на CEIR данных об изъятых из оборота SIM-картах. Источником таких данных может быть, например, биллинг оператора. Передачу и связывание идентификаторов можно реализовать двумя способами.

- a. Каждый оператор поддерживает список актуальных пар IMSI-MSISDN в БД EIR. EIR дополняет всё, что может, до полных триплетов, а потом передаёт их в БД CEIR.
- b. Операторы реализуют выгрузку пар IMSI-MSISDN сразу на CEIR, все системы EIR передают в БД CEIR события регистрации как есть, а сборка триплетов IMEI-IMSI-MSISDN выполняется только на стороне CEIR.

В. Сотовый оператор предоставляет для системы EIR интерфейс на стороне HLR и HSS, по которым эти узлы будут выдавать MSISDN для запрошенного IMSI. При необходимости EIR делает запрос в HLR или HSS.

Таким образом, на этапе проектирования необходимо определиться, где будут нужны номера абонентов, и как их будет предпочтительнее связывать с другими идентификаторами.

Частичная блокировка услуг вместо полной блокировки. Заказчиком может быть определено, что при нахождении IMEI или какого-либо кортежа с ним в чёрном и/или сером списке этому устройству вместо запрета регистрации в сети, ему должны быть ограничены некоторые услуги. Например, в сером списке разрешается только звонить на местные номера, отправлять и получать SMS, а в чёрном списке разрешается только получать SMS, а также совершать звонки на несколько коротких номеров. Такие ограничения могут быть реализованы различными путями.

1. Управление услугами абонента в HLR/HSS и других системах оператора. Потребуется интеграция EIR с этими системами.
2. EIR сообщает о помещении в список некую систему в сети каждого оператора, которая уже сама совершает настройки во всех необходимых узлах. Скорее всего, такой системой может выступать биллинговая система. При этом абоненту может назначаться определённая услуга или тарифный план. Разумеется, потребуется интеграция EIR и биллинга.
3. Коммутационное оборудование (MSC/SGSN/MME) само реализует ограничения, в зависимости от ответа на запрос проверки IMEI (whitelisted/greylisted/blacklisted).

Кроме увеличения сложности (и, скорее всего, стоимости проекта) такие ограничения услуг обладают существенным свойством – в системах сотового оператора они назначаются не на IMEI, а на абонента (IMSI-MSISDN). Отсюда появляется ряд недостатков:

- 1) если в событии регистрации не поступил IMSI, то никакого ограничения выполнить нельзя;
- 2) при каждой переустановке абонентом SIM-карты в устройство, которое находится в другом списке, придётся снимать/назначать ограничения, от чего увеличится нагрузка на все вовлечённые узлы;
- 3) если в какой-то из сетей есть услуга, при которой у абонента может быть несколько SIM-карт с одним IMSI, то при частичной блокировке она будет распространяться на все устройства абонента.

Уведомление о блокировке. Интересный вопрос: надо ли информировать абонента о том, что его устройству запрещена регистрация в сетях страны? Любой абонент скажет, что нужно. Ведь на первый взгляд такая блокировка похожа и на поломку телефона, и на неисправность SIM-карты. Однако в некоторых странах блокировка происходит без всяких уведомлений. Всё дело в технических сложностях, возникающих при доставке уведомлений.

Во-первых, нельзя заблокировать устройство, а потом отправить на него SMS. Блокировка – это отказ в регистрации в сети, а если устройство не в сети, то SMS до него уже не будет доставлена. Возможные решения:

1. Частичное ограничение услуг вместо полной блокировки. Надо оставить абоненту возможность получать SMS. Возникающие при этом технические сложности описаны выше.
2. Можно сразу не блокировать, а сначала отправить SMS, дождаться его доставки, и затем заблокировать. Решение имеет следующие недостатки.

- А. Обработка таких событий регистрации оказывается растянутой во времени для EIR, что увеличивает требования к необходимым ресурсам.
- В. Это новая функциональность для EIR. То есть штатным решением уже будет не обойтись.
- С. EIR не может блокировать устройство в любой момент, а только при поступлении на него запроса проверки IMEI. Между такими запросами может пройти довольно длительное время. Ускорить процесс может принудительная отправка команды Cancel Location или команды PurgeMS протокола MAP (или их аналоги в протоколе Diameter), после которых устройство будет заново регистрироваться в сети. Однако отправка этих команд – тоже не стандартная функция EIR, наличие которой превращает его в активный узел сигнальной сети.

Во-вторых, SMS можно отправить только на устройства с поддержкой этой услуги, зарегистрировавшиеся в 2G-сети. Но есть устройства, которые регистрируются только в сети 3G или 4G. Варианты решения проблемы для таких устройств могут быть следующими.

1. Не отправлять ничего.
2. Для 4G-устройств можно использовать возможности IMS-сети (IP Multimedia Subsystem) по отправке сообщений. В сетях отдельных операторов возможности могут различаться.
3. Все HTTP-запросы с таких устройств перенаправлять на веб-страницу с уведомлением. Остальной трафик блокировать.
4. Если на этого же абонента зарегистрирована другая SIM-карта, вставленная в 2G-устройство, то отправлять уведомление на него.

В-третьих, следует учесть, что есть устройства, поддерживающие все типы сетей 2G/3G/4G или два типа сетей, и при этом они могут совершать попытки регистрации в разные сети в разном порядке.

В-четвёртых, необходимо решить нужно ли делать повторные уведомления (как часто и в каких ситуациях?).

В-пятых, необходимо решить, какой узел будет совершать формирование и отправку SMS-уведомлений – CEIR или каждый EIR. Для EIR это нестандартный функционал. Если это делает CEIR, то, скорее всего, отправка будет производиться по отдельным SMPP-соединениям с каждым сотовым оператором. При этом CEIR должен уметь по IMSI определять принадлежность к оператору, чтобы знать, в какой канал отправлять уведомление.

Таким образом, отправка уведомлений требует анализа всех возможных ситуаций, выработки сценариев для каждого из них и решения ряда сопутствующих технических и других задач.

Заключение

Вышеуказанное позволяет сделать вывод о том, что запуск в стране центрального реестра идентификации мобильного оборудования – довольно многогранный и сложный проект, в который вовлечено много сторон. И если са-

мый базовый вариант, реализующий только блокировку краденных и утерянных устройств, может быть формализован в понятные сроки, то добавление любого дополнительного функционала сразу добавляет в проект много неизвестных.

Практика показывает, что в странах, где власть законодательно приказывает ввести с определённой даты контроль мобильного оборудования по идентификаторам IMEI без предварительных исследований и разработки достаточно полных непротиворечивых требований, такой проект никогда в срок не выполнялся.

Для уменьшения проблем и задержек при внедрении национального центрального реестра идентификации мобильного оборудования рекомендуется начать проработку проекта с заблаговременного создания рабочей группы. В её состав должны входить представители следующих сторон: инициатор проекта, государственный орган, ответственный за реализацию проекта, будущий оператор реестра, сотовые операторы, эксперты по данной тематике (например, поставщики систем EIR и CEIR). На временной основе к участию в работе группы должны привлекаться юристы, представители служб государственной безопасности, таможни, импортёров, ритейлеров и производителей мобильных устройств.

Литература

1. Закон Республики Казахстан от 22 декабря 2016 года № 28-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам противодействия экстремизму и терроризму» (старая редакция) // ИС «Параграф» [Электронный ресурс]. 2016 – URL: https://online.zakon.kz/Document/?doc_id=38918483 (дата обращения 05.02.2019).
2. Об утверждении Правил регистрации абонентских устройств сотовой связи от 23 мая 2018 // Информационно-правовая система нормативных правовых актов Республики Казахстан [Электронный ресурс]. 2018. – URL: <http://adilet.zan.kz/rus/docs/V1800017028> (дата обращения 09.01.2019).
3. Справка о концепции контроля абонентских устройств по номеру IMEI // Экспертный совет при Правительстве РФ [Электронный ресурс]. 02.07.2018. – URL: <https://open.gov.ru/upload/iblock/1fa/1fafca03b6e6cf02d9204e89c86f8308.pdf> (дата обращения 09.01.2019).
4. Концепция контроля абонентских устройств по IMEI // Экспертный совет при Правительстве РФ [Электронный ресурс]. 02.07.2018. – URL: <https://open.gov.ru/upload/iblock/f3e/f3ee0b03df7bf3633721d9c0928e8147.pdf> (дата обращения 09.01.2019).
5. ETSI TS 123 003 V15.5.0 “Numbering, addressing and identification” // Сайт ETSI [Электронный ресурс]. 04.10.2018. – URL: https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/15.05.00_60/ts_123003v150500p.pdf (дата обращения 24.01.2019).
6. 3GPP TS 22.016 V15.0.0 “International Mobile station Equipment Identities (IMEI)” // Сайт 3GPP [Электронный ресурс]. 04.07.2018. – URL:

http://www.3gpp.org/ftp//Specs/archive/22_series/22.016/ (дата обращения 24.01.2019).

7. GSM Association Official Document TS.06 “IMEI Allocation and Approval Process”, Version 15.0 // Сайт GSM Association [Электронный ресурс]. 10.05.2018 – URL: <https://www.gsma.com/newsroom/wp-content/uploads//TS.06-v15.0.pdf> (дата обращения 10.01.2019).

8. IMEI Database // Сайт GSM Association [Электронный ресурс] – URL: <https://www.gsma.com/latinamerica/wp-content/uploads/2012/05/IMEI-Database-Overview.pdf> (дата обращения 24.01.2019).

9. GSM Association Official Document SG.18 “IMEI Database File Format Specification”, Version 5.1 // Сайт GSM Association [Электронный ресурс]. 16.12.2014. – URL: <https://www.gsma.com/newsroom/wp-content/uploads/SG.18-v5.12.pdf> (дата обращения 24.01.2019).

10. Coloured Lists // Сайт GSM Association [Электронный ресурс] – URL: <https://www.gsma.com/services/gsma-imei/tac-allocation/imei-database/coloured-lists/> (дата обращения 10.01.2019).

11. Mobile Network Operator Best Practices // Сайт GSM Association [Электронный ресурс] – URL: <https://www.gsma.com/services/gsma-imei/tac-allocation/imei-database/mobile-network-operator-best-practices/> (дата обращения 10.01.2019).

12. MEID Database // Сайт Telecommunications Industry Association [Электронный ресурс] – URL: <https://www.tiaonline.org/what-we-do/products-services/meid-database/> (дата обращения 10.01.2019).

13. Associate Membership // Сайт GSM Association [Электронный ресурс] – URL: <https://www.gsma.com/membership/who-are-our-gsma-members/associate-membership/> (дата обращения 10.01.2019).

14. Protsenko D. Overview of national initiatives and solutions to combat counterfeit mobile devices // ITU Workshop on “Combating Counterfeit Using Conformance and Interoperability Solutions”. Geneva, Switzerland, 28 June 2016. [Электронный ресурс]. 28.06.2016. – URL: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Documents/PPT/S1P3_D_Protsenko.pdf (дата обращения 22.01.2019).

References

1. Zakon Respubliki Kazakhstan ot 22 dekabria 2016 goda № 28-VI «O vnese-nii izmenenii i dopolnenii v nekotorye zakonodatel'nye akty Respubliki Kazakhstan po voprosam protivodeistviia ekstremizmu i terrorizmu» (staraia redaktsiia) [Law of the Republic of Kazakhstan of December 22, 2016 № 28-VI “About modification and additions in some acts of the Republic of Kazakhstan concerning counteraction to extremism and terrorism” (old edition)]. *IS “Paragraf”*. 2016. Available at: https://online.zakon.kz/Document/?doc_id=34199995 (accessed 09 January 2019) (in Russian).

2. Ob utverzhdenii Pravil registratsii abonentskikh ustroystv sotovoi sviazi ot 23 maia 2018 [On approval of the Rules for registration of subscriber cellular communication devices]. *Informacionno-pravovaja sistema normativnyh pravovyh aktov*

Respubliki Kazakhstan [Information and legal system of regulations of the Republic of Kazakhstan]. 23 May 2018. Available at: <http://adilet.zan.kz/rus/docs/V1800017028> (accessed 09 January 2019) (in Russian).

3. Spravka o kontseptsii kontrolya abonentskikh ustroystv po nomeru IMEI [Reference on the concept of control of subscriber devices by IMEI number]. *Jekspertnyj sovet pri Pravitel'stve RF* [Expert Council under the Government of the Russian Federation]. 2 July 2018. Available at: <https://open.gov.ru/upload/iblock/1fa/1fafca03b6e6cf02d9204e89c86f8308.pdf> (accessed 09 January 2019) (in Russian).

4. Kontseptsia kontrolya abonentskikh ustroystv po IMEI [Concept of control of subscriber devices by IMEI number]. *Jekspertnyj sovet pri Pravitel'stve RF* [Expert Council under the Government of the Russian Federation]. 2 July 2018. Available at: <https://open.gov.ru/upload/iblock/f3e/f3ee0b03df7bf3633721d9c0928e8147.pdf> (accessed 09 January 2019) (in Russian).

5. ETSI TS 123 003 V15.5.0 “Numbering, addressing and identification”. *ETSI*, 04 October 2018. Available at: https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/15.05.00_60/ts_123003v150500p.pdf (accessed 24 January 2019).

6. 3GPP TS 22.016 V15.0.0 “International Mobile station Equipment Identities (IMEI)”. *3GPP*, 04 July 2018. Available at: http://www.3gpp.org/ftp//Specs/archive/22_series/22.016/ (accessed 24 January 2019).

7. GSM Association Official Document TS.06 “IMEI Allocation and Approval Process”, Version 15.0. *GSM Association*, 10 May 2018. Available at: <https://www.gsma.com/newsroom/wp-content/uploads//TS.06-v15.0.pdf> (accessed 10 January 2019).

8. IMEI Database. *GSM Association*. Available at: <https://www.gsma.com/latinamerica/wp-content/uploads/2012/05/IMEI-Database-Overview.pdf> (accessed 24 January 2019).

9. GSM Association Official Document SG.18 “IMEI Database File Format Specification”, Version 5.1. *GSM Association*, 16 December 2014. Available at: <https://www.gsma.com/newsroom/wp-content/uploads/SG.18-v5.12.pdf> (accessed 24 January 2019).

10. Coloured Lists. *GSM Association*. Available at: <https://www.gsma.com/services/gsma-imei/tac-allocation/imei-database/coloured-lists/> (accessed 10 January 2019).

11. Mobile Network Operator Best Practices. *GSM Association*. Available at: <https://www.gsma.com/services/gsma-imei/tac-allocation/imei-database/mobile-network-operator-best-practices/> (accessed 10 January 2019).

12. MEID Database. *Telecommunications Industry Association*. Available at: <https://www.tiaonline.org/what-we-do/products-services/meid-database/> (accessed 10 January 2019).

13. Associate Membership. *GSM Association*. Available at: <https://www.gsma.com/membership/who-are-our-gsma-members/associate-membership/> (accessed 10 January 2019).

14. Protsenko D. Overview of national initiatives and solutions to combat counterfeit mobile devices. *ITU Workshop on “Combating Counterfeit Using Conformance and Interoperability Solutions”*. Geneva, Switzerland, 28 June 2016. Available at: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Documents/PPT/S1P3_D_Protsenko.pdf (accessed 22 January 2019).

Статья поступила 5 февраля 2019 г.

Информация об авторе

Никитин Дмитрий Александрович – кандидат физико-математических наук. Аналитик. ООО «Связьком». Область научных интересов: разработка дополнительных сервисов в мобильных сетях; оптимизация бизнес-процессов. E-mail: nikitin@svyazcom.ru

Адрес: 660100, Россия, г. Красноярск, ул. Ладос Кецохели, д.29, кв. 22.

Significant issues of introduction of a central register for mobile equipment identification in a country

D. A. Nikitin

Problem statement. *The central register of mobile equipment identification is already implemented in a number of the countries, including several countries of the ex-USSR. Now projects on elaboration of requirements, features of implementation and on introduction of such systems are going on in Russia, Uzbekistan, Tajikistan and other countries. Such projects are difficult (not only in the mentioned countries) and, as a rule, long. At the same time, there are practically no publications in Russian that comprehensively consider the use of such systems. The aim of the work is to consider the significant issues that all participants of project on introduction in the country of the central equipment identity register (CEIR) may face. Methods.* *A systems analysis of the information obtained during participation in the development of requirements for CEIRs and for equipment identity registers (EIRs) of separate cellular operators, during the designing of their functioning in various conditions, as well as information obtained in the preparation and implementation of such projects. Novelty.* *A block diagram of the national central mobile equipment identification register is provided. The most significant issues, which arise during the introduction of CEIR, are highlighted and classified by type: conceptual, organizational (including legal), economic and technical. For conceptual significant issues it is described how their solution affects structure and the principles of the register functioning. For organizational, economic and technical issues, solutions are proposed. Practical relevance.* *The presented analysis will help the customer of such system to consider all the most difficult moments in advance and develop a consistent specification, and also to plan adequate terms of project implementation. Further, article is interesting to mobile network operators that it contains requirements to their networks, which arises during the introduction central register for mobile equipment identification in a country.*

Keywords: *Central Equipment Identity Register, Central EIR, CEIR, Equipment Identity Register, EIR, IMEI, IMSI, MSISDN, GSMA, IMEI DB, IMEI duplicates, CheckIMEI, IMEI check, blocking of communication services, registration on the mobile network.*

Information about Author

Nikitin Dmitry Aleksandrovich – Ph.D. of Physical and Mathematical Sciences. Analyst. “Svyazcom” LLC. Field of research: development of additional services in mobile networks; optimization of business processes. E-mail: nikitin@svyazcom.ru

Address: Russia, 660100, Krasnoyarsk, Lado Ketskhoveli street, 29, Apt. 22.