Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Q.5051

(03/2020)

SERIES Q: КОММУТАЦИЯ И СИГНАЛИЗАЦИЯ, А ТАКЖЕ СООТВЕТСТВУЮЩИЕ ИЗМЕРЕНИЯ И ИСПЫТАНИЯ

Борьба с контрафакцией и использованием похищенных устройств ИКТ

Принципы борьбы с использованием похищенных мобильных устройств

Рекомендация МСЭ-Т Q.5051

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Q

КОММУТАЦИЯ И СИГНАЛИЗАЦИЯ, А ТАКЖЕ СООТВЕТСТВУЮЩИЕ ИЗМЕРЕНИЯ И ИСПЫТАНИЯ

СИГНАЛИЗАЦИЯ ПРИ РУЧНОМ СПОСОБЕ УСТАНОВЛЕНИЯ МЕЖДУНАРОДНЫХ СОЕДИНЕНИЙ	Q.1–Q.3
АВТОМАТИЧЕСКОЕ И ПОЛУАВТОМАТИЧЕСКОЕ МЕЖДУНАРОДНОЕ СОЕДИНЕНИЕ	Q.4–Q.59
ФУНКЦИИ И ИНФОРМАЦИОННЫЕ ПОТОКИ ДЛЯ СЛУЖБ ЦСИС	Q.60–Q.99
СЛУЧАИ, ПРИМЕНИМЫЕ К СТАНДАРТИЗИРОВАННЫМ СИСТЕМАМ МСЭ-Т	Q.100–Q.119
ТРЕБОВАНИЯ К СИСТЕМАМ СИГНАЛИЗАЦИИ № 4, 5, 6, R1 И R2	Q.120–Q.499
ЦИФРОВЫЕ СТАНЦИИ	Q.500–Q.599
ВЗАИМОДЕЙСТВИЕ СИСТЕМ СИГНАЛИЗАЦИИ	Q.600–Q.699
ТРЕБОВАНИЯ К СИСТЕМЕ СИГНАЛИЗАЦИИ № 7	Q.700–Q.799
ИНТЕРФЕЙС Q3	Q.800–Q.849
ЦИФРОВАЯ АБОНЕНТСКАЯ СИСТЕМА СИГНАЛИЗАЦИИ № 1	Q.850–Q.999
СЕТЬ СУХОПУТНОЙ ПОДВИЖНОЙ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ	Q.1000–Q.1099
ВЗАИМОДЕЙСТВИЕ СО СПУТНИКОВЫМИ ПОДВИЖНЫМИ СИСТЕМАМИ	Q.1100–Q.1199
ИНТЕЛЛЕКТУАЛЬНАЯ СЕТЬ	Q.1200–Q.1699
ТРЕБОВАНИЯ К СИГНАЛИЗАЦИИ И ПРОТОКОЛЫ IMT-2000	Q.1700–Q.1799
ХАРАКТЕРИСТИКИ СИГНАЛИЗАЦИИ, ОТНОСЯЩИЕСЯ К УПРАВЛЕНИЮ ВЫЗОВАМИ НЕЗАВИСИМО ОТ СЛУЖБЫ ПЕРЕДАЧИ ДАННЫХ (BICC)	Q.1900–Q.1999
ШИРОКОПОЛОСНАЯ ЦСИС	Q.2000–Q.2999
ТРЕБОВАНИЯ К СИГНАЛИЗАЦИИ И ПРОТОКОЛЫ СИГНАЛИЗАЦИИ ДЛЯ СПП	Q.3000–Q.3709
ТРЕБОВАНИЯ К СИГНАЛИЗАЦИИ И ПРОТОКОЛЫ СИГНАЛИЗАЦИИ ДЛЯ SDN	Q.3710–Q.3899
СПЕЦИФИКАЦИИ ТЕСТИРОВАНИЯ	Q.3900–Q.4099
ТРЕБОВАНИЯ К СИГНАЛИЗАЦИИ И ПРОТОКОЛЫ IMT-2020	Q.5000–Q.5049
БОРЬБА С КОНТРАФАКЦИЕЙ И ИСПОЛЬЗОВАНИЕМ ПОХИЩЕННЫХ УСТРОЙСТВ ИКТ	**Q.5050–Q.5069**

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т Q.5051

Принципы борьбы с использованием похищенных мобильных устройств

Резюме

В Рекомендации МСЭ-Т Q.5051 предлагаются принципы, предусматривающие требования и широкий круг комплексных и рекомендуемых мер, которые могут быть приняты и реализованы для борьбы с хищением и повторным использованием похищенных мобильных устройств.

В результате увеличения количества функций и расширения возможностей, доступных в мобильных устройствах, в последние годы возрастает значение этих устройств и уровень их использования в повседневной жизни людей. Побочным результатом этого стало расширение в ряде стран масштаба действий, направленных на хищение этих устройств и получение доходов не только за счет продажи самого оборудования, но и путем незаконного использования содержащихся в них информации.

В качестве ответной меры необходимы инициативы для противодействия хищению и повторному использованию похищенных мобильных устройств, а также для защиты хранимых в этих устройствах данных потребителей от незаконного использования. Зачастую устройства похищаются в одной стране, где могут быть внедрены решения по борьбе с использованием похищенных устройств, для последующей продажи в других странах или регионах, где аналогичные решения не развернуты. Следовательно, для успеха таких инициатив важно обеспечить координацию и совместное использование информации правительствами и операторами, направленные на борьбу с хищением и повторным использованием похищенных мобильных устройств во всемирном масштабе. В противном случае существует риск незаконной трансграничной торговли похищенными устройствами.

Следует отметить, что большинство применяемых в настоящее время решений для предотвращения хищения устройств и их повторного использования базируются на списках уникальных идентификаторов. По этой причине торговцы краденными устройствами, как правило, для обхода этих мер взламывают устройства, чтобы изменить их уникальные идентификаторы, причем иногда они выбирают идентификатор, уже используемый легальным устройством. Это открывает возможность возврата оборудования на рынок и его подключения к сетям подвижной связи.

В связи с таким положением дел многие страны не только борются с использованием похищенных мобильных устройств, но и предотвращают повторное появление в сетях устройств с неразрешенными перепрограммированными уникальными идентификаторами, обычно именуемыми поддельными идентификаторами. В то же время правительства других стран сталкиваются с проблемами и не имеют четкого представления о наилучших стратегиях, которые следует принять, что обусловлено, в основном, нехваткой знаний и специального опыта для понимания проблемы и возможных способов ее решения, а также для осознанного выбора эффективных вариантов, подходящих для своей конкретной страны. Ввиду этого необходимы руководящие принципы для решения этой проблемы, как указано в Резолюции 97 (Хаммамет, 2016 г.) ВАСЭ.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Q.5051	13.03.2020 г.	11-я	11.1002/1000/14140

Ключевые слова

Борьба с хищением мобильных устройств, соответствие, принципы, требования, безопасность.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т Q.5051

Принципы борьбы с использованием похищенных мобильных устройств

1 Сфера применения

В настоящей Рекомендации содержатся базовые принципы и требования, которые следует учитывать при реализации решений по борьбе с использованием похищенных мобильных устройств.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T Q.5050] Рекомендация МСЭ-Т Q.5050 (2019 г.) *Концептуальное решение по борьбе с контрафактными устройствами ИКТ*.

[ITU-T X.1058] Рекомендация МСЭ-Т X.1058 (2017 г.) *Информационные технологии – Методы обеспечения безопасности – Свод правил и норм для защиты информации, позволяющей установить личность*.

[ITU-T X.1127] Рекомендация МСЭ-Т X.1127 (2017 г.) *Функциональные требования безопасности и функциональная архитектура для мер противодействия кражам мобильных телефонов*.

3 Термины и определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 пользователь устройства (device user) [ITU-T X.1127]: Авторизованный пользователь мобильного устройства.

3.1.2 блокирование "kill switch" (kill switch) [b-GSMA]: Блокирование "kill switch" – это способ отключения важных функций мобильного устройства. По сути, это функция мобильного оборудования, при инициировании которой, например путем передачи в мобильное устройство сообщения определенного формата, устройство прекращает работу в соответствии со своим назначением, и его работа (или использование) может быть восстановлена только с разрешения владельца этого устройства.

3.1.3 мобильный телефон (mobile phone) [b-ITU-T X.Sup.19]: Электронное устройство, используемое для осуществления телефонных вызовов и отправки текстовых сообщений на обширной территории с помощью радиодоступа к сетям подвижной связи общего пользования и при этом обеспечивающее мобильность пользователя.

3.1.4 смартфон (smartphone) [b-ITU-T X.Sup.19]: Мобильный телефон с большими вычислительными возможностями, поддержкой различных типов соединений и усовершенствованной операционной системой, предоставляющей платформу для сторонних приложений.

3.1.5 поддельное устройство ИКТ (tampered ICT device) [ITU-T Q.5050]: Устройство на базе информационно-коммуникационных технологий (ИКТ), в котором имеются компоненты, программное обеспечение, уникальный идентификатор, элементы, защищенные правами

интеллектуальной собственности, или торговые знаки, в отношении которых совершена попытка изменения или которые фактически изменены без получения согласия непосредственно от изготовителя или его правомочного представителя.

3.1.6 уникальный идентификатор (unique identifier) [ITU-T Q.5050]: Идентификатор, связанный с единственным устройством и предназначенный для уникальной идентификации этого устройства.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации используются следующие термины:

3.2.1 недействительный идентификатор (invalid identifier): Уникальный идентификатор, не соответствующий формату, определенному в технических стандартах, или не включенный в справочную базу данных по идентификаторам устройств, распространяемую ответственной управляющей организацией.

3.2.2 клонированный идентификатор (cloned identifier): Действительный идентификатор устройства, должным образом присвоенный ответственной управляющей организацией одному устройству, но используемый другими, отличными от него, устройствами.

3.2.3 надежные уникальные идентификаторы (reliable unique identifiers): Должны быть уникальными для каждого устройства, которое они призваны идентифицировать, могут присваиваться только ответственной управляющей организацией и не должны меняться неавторизованными сторонами.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

EIR	Equipment Identity Register	Регистр идентификаторов оборудования
IMEI	International Mobile Equipment Identity	Международный идентификатор мобильного оборудования
IMSI	International Mobile Subscriber Identity	Международный идентификатор абонента подвижной связи
PII	Personally Identifiable Information	Информация, позволяющая установить личность
RUI	Reliable Unique Identifier	Надежный уникальный идентификатор
TAC	Type Allocation Code	Код распределения типов

5 Соглашения

В настоящей Рекомендации применяются следующие глагольные формы для формулировки положений:

a) ключевые слова "требуется, чтобы" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если делается утверждение о соответствии настоящей Рекомендации;

b) ключевые слова "следует" и "рекомендуется" означают требования, которые рекомендуются, но не являются абсолютно необходимыми. Таким образом, для утверждения о соответствии это требование не является обязательным;

c) ключевое слово "может" означает необязательное требование, которое допустимо, но не имеет рекомендательного значения. Этот термин не означает, что вариант реализации поставщика должен обеспечивать выполнение этой функции, и функция может быть активирована по желанию оператора сети/поставщика услуг. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии настоящей Рекомендации.

6 Общие аспекты

В результате увеличения количества функций и расширения возможностей, доступных в мобильных устройствах, в последние годы возрастает значение этих устройств и уровень их использования в повседневной жизни людей. Побочным результатом этого стало расширение в ряде стран масштаба действий, направленных на хищение этих устройств и получение доходов не только за счет продажи самого оборудования, но и путем незаконного использования содержащихся в них информации.

В качестве ответной меры необходимы инициативы для противодействия хищению и повторному использованию похищенных мобильных устройств, а также для защиты хранимых в этих устройствах данных потребителей от незаконного использования. Зачастую устройства похищаются в одной стране, где могут быть внедрены решения по борьбе с использованием похищенных устройств, для последующей продажи в других странах или регионах, где аналогичные решения не развернуты. Следовательно, для успеха таких инициатив важно обеспечить координацию и совместное использование информации правительствами и операторами, направленные на борьбу с хищением и повторным использованием похищенных мобильных устройств во всемирном масштабе. В противном случае существует риск непреднамеренного содействия незаконной трансграничной торговле похищенными устройствами.

В связи с таким положением дел многие страны мира не только борются с использованием похищенных мобильных устройств, но и предотвращают повторное появление в сетях устройств с неразрешенными перепрограммированными уникальными идентификаторами, обычно именуемыми поддельными идентификаторами. В то же время правительства других стран сталкиваются с проблемами и не имеют четкого представления о наилучших стратегиях, которые следует принять, что обусловлено, в основном, нехваткой знаний и специального опыта для понимания проблемы и возможных способов ее решения, а также для осознанного выбора эффективных вариантов, подходящих для своей конкретной страны. Ввиду этого необходимы руководящие принципы для решения этой проблемы, как указано в Резолюции 97 (Хаммамет, 2016 г.) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ).

Таким образом в настоящей Рекомендации описаны принципы, предусматривающие требования и широкий круг комплексных и рекомендуемых мер, которые могут быть приняты и реализованы для борьбы с хищением и повторным использованием похищенных мобильных устройств.

7 Требования высокого уровня

Заинтересованные стороны, реализующие различные решения по борьбе с использованием похищенных мобильных устройств, испытывают определенные проблемы. Внедряя решения по борьбе с использованием похищенных мобильных устройств, странам следует учитывать требования, описанные в настоящем разделе.

7.1 Предотвращение использования похищенных мобильных устройств неавторизованными пользователями

Требуется внедрять решения, позволяющие отключать устройства в случае их хищения или потери, приводя их в нерабочее состояние для неавторизованных пользователей.

Требуется, чтобы это происходило автоматически при попытке неавторизованного пользователя получить доступ к устройству определенное количество раз (например, если неавторизованный пользователь после определенного ряда попыток не может ввести правильный пароль или персональный идентификационный номер (PIN) пользователя).

Рекомендуется обеспечить возможность дистанционного запуска этого процесса авторизованным пользователем устройства по запросу (например, путем активации функции блокирования "kill switch" на утерянном/похищенном устройстве).

Требуется обеспечить возможность приведения устройства в рабочее состояние при его возвращении авторизованному пользователю устройства и, по возможности, восстановления хранившихся в нем пользовательских данных.

В [ITU-T X.1127] рассматриваются функциональные требования безопасности и функциональная архитектура для мер противодействия кражам мобильных телефонов. В настоящей Рекомендации описана реализация инструмента блокирования "kill switch" для использования в случае потери или хищения смартфона. Такой инструмент должен обеспечивать следующие возможности:

– дистанционное удаление хранящихся в смартфоне данных авторизованного пользователя;

– приведение смартфона в нерабочее состояние для неавторизованного пользователя;

– предотвращение возможности возобновления его работы без разрешения авторизованного пользователя, насколько это технически возможно;

– приведение смартфона в рабочее состояние при его возвращении авторизованному пользователю и, по возможности, восстановления хранившихся в нем пользовательских данных;

– обеспечение отслеживания местоположения утерянного или похищенного мобильного устройства.

Наряду с этим рекомендуется информировать пользователей мобильных устройств о порядке настройки и использования этих функциональных возможностей и о необходимости сообщать о потере/хищении мобильных устройств поставщикам услуг или соответствующим органам полиции или правосудия, чтобы препятствовать доступу этих устройств к сетям подвижной связи и давать правоохранительным органам возможность принимать соответствующие меры.

7.2 Предотвращение доступа в сеть похищенных мобильных устройств

Требуется внедрять решения для предотвращения доступа похищенных мобильных устройств в сети подвижной связи, предпочтительно посредством автоматизированных систем, работа которых поддается проверке.

Требуется, чтобы только авторизованные лица, такие как законный владелец устройства, имели возможность запрашивать включение похищенного мобильного устройства или его исключение из всех сетей в стране.

Рекомендуется разработать принципы политики для предотвращения использования в сети похищенных устройств.

Важно иметь в виду, что устройства, которые блокируются в сетях подвижной связи, где используются их уникальные идентификаторы, могут все же получать доступ в сети, которые не проверяют уникальные идентификаторы мобильных устройств, такие как сети беспроводного доступа (Wi-Fi). Поэтому важно дополнять данный подход другими, например описываемыми в разделе 7.1

7.3 Предотвращение использования мобильных устройств с поддельными и/или клонированными уникальными идентификаторами

Требуется внедрять решения для выявления мобильных устройств с поддельными и/или клонированными идентификаторами и проведения различия между ними и подлинными устройствами с достаточной точностью, чтобы можно было принимать меры противодействия, предпочтительно посредством автоматизированных систем, не оказывая воздействия на подлинное устройство.

Рекомендуется, чтобы в этих решениях использовались справочные базы данных для определения информации, относящейся к подлинным устройствам и их законному происхождению. Следует использовать в качестве источника информации для справочной базы данных национальные регистрационные базы данных для идентификации законным образом ввезенных и приобретенных телефонных аппаратов, а также базы данных по идентификаторам, выделенным производителям, и другим характеристикам устройств, для содействия проведения различия между подлинными и поддельными устройствами.

В этих решениях требуется учесть, что поддельный идентификатор может приобрести иные характеристики, которые следует принимать во внимание в процессе обнаружения и контроля, такие как идентификаторы без формата, недействительные идентификаторы, не имеющие одобрения типа, клонированные, не занесенные в национальные справочные базы данных и т. п.

7.4 Предотвращение доступа в сеть похищенных мобильных устройств из других стран

Рекомендуется, чтобы местные законы и регуляторные нормы содействовали координации и обмену информацией между правительствами и операторами из различных стран с целью предотвращения использования похищенных устройств, вне зависимости от того, где они были похищены.

Если не поощрять совместное использование данных на международном уровне и не содействовать этому, продолжится беспрепятственный рост незаконной международной торговли похищенными устройствами, что приведет к тому, что устройства, похищенные в одной стране, будут вывозиться в другие страны и регионы и там продаваться.

Для рассмотрения и решения этой проблемы рекомендуется, чтобы глобальная база данных по похищенным устройствам была доступна для всех в любой точке земного шара для сообщения о похищенных устройствах и проверки статуса устройства.

Следует обмениваться местными национальными "черными" списками устройств и делать их доступными для глобального сообщества, устанавливая требования предоставления местных данных о похищенных устройствах и обмена ими с глобальной базой данных по похищенным устройствам.

7.5 Снижение воздействия на потребителя

При принятии любых решений по борьбе с использованием похищенных мобильных устройств следует учитывать воздействие на потребителей. В случае если для достижения одной и той же цели потребителю доступны несколько способов, следует выбирать тот, который в наименьшей степени затрагивает законных потребителей.

Рекомендуется организовывать контроль за недавно активированными в сетях устройствами с недействительными идентификаторами и обеспечить заблаговременное извещение пользователей, предоставляя им достаточные и надлежащие сроки для предъявления доказательств законного приобретения, а также снижать последствия внезапного отказа в обслуживании таких устройств или избегать таких последствий.

Рекомендуется избегать блокирования контракта пользователя на обслуживание, когда принимаются меры для контролирования устройств с поддельными и/или клонированными идентификаторами.

Рекомендуется всеми возможными способами проводить открытые информационно-пропагандистские кампании относительно принимаемых мер, их цели, их преимуществ, а также вариантов и мер, которые пользователи могут принимать в случае потери или хищения их телефонов, или же если они приобрели устройства с поддельными или клонированными идентификаторами.

Рекомендуется при принятии мер в связи с устройствами с поддельными и/или клонированными идентификаторами рассматривать вопрос о введении периодов амнистии или переходных периодов. Уже используемые устройства могли быть приобретены добросовестным образом, и их пользователи могут не знать о рисках. Если принимается решение не блокировать уже действующие устройства, следует принять дополнительные меры для недопущения активирования этих устройств новыми пользователями.

Рекомендуется ввести эффективные способы получения сообщений и информации от пользователей и принятия мер для осуществления приостановки обслуживания и блокирования идентификаторов устройств.

Рекомендуется упростить блокирование идентификатора устройства, не предлагая пользователю вспомнить или найти его, например, установить историю вызовов устройства в сети оператора для определения утерянного/похищенного идентификатора.

Рекомендуется незамедлительно приостанавливать обслуживание и блокировать идентификаторы утерянных/похищенных устройств. Например, блокировать устройство сразу после подтверждения просьбы об этом заинтересованными сторонами, ответственными за блокирование устройства.

Требуется обеспечить все заинтересованные стороны инструментами для проверки и подтверждения блокирования устройства.

Рекомендуется, чтобы заинтересованная сторона, ответственная за блокирование устройства, сообщала пользователю о блокировании или приводила причины того, что устройство, о котором поступило сообщение, не может быть блокировано, в случае отказа в просьбе.

7.6 Защита личных данных потребителя

Следует защищать личные данные потребителя в случае потери или хищения устройства. В качестве первоочередной меры рекомендуется внедрять механизмы запрета использования устройств, включая запрет доступа к хранимых на них личным данным неавторизованными пользователями.

Рекомендуется информировать пользователей о значении защиты и создания резервной копии их личных данных, а также о том, как использовать функции, дающие им возможность дистанционно удалять информацию, позволяющую установить личность (PII), из похищенного устройства.

Рекомендуется, чтобы производители по умолчанию включали элементы [ITU-T X.1127] во все новые устройства.

Рекомендуется, чтобы заинтересованные стороны информировали пользователей о способах настройки и использования этой функции.

7.7 Предотвращение доступа на рынки похищенных мобильных устройств

Национальным регуляторным органам электросвязи рекомендуется сотрудничать с другими соответствующими национальными учреждениями (например, с таможней) для совершенствования контролирования устройств, заявленных как утерянные или похищенные, в данной стране и в других странах.

В рамках этого сотрудничества необходимо предусмотреть обеспечение следующих элементов, когда это применимо:

1) доступ к базам данных по похищенным устройствам, а также, поскольку существует возможность изменения уникального идентификатора для обхода национальных и международных баз данных по похищенным устройствам, к дополнительной информации (например, по недействительным устройствам, не имеющим одобрения типа);
2) доступ к глобальной базе данных по идентификаторам, выделенным законным производителям, для проверки структуры идентификаторов устройств, подлежащих ввозу;
3) доступ к списку марок и моделей устройств, имеющих одобрение типа, для обеспечения ввоза только моделей устройств, имеющих одобрение типа, в соответствии с надлежащими национальными нормами;
4) в зависимости от случая, доступ к национальным справочным базам данных по ввезенным и приобретенным законным образом идентификаторам устройств;
5) доступ к глобальной базе данных по похищенным устройствам, а также доступ к базе данных, содержащей конкретную информацию, которая дает возможность определить подлинность устройств. Это будет полезным, если уникальный идентификатор похищенного устройства мог быть изменен и перепрограммирован на идентификатор, представляющий другое устройство.

Рекомендуется полностью проверить идентификатор по национальной базе данных по устройствам, чтобы избежать появления устройства с идентификатором, принадлежащим другому устройству, уже ввезенному в страну.

Рекомендуется принимать меры правового характера против точек продаж, предлагающих похищенные устройства.

7.8 Другие аспекты, подлежащие рассмотрению в связи с подделкой уникальных идентификаторов похищенных мобильных устройств

К другим аспектам, подлежащим рассмотрению в связи с подделкой похищенных мобильных устройств, могут относиться следующие:

- рассмотрение вопроса о разработке принципов политики для предотвращения использования и продажи на рынке похищенных мобильных устройств;
- обеспечение информирования и профессиональной подготовки по техническим аспектам, связанным с хищением и подделкой уникальных идентификаторов мобильных устройств;
- рассмотрение возможности контролирования использования аппаратного и/или программного обеспечения, применяемого для подделки идентификаторов мобильных устройств.

Рекомендуется располагать правовыми основаниями и поддержкой, которые давали бы возможность правоохранительным органам наказывать тех, кто меняет, видоизменяет, стирает или подделывает идентификаторы мобильных устройств с целью обхода мер предотвращения использования на рынке похищенных устройств.

Рекомендуется, чтобы такая правовая система также охватывала меры, которые могут приниматься против тех, кто предлагает, ввозит или продает аппаратное и/или программное обеспечение, используемое для подделки идентификаторов мобильных устройств.

Рекомендуется проводить информирование и профессиональную подготовку правоохранительных органов по техническим аспектам, связанным с хищением и подделкой уникальных идентификаторов мобильных устройств, и по правовой системе, на основании которой преследуются правонарушения.

Рекомендуется, чтобы производители мобильных устройств включали механизмы, обеспечивающие надежность и целостность уникальных идентификаторов мобильных устройств.

8 Концептуальные требования

При реализации решений по борьбе с использованием похищенных мобильных устройств следует учитывать следующие требования.

8.1 Централизованная справочная база данных

Рекомендуется использовать централизованную справочную базу данных для хранения информации по утерянным и похищенным устройствам. Ввиду этого все операторы должны использовать эту базу данных для предотвращения доступа похищенных устройств к сетям подвижной связи.

База данных должна по меньшей мере содержать уникальный идентификатор похищенного устройства, дату события и наименование организации, которая включила эту информацию в базу данных.

Рекомендуется также включать в такую базу данных другие типы идентификаторов и информацию, которая способствовала бы выявлению похищенных устройств с поддельными идентификаторами и принятию мер в связи с ними.

Рекомендуется включать в эту базу данных информацию, связанную с устройствами, законно ввезенными и/или приобретенными.

Рекомендуется обеспечивать всем авторизованным лицам доступ к соответствующим базам данных.

Рекомендуется ввести обязательную регистрацию устройств. При проведении обязательной регистрации устройств следует проявлять осторожность при увязывании устройства с PII и учитывать побочное воздействие на торговлю легальными мобильными устройствами и конкуренцию на рынке мобильных устройств.

Рекомендуется ввести процедуры для проверки того, были ли блокированы устройства, заявленные как похищенные, и были ли применены надлежащие процедуры всеми заинтересованными сторонами.

8.2 Поддержка сети при блокировании устройств

Требуется, чтобы сети подвижной связи содержали элементы, способные предотвращать доступ похищенных устройств, действительные идентификаторы которых включены в "черный" список, а также устройств, которые передают идентификаторы в формате, не соответствующем стандартам уникальных идентификаторов[1].

Рекомендуется, чтобы решения, используемые для блокирования в сетях подвижной связи, поддерживали характеристики, позволяющие избегать использования устройств с клонированными уникальными идентификаторами и тем самым отличать подлинные устройства от клонированных[2].

8.3 Надежные уникальные идентификаторы

Рекомендуется, чтобы справочные базы данных, используемые для предотвращения доступа похищенных мобильных устройств к сетям подвижной связи, базировались на надежных уникальных идентификаторах (RUI), поскольку подделка уникальных идентификаторов устройств может отрицательно сказаться на эффективности решений, направленных на вывод похищенных устройств с рынка.

Рекомендуется, чтобы в мобильных устройствах их уникальные идентификаторы хранились [3] в защищенном элементе оборудования и чтобы в устройстве в технологически возможной мере принимались меры безопасности для обнаружения подделки защищенного элемента или хранящейся в нем информации и, в результате, приведения устройства в нерабочее состояние до и при условии восстановления первоначальных данных.

Рекомендуется, чтобы управляющая организация, ответственная за уникальные идентификаторы, проводила процесс, который бы стимулировал надлежащее и безопасное использование уникальных идентификаторов законными производителями устройств, которым были выделены идентификаторы.

Рекомендуется, чтобы эти уникальные идентификаторы соблюдали принципы целостности (все производители должны получать от соответствующей организации выделенные диапазоны идентификаторов) и определенные в отрасли принципы безопасности (все установленные меры или их сочетание для установки идентификаторов таким образом, чтобы их подделка была невозможной)[4].

Рекомендуется, чтобы применяемые для реализации этих принципов в отрасли процессы поддерживались правительствами или национальными нормативными базами.

Требуется, чтобы уникальные идентификаторы не поддавались перепрограммированию, даже при техническом обслуживании. Если имеется возможность изменять идентификаторы после завершения процесса производства, это может уменьшить безопасность уникальных идентификаторов, и неавторизованные третьи стороны получат возможность их подделывать.

8.4 Тесное сотрудничество с правоохранительными органами и другими учреждениями страны

Для эффективного ограничения обращения похищенных устройств на рынке требуется наладить тесное сотрудничество между организациями, ответственными за ведение и предоставление справочных баз данных, национальными таможенными управлениями и их коллегами из других стран и соответствующими заинтересованными сторонами. Следует учитывать следующие аспекты:

---

1 См. [b-3GPP TS 122.016] и [b-3GPP TS 123.003] для устройств, соответствующих 3GPP/3GPP2.

2 Для устройств, соответствующих 3GPP/3GPP2, при использовании IMEI в качестве уникальных идентификаторов поддержку выполнению этого требования может оказать проверка IMEI-IMSI от радиосети доступа к базовой сети.

3 Например, в [b-3GPP TS 122.016] определяется, что IMEI не должен изменяться.

4 Например, см. [b-IMEI-SEC] для мобильных устройств, соответствующих 3GPP.

- таможенные управления и другие соответствующие национальные уполномоченные организации играют решающую роль в отслеживании и выявлении похищенных, утерянных или поддельных продуктов, поэтому важно снабдить их инструментами для определения похищенных, утерянных, поддельных и даже законных устройств, например с использованием централизованной справочной базы данных;
- необходимо установить и в полной мере применять процедуры правоприменения и связи между различными организациями. Это может включать обмен соответствующей информацией, такой как базы данных по мобильным устройствам в соответствии с национальными, региональными и международными стандартами;
- можно бороться с незаконной торговлей похищенными мобильными устройствами, применяя механизмы удостоверения идентичности отдельного устройства для проверки того, подлинное ли это устройство и разрешено ли его использование законами и нормами данной страны;
- правоохранительные органы на основании национальных правовых систем могут решить не сразу блокировать устройства в целях расследования, чтобы выяснить происхождение похищенных устройств, реализуемых на рынках, хотя следует стремиться по возможности оперативно блокировать все устройства, если отсутствуют действительные и исключительные основания не делать этого в отдельных случаях.

Рекомендуется на основании руководящей стратегии высокого уровня от высших органов власти создавать союзы и применять комплексный набор мер, чтобы содействовать обязательствам и осуществлению деятельности различных секторов и органов государственного управления, не относящихся к отрасли (например, правоохранительных органов, таможни, торговых организаций и т. п.).

8.5 Инструменты для проверки статуса мобильных устройств

Необходимо обеспечить общедоступный инструмент, для того чтобы потребители и другие заинтересованные стороны могли проверять статус мобильных устройств. Потребители и другие заинтересованные стороны должны иметь возможность проверить, по возможности через интернет, заявлены ли определенные устройства как похищенные или утерянные.

Рекомендуется, чтобы организация, ответственная за блокирование устройства, была указана в ответе на проверку устройства (включая страну, в которой осуществляется блокирование), чтобы потребитель мог избежать покупки или приобретения похищенных устройств, а также для адресации жалоб в случае неверного блокирования или блокирования третьей стороной в случае клонированного устройства с тем же идентификатором. Это также является важным инструментом для осуществления потребителем предпродажной проверки.

Рекомендуется, чтобы предприятия розничной торговли и организации, имеющие дело с устройствами, проводили проверки в отношении приобретаемых ими устройств, чтобы удостовериться, что эти устройства не были заявлены как утерянные, похищенные или имеющие дубликат уникального идентификатора. Следует вести учет для доказательства осуществления надлежащей проверки с целью уменьшения возможности продажи устройств, заявленных как утерянные, похищенные или имеющие дубликат уникального идентификатора.

8.6 Поддержка со стороны действующих национальных нормативно-правовых баз

Рекомендуется разрабатывать механизмы для выявления и блокирования утерянных и похищенных устройств, а также устройств с поддельными уникальными идентификаторами в сети подвижной связи, при наличии технической способности осуществления этих возможностей. Это следует проверять с местными операторами сетей подвижной связи.

Перед реализацией тех или иных ограничительных мер ограничительных мер в отношении похищенных устройств с поддельными и дублированными уникальными идентификаторами рекомендуется обеспечить поддержку со стороны действующих национальных нормативно-правовых баз, которая бы охватывала:

– ограничение сетевого доступа к похищенным устройствам в сетях электросвязи, заявленным на национальном уровне или в другой стране;

– ограничение сетевого доступа к устройствам с поддельными идентификаторами в сетях электросвязи;

– ограничение подделок уникальных идентификаторов мобильных устройств и последствий этого;

– принятие необходимых мер для проведения различия между подлинными и похищенными поддельными устройствами органами государственного управления, потребителями и предприятиями торговли;

– наличие органа власти, который отвечал бы за осуществление вышеуказанных пунктов.

При рассмотрении этого требования следует должным образом учитывать существующие национальные законодательные и нормативные базы, в которых могут затрагиваться уже охваченные аспекты.

9 Базовые принципы

На основании концептуальных требований, изложенных в разделе 8, предлагаются базовые принципы борьбы с хищением и использованием похищенных мобильных устройств, представленные на рисунке 1. Важно отметить, что не все описанные на рисунке 1 функциональные элементы являются необходимыми, и каждая страна может внедрять элементы в соответствии со своими потребностями.

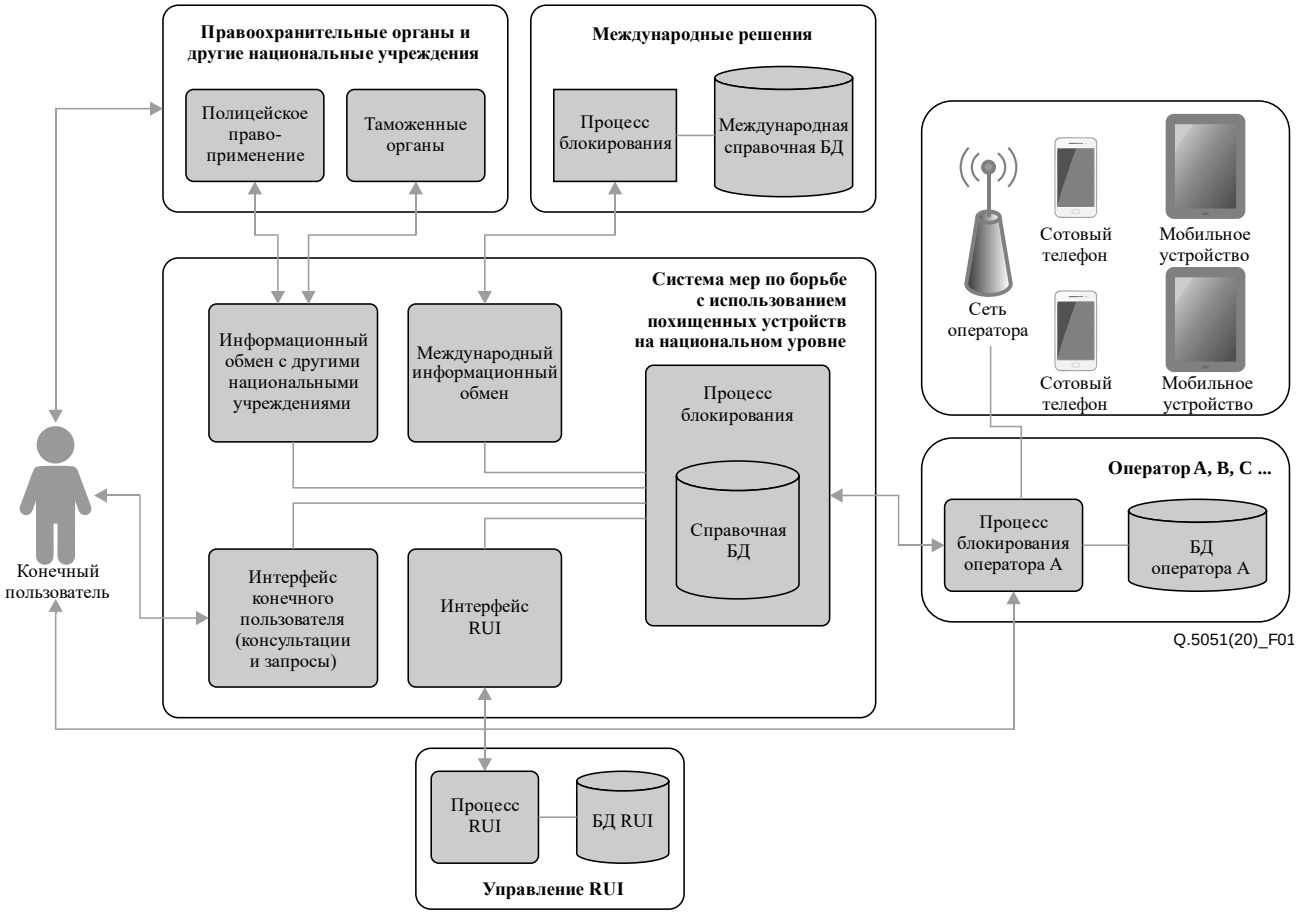

Рисунок 1 – Предлагаемые общие принципы

Следует слаженно осуществлять широкий круг мероприятий и применять информационные системы, управляемые различными организациями, для контролирования и получения критически важной информации с целью выявления утерянных, похищенных мобильных устройств и устройств с недействительными идентификаторами.

Потребители и другие заинтересованные стороны должны иметь возможность проверить, существуют ли ограничения в отношении конкретного устройства (было ли оно утеряно, похищено или имеет недействительный идентификатор).

Просьбу о блокировании похищенного устройства можно подавать через различные заинтересованные стороны (общества потребителей, правоохранительные учреждения, операторов подвижной связи или непосредственно в центральную систему). Независимо от того, куда была подана просьба о блокировании, следует принять меры для подтверждения личности пользователя и прав собственности на устройство. В отношении устройств, которые не были проданы потребителю, например похищенных при транзитных перевозках, из точек розничной торговли и т. п., просьба о блокировании устройства должна сопровождаться правовым опровержением.

Для ограничения обращения похищенных устройств на рынке другие соответствующие национальные учреждения (например, правоохранительные и таможенные органы) должны быть в состоянии проверить статус устройства, используя все имеющиеся справочные базы данных и источники.

Решающее значение также имеет обмен с иностранными организациями, который может осуществляться на двухсторонней основе или через глобальную справочную базу данных.

Чтобы гарантировать эффективное блокирование похищенных устройств в сетях подвижной связи, все операторы должны действовать в координации с национальными и глобальными справочными базами данных.

Требуется, чтобы управление RUI было интегрировано с процессом блокирования похищенных мобильных устройств, поскольку существует возможность подделки уникальных идентификаторов некоторых устройств для обхода процесса блокирования.

Требуется осуществлять процесс определения и контролирования в сетях мобильных устройств с недействительными идентификаторами, которые могут быть результатом подделки похищенного устройства после его блокирования.

10 Желательные характеристики

При реализации решений по борьбе с использованием похищенных мобильных устройств странам следует учитывать желательные характеристики, приведенные в нижеследующих разделах.

10.1 Глобальная справочная база данных по утерянным и похищенным устройствам

Блокированные устройства могут перевозиться и даже продаваться потребителям в различных странах, поэтому рекомендуется использовать глобальную справочную базу данных для совместного использования информации по идентификаторам утерянных и похищенных устройств и их блокирования, чтобы иметь единую информационную основу для занесения похищенных устройств в "черный" список, что упрощает совместное использование и сокращает время блокирования.

Рекомендуется, чтобы вне зависимости от масштабов работы оператора все устройства с идентификаторами, включенными в эту глобальную справочную базу данных, не допускались к соединению с местной сетью. Однако возможно рассматривать и альтернативные варианты, в зависимости от конкретных условий каждой реализации (например, при пакетной обработке активных уникальных идентификаторов в глобальной справочной базе данных).

Требуется, чтобы глобальная справочная база данных была доступна для правоохранительных органов и других государственных учреждений, которые могли бы сообщать о группах идентификаторов и осуществлять в отношении их запросы для содействия своим правовым действиям при борьбе с хищением мобильных устройств.

Рекомендуется, чтобы проверялась точность сообщаемой в глобальную базу данных информации по устройствам, заявленным как похищенные. Только после такого подтверждения списки похищенных устройств, составленные вышеуказанными сторонами, следует предоставлять для включения в эту глобальную базу данных по похищенным устройствам.

Доступ к этой глобальной базе данных следует обеспечивать для всех заинтересованных сторон во всем мире, чтобы они могли проверять, заявлено ли то или иное устройство как похищенное. Доступ к базе данных следует обеспечивать как на системном уровне, сторонам, которые могут блокировать похищенные устройства, так и на уровне потребителей, чтобы потребители из любой страны могли проверять, заявлено ли устройство как похищенное.

В глобальной базе данных должна содержаться соответствующая информация в случае ее наличия (например, характеристики устройства, страна, где оно было похищено, дата этого события и т. п.). Если идентификаторы похищенного устройства найдены в нескольких странах, в глобальной базе данных следует представлять информацию по результатам этого.

Следует вводить процедуры, с помощью которых участники глобальной базы данных могли бы рассматривать неумышленное блокирование (например, ошибочное блокирование, блокирование, связанное с дублированными и клонированными идентификаторами устройств).

10.2 Меры в отношении заведений, которые торгуют утерянными, похищенными и поддельными устройствами

Странам рекомендуется рассмотреть вопрос о создании системы, в которой устанавливались бы обязательства точек продаж предлагать только устройства, имеющие одобрение типа, и последствия предложения похищенных устройств или устройств с поддельными идентификаторами. Это расширит права и возможности правоохранительных органов, обеспечивая правовую поддержку для борьбы с продажами этих устройств и спросом на них.

Возможно включить в национальную справочную базу данных идентификаторы законно ввозимых и продаваемых устройств. Эта база данных могла бы быть полезной для различных действий и мер по правоприменению на национальном уровне в таких областях, как ввоз, продажи, использование в сетях и деятельность правоохранительных органов и т. п.

Таким образом, доступ к этой базе данных по авторизованным устройствам мог бы содействовать правоохранительным органам в принятии мер против заведений, предлагающих населению похищенные, поддельные или клонированные устройства, а также в выявлении и перехвате незаконно ввозимых продуктов.

Дополнение I

Подход Ассоциации GSM к борьбе с хищениями мобильных устройств

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Во все большем числе стран операторы дают потребителям возможность сообщать о потере или хищении мобильного устройства. Затем оператор может установить уникальный идентификатор устройства, т. е. международный идентификатор мобильного оборудования (IMEI), и оператор сети подвижной связи может блокировать телефон и лишить его доступа к своей сети подвижной связи. Это называется внесением в "черный" список IMEI[5].

Пример использования глобальной базы данных: в сообществе операторов подвижной связи занесенные в "черный" список IMEI включаются в глобальную базу данных по IMEI Ассоциации GSM (GSMA), что дает операторам возможность обмениваться данными и блокировать устройства в нескольких сетях на национальном и международном уровнях.

В базе данных по IMEI Ассоциации GSM ведется глобальный "черный" список на основе данных, предоставляемых участвующими в ее работе операторами. Ассоциация GSM предоставляет информацию из "черного" списка на круглосуточной основе без выходных операторам, которые установили связи с базой данных по IMEI, чтобы они могли загружать и использовать информацию в собственных сетях для блокирования устройств. Участвующие операторы выбирают список операторов, из которого они получают информацию "черного" списка, и это определяет степень обеспечения охвата совместного использования данных.

Для абонента, сообщающего об отсутствии устройства, зачастую неясно, утеряно или похищено было устройство, поэтому между этими двумя состояниями обычно не проводится различия. Если владелец находит устройство и сообщает об этом своему поставщику услуг, устройство может быть разблокировано, а IMEI удален из базы данных по IMEI. Затем Ассоциация GSM направляет указание по удалению из "черного" списка соединенным операторам, которые загружали первоначальную запись из "черного" списка.

Ввиду характера этой глобальной базы данных и решимости различных заинтересованных сторон на рынке предотвращать хищения устройств Ассоциация GSM разработала способ проверки статуса IMEI. Он называется "проверка устройства" и дает возможность совместного использования данных и информации о статусе устройства с утвержденными партнерами, в том числе с предприятиями розничной торговли, страховщиками, перерабатывающими предприятиями и правоохранительными органами.

В этой системе заинтересованные стороны могут узнать, заявлено ли то или иное устройство как утерянное или похищенное, причем сообщается история работы устройства за несколько лет, а также информация о модели и возможностях устройства. Такого рода возможность проверки имеет ряд преимуществ: a) помогает организациям, занимающимся перепродажей, выявлять и ликвидировать похищенные устройства до их попадания в цепочки поставки; b) подтверждает подлинность модели устройства и помогает рассчитать стоимость устройства; c) препятствует хищению устройств, снижая стоимость похищенного устройства; а также d) подтверждает сведения оператора, сообщившего о хищении или потере, что помогает вернуть устройство законному владельцу.

Наряду с операторами сетей услугой проверки устройства могут пользоваться многие другие организации в экосистеме мобильных устройств, в том числе: a) осуществляющие переработку устройств и их розничную продажу, а также дилеры, которые используют данные для снижения вероятности того, что устройства, заявленные как утерянные или похищенные, попадут в поток переработки или перепродажи; b) страховые компании, которые полагаются на базу данных для сокращения числа ложных или завышенных страховых исков по утерянным/похищенным

[5] См. [b-GSMA-IMEI-Blklst].

устройствам; а также c) правоохранительные органы, которые используют ее для выявления похищенных или утерянных товаров и содействия в расследовании и/или их возвращении[6].

Доступ для проверки единичного идентификатора в глобальной базе данных по IMEI может предоставляться ряду дополнительных заинтересованных сторон, включая потребителей, посредством предложения услуг от таких уполномоченных сторон, как национальные органы государственного управления, которые обеспечивают внешние порталы на местных языках, позволяющие знакомиться с информацией по IMEI. В настоящее время доступ для представления записей для внесения в "черный" список и/или исключения из него предоставляется только операторам сетей, которые могут однозначно определить и оценить данные по IMEI для своих клиентов, тем самым сохраняя целостность "черного" списка. Рассматривается возможность предоставления права внесения записей в "черный" список другим сторонам, таким как производители устройств, предприятия розничной торговли и т. п., которые могут дать оценку подлежащим блокированию IMEI или, напротив, поручиться за них.

Описанные выше системы (база данных по IMEI Ассоциации GSM и проверка устройств IMEI) дают пользователям ряд преимуществ по сравнению с национальными базами данных, которые вызывают фрагментацию, но могут создаваться на основе двусторонних или многосторонних действий по обмену сведениями об идентификаторах, заявленных как утерянные или похищенные, и по их блокированию. К этим преимуществам относятся: a) сокращение времени, требуемого для реализации и доводки; b) сокращение капитальных затрат (CAPEX) и эксплуатационных затрат (OPEX); c) меньшая сложность и бóльшая эффективность (одна общая точка происхождения вместо нескольких мест происхождения и назначения); а также d) меньший объем дублирования информации. Эти пункты базируются на следующих характеристиках описанных систем: a) модульность, b) отсутствие сборов за соединение для операторов/правительств; а также c) база данных по IMEI представляет собой проработанную и стабильную технологическую платформу, существующую с 1996 года.

[6] См. [b-GSMA-IMEI-DevChk].

Библиография

[b-ITU-T X-Sup.19] ITU-T X-series Recommendations – Supplement 19 (2013), *Supplement on security aspects of smartphones*.

[b-IMEI-SEC] GSMA (2016), *IMEI Security Design Principles. Enabling stolen mobile device blocking. V4.0*. <https://imeidb.gsma.com/imei/resources/documents/IMEI-Security-Technical-Design-Principles-v4.pdf>

[b-3GPP TS 122.016] ETSI TS 122 016 V3.1.0 (2000-01), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); International Mobile station Equipment Identities (IMEI) (3G TS 22.016 version 3.1.0 Release 1999)*.

[b-3GPP TS 23.003] ETSI TS 123 003 V10.5.0 (2012-04), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 10.5.0 Release 10)*.

[b-GSMA] GSM Association, Official Document SG.24 (2016), *Anti-Theft Device Feature Requirements v3.0*.

[b-GSMA-IMEI-Blklst] GSMA Services, *IMEI Blacklisting*. <https://www.gsma.com/services/gsma-imei/imei-blacklisting/> (last accessed 13 April 2020)

[b-GSMA-IMEI-DevChk] GSMA Services, *Device Check*. <https://www.gsma.com/services/gsma-imei/about-device-check/> (last accessed 13 April 2020)

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	**Коммутация и сигнализация, а также соответствующие измерения и испытания**
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2020 г.