Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Q.5050

(03/2019)

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

Борьба с контрафакцией и использованием похищенных устройств ИКТ

Концептуальное решение по борьбе с контрафактными устройствами ИКТ

Рекомендация МСЭ-Т Q.5050

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.5050

Концептуальное решение по борьбе с контрафактными устройствами ИКТ

Резюме

В последнее время оборудование на базе информационно-коммуникационных технологий (ИКТ) все шире используется в повседневной жизни людей, однако при этом наблюдаются нежелательные побочные явления, связанные с ростом продажи, оборота и использования контрафактных устройств ИКТ на рынке.

Контрафактное устройство ИКТ является продуктом, который в явном виде нарушает права на товарный знак, копирует разработки аппаратного или программного обеспечения, а также нарушает права на торговый знак или упаковку исходного или аутентичного продукта и в целом нарушает применимые национальные и/или международные технические стандарты, нормативные требования или процессы оценки соответствия, лицензионные соглашения на производство или другие применимые требования законодательства.

Смартфоны и другие мобильные устройства сегодня являются одними из наиболее распространенных и востребованных видов оборудования ИКТ во всем мире. При этом в качестве побочного явления все больше внимания обращает на себя деятельность черного/серого рынка таких устройств на глобальном уровне.

Это приводит к нежелательным последствиям практически для всех участников рынка – пользователей, сетевых операторов, производителей подлинных устройств, продавцов и государственных органов, включая, в частности, снижение уровня безопасности и качества обслуживания пользователей, а также убытки, претерпеваемые многими участниками рынка.

Экономические составляющие спроса на контрафактные устройства ИКТ и их предложения затрудняют попытки обуздать мировой рынок контрафактной продукции, поэтому данная проблема не может быть решена каким-либо одним методом. Ситуация требует комплексного подхода и принятия широкого спектра мер.

Целью Рекомендации МСЭ-Т Q.5050 вследствие этого является описание базового концептуального решения, включая задачи и требования высокого уровня, которые следует учитывать при реализации решений по борьбе с оборотом и использованием контрафактных устройств ИКТ.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Q.5050	15.03.2019 года	11-я	11.1002/1000/13702

Ключевые слова

Борьба с контрафактными устройствами ИКТ, соблюдение, соответствие, оценка соответствия, концептуальное решение, требования, безопасность, стандарт, уникальные идентификаторы.

* 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

Стр.

Рекомендация МСЭ-Т Q.5050

Концептуальное решение по борьбе с контрафактными устройствами ИКТ

1 Сфера применения

Настоящая Рекомендация содержит базовое концептуальное решение и требования, которые следует учитывать при реализации мер по борьбе с оборотом и использованием контрафактных устройств на базе информационно-коммуникационных технологий (ИКТ).

2 Справочные документы

В перечисленных ниже Рекомендациях МСЭ-Т и других справочных документах содержатся положения, которые посредством 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.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 оценка соответствия (conformity assessment) [b-ISO/IEC 17000]: демонстрация выполнения определенных требований, касающихся продукта, процесса, системы, лица или организации.

3.1.2 схема (или программа) оценки соответствия (conformity assessment scheme (or programme)) [b-ISO/IEC 17000]: система оценки соответствия, связанная с определенными объектами оценки соответствия, к которой применяются одни и те же заданные требования, конкретные правила и процедуры.

3.1.3 надзор за рынком (market surveillance) [b-EC-Regulation]: действия и меры, предпринимаемые государственными органами в целях обеспечения того, чтобы продукция соответствовала требованиям, изложенным в действующем законодательстве, и не ставила под угрозу здоровье, безопасность или какой-либо иной аспект защиты общественных интересов.

3.1.4 стандарт (standard) [b-WTO-TBT]: документ, одобренный уполномоченным органом и предоставляющий для общего и многократного использования правила, руководящие указания или характеристики для продуктов или связанных с ними процессов и методов производства, соблюдение которых не является обязательным. Он также может включать или охватывать исключительно требования к терминологии, символике, упаковке, маркировке или присваиванию обозначений в той мере, в какой они применяются к продукту, процессу или методу производства.

3.1.5 надзор (surveillance) [b-ISO/IEC 17000]: систематическая деятельность по оценке соответствия в качестве основы для обеспечения достоверности заключения о соответствии.

3.1.6 технический барьер в торговле (ТБТ) (technical barrier to trade): Соглашение Всемирной торговой организации (ВТО) о технических барьерах в торговле предназначено для того, чтобы технические нормы, стандарты и процедуры оценки соответствия были недискриминационными и не создавали излишних препятствий для торговли.

3.1.7 технические нормы (technical regulation) [b-WTO-TBT]: документ, в котором указаны характеристики продукта или связанные с ними процессы и методы производства, включая применимые положения административного законодательства, соблюдение которых является обязательным. Эти нормы также могут включать или охватывать исключительно требования

к терминологии, символике, упаковке, маркировке или присваиванию обозначений в той мере, в какой они применяются к продукту, процессу или методу производства.

3.1.8 серый рынок (gray market) [b-Gartner]: данный термин обозначает импорт и продажу устройств за пределами традиционных коммерческих каналов, определенных изготовителем оригинальной продукции или соответствующим правительственным органом; при этом формируется рынок, действующий параллельно официальным каналам распространения продукции.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 контрафактное устройство ИКТ (counterfeit ict device): устройство на базе информационно-коммуникационных технологий (ИКТ), которое в явном виде нарушает права на товарный знак, копирует разработки аппаратного или программного обеспечения, нарушает права на торговый знак или упаковку исходного или аутентичного продукта и в целом нарушает применимые национальные и/или международные технические стандарты, нормативные требования или процессы оценки соответствия, лицензионные соглашения на право производства или другие применимые требования законодательства.

3.2.2 поддельное устройство ИКТ (tampered ict devices) :устройство на базе информационно-коммуникационных технологий (ИКТ), в котором имеются компоненты, программное обеспечение, уникальный идентификатор, элементы, защищенные правами интеллектуальной собственности, и торговые знаки, в отношении которых совершена попытка изменения или которые изменены без получения согласия непосредственно от изготовителя или его правомочного представителя.

3.2.3 уникальный идентификатор (unique identifier): идентификатор, связанный с единственным устройством и предназначенный для уникальной идентификации этого устройства.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

CAS	Conformity Assessment Scheme		Схема оценки соответствия
DevID	Device Identifier		Идентификатор устройства
DIRBS	Device Identification, Registration, and Blocking System		Система идентификации, регистрации и блокировки устройств
EAP	Extensible Authentication Protocol		Расширяемый протокол аутентификации
EIR	Equipment Identity Register		Регистр идентификаторов оборудования
ICT	Information and Communications Technology	ИКТ	Информационно-коммуникационные технологии
IMEI	International Mobile Equipment Identity		Международный идентификатор мобильного оборудования
IoT	Internet of Things		Интернет вещей
IPR	Intellectual Property Rights	ПИС	Права интеллектуальной собственности
IVR	Interactive Voice Response		Интерактивный голосовой ответ
PCB	Printed Circuit Board	ПП	Печатная плата
SIM	Subscriber Identification Module		Модуль идентификации абонента
TAC	Type Allocation Code		Код распределения типов
TBT	Technical Barrier to Trade	ТБТ	Технический барьер в торговле
TEE	Trusted Execution Environment		Доверенная среда исполнения
TPM	Trusted Platform Module		Модуль доверенной платформы
TRIPS	Trade-Related Aspects of Intellectual Property Rights	ТРИПС	Торговые аспекты прав интеллектуальной собственности

5 Условные обозначения

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 будет сделано заявление о соответствии этой Рекомендации.

b) Ключевое слово "следует" означают требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом для заявления о соответствии это требование не является обязательным.

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

6 Общие аспекты

В последнее время устройства ИКТ все шире и активнее используются в повседневной жизни людей, однако при этом наблюдаются нежелательные побочные явления, связанные с ростом продажи, оборота и использования контрафактных устройств ИКТ на рынке. Это приводит к нежелательным последствиям для многочисленных участников рынка – пользователей, сетевых операторов, производителей подлинных устройств, продавцов и государственных органов, включая, в частности, снижение уровня безопасности и качества обслуживания пользователей, а также убытки, претерпеваемые многими участниками рынка.

Признано, что экономические составляющие спроса на контрафактные устройства ИКТ и их предложения затрудняют попытки обуздать мировой черный/серый рынок и что ни одно отдельно взятое решение по борьбе с контрафакцией не может служить универсальным средством для достижения этой цели. В настоящей Рекомендации предлагается концептуальное решение, включающее широкий спектр мер, которые могут быть приняты и применены в комплексном подходе к решению данной проблемы. Кроме того, с источниками контрафактной продукции следует максимально активно бороться на рынках стран, где они производятся и из которых экспортируются, с помощью государственных органов стран, в которых они продаются.

Определение различий между подлинными и поддельными устройствами ИКТ может представлять особую сложность для тех, кто проверяет или тестирует продукт, поскольку производители контрафакта нацелены на создание продуктов, очень похожих на подлинные устройства, путем предоставления фальшивой или украденной подлинной документации. В ряде случаев используются аппаратные компоненты, взятые из подлинного продукта или принадлежностей к нему, и даже копируются легальное программное обеспечение или уникальные идентификаторы, что затрудняет идентификацию контрафакта заинтересованными сторонами. Крайне важно учитывать упомянутые факторы наряду с другими в процессе реализации решений, чтобы у пользователей и производителей подлинного оборудования не возникало дополнительных проблем.

Смартфоны и другие мобильные устройства сегодня являются одними из наиболее распространенных и востребованных видов устройств ИКТ во всем мире. При этом в качестве побочного явления все больше внимания обращает на себя деятельность черного/серого рынка таких устройств на глобальном уровне. В рамках решения проблемы контрафактных устройств ИКТ некоторые страны приняли меры и успешно реализовали решения по сдерживанию оборота и использования контрафактных устройств ИКТ, в то же время правительства других стран сталкиваются с трудностями в выборе наилучшей стратегии.

Многие из решений, нацеленных на борьбу с контрафактными устройствами ИКТ, имеют сходные признаки, например использование уникальных идентификаторов устройств, применение режима оценки соответствия и методы блокировки доступа фальсифицированных устройств к сети (как это предложено для мобильных устройств в Приложении A).

Тем не менее правительства некоторых стран по-прежнему испытывают затруднения в борьбе с контрафактными устройствами ИКТ по разным причинам, которые включают технические аспекты, активные действия производителей контрафакта по сокрытию и защите от обнаружения, а также высокую востребованность контрафактных устройств, в связи с чем потребители часто принимают решения об их покупке.

Таким образом страны, которые ведут борьбу с контрафактной продукцией ИКТ, должны рассматривать в качестве руководства к действию и примеров передовой практики комплексные межведомственные подходы с учетом интересов всех участников рынка, а также технологические решения, применяемые в других странах, которые уже занимаются этой проблемой.

7 Основы упорядоченного рынка оборудования электросвязи

В основе создания упорядоченного рынка продуктов и услуг электросвязи лежит множество факторов. Основным требованием является формирование продуманных технических требований для продуктов, поступающих на рынок. Такие требования касаются, в частности, безопасности персонала, включая как пользователей, так и сотрудников поставщиков сетевых услуг, а также создания свободной от помех среды для услуг электросвязи.

Свободные от помех услуги, как проводные, так и беспроводные, тесно связаны с экономическим развитием общества, поскольку участие в глобальной цифровой экономике предполагает наличие устойчивых, безопасных и надежных платформ электросвязи, лежащих в основе экономической деятельности. Кроме того, четко определенный, хорошо управляемый, недискриминационный и прозрачный режим доступа к рынку формирует доверие к поставщикам оборудования и услуг, а также к людям в целом. Такой режим, подкрепленный соответствующей законодательной и нормативной базой, является фундаментом для обеспечения необходимого качества сетевого взаимодействия на национальном и международном уровнях, которое имеет решающее значение для участия в глобальной цифровой экономике. По сути он наиболее реально отражает приоритеты и ценности общества [b-ITU-D-CI-Guidelines].

8 Соображения, которые следует учитывать при реализации решений для борьбы с контрафактными устройствами ИКТ

При реализации решений по борьбе с контрафактными устройствами ИКТ участники рынка столкнутся с рядом непростых задач.

8.1 Обнаружение и идентификация контрафактных устройств ИКТ

Одна из целей производителей контрафакта – развернуть продажи своего продукта на рынках по всему миру. Производители контрафакта прикладывают все усилия, чтобы сделать свой продукт как можно более похожим на подлинный; это касается внешнего вида, копий уникальных идентификаторов, программного обеспечения и даже внутренних компонентов устройств ИКТ.

В связи с этим возникают определенные трудности. Например, все идентификаторы, создаваемые производителями подлинной продукции, могут неправомерно использоваться производителями контрафакта в собственных целях, то есть для обмана потребителей и органов власти, который заключается в том, что их продукт выдается за подлинный. Любые механизмы идентификации и системы их защиты могут стать мишенями для производителей контрафакта и преступных элементов. Логотипы и знаки одобрения типа, а также электронные идентификаторы зачастую умышленно искажаются или даже устанавливаются на пустое значение для последующего самопрограммирования на местных рынках. Это делается для того, чтобы избежать проверки таможенными и правоохранительными органами на границах [b-ITU-T TR-Counterfeit].

Все идентификаторы, создаваемые производителями подлинной продукции, могут быть подделаны производителями контрафакта в собственных целях, то есть для обмана потребителей и органов власти, который заключается в том, что их продукт выдается за подлинный. Эта проблема существует не только в секторе ИКТ, но и во многих других отраслях. Читателю следует иметь в виду, что любой механизм идентификации и система его защиты могут стать мишенью для производителей контрафакта и преступных элементов [b-ITU-T TR-Counterfeit].

Например, обычной практикой для производителей контрафакта является подделка уникальных идентификаторов, которые используются для аутентификации некоторых устройств в сети, с тем чтобы контрафактные устройства ИКТ распознавались сетью как подлинное оборудование. Кроме того, злоумышленники занимаются взломом и подделкой программного обеспечения подлинных устройств, для того чтобы оно выглядело как обновленная (и более дорогая) версия. Часто подлинные внутренние компоненты (например, батареи) заменяются поддельными в целях продажи подлинных элементов на рынке.

Логотипы и знаки одобрения типа, а также электронные идентификаторы зачастую умышленно искажаются. Это делается для того, чтобы избежать проверки таможенными и правоохранительными органами на границах. Все эти действия создают серьезные проблемы для производителей, потребителей, сотрудников таможенных и правоохранительных органов, которые часто испытывают затруднения в том, чтобы отличить поддельные идентификационные знаки контрафактного оборудования от подлинных знаков даже еще до проверки самого устройства.

8.2 Отслеживание производителей и распространителей контрафактных устройств ИКТ

При обнаружении устройства, не отвечающего стандартам, уполномоченные лица должны отслеживать страну происхождения, производителей и распространителей незаконных устройств и освобождать от них рынок [b-OECD].

В отсутствие эффективной идентификации и принудительных мер в отношении производителей и распространителей в странах происхождения любые меры в странах сбыта могут оказаться неэффективными.

8.3 Удаление с рынка уже используемых контрафактных устройств ИКТ

Контроль над контрафактными устройствами ИКТ, уже попавшими на рынок, зависит от возможностей воздействия на данную ситуацию. Потенциально могут применяться такие действия, как: i) обнаружение и проверка таких устройств (как физическая, так и дистанционная) по сравнению с характеристиками оригинального продукта; ii) прекращение их использования; а также iii) конфискация устройств.

Использование этих возможностей и принятие соответствующих мер связано с рядом проблем.

– Возможность физической проверки продукции может возникать в следующих ситуациях: в процессе технического обслуживания, в процессе надзора за рынком, а также в случаях, когда юридический орган имеет право проверить устройство. В данном случае вопрос заключается в создании необходимой базы данных и заинтересованности организаций в выполнении подобных задач.

– Проверка может проводиться как логически, так и дистанционно, например путем перекрестной проверки уникальных идентификаторов и характерных признаков продукта во время регистрации в режиме онлайн. Однако для этого, как правило, необходимо подключение к интернету, которое может быть затруднено в отдаленных и сельских регионах, особенно в развивающихся странах. Даже если все процессы проводятся в электронном виде, необходимо иметь возможность сопоставлять физические характеристики продукта с информацией об этом продукте, содержащейся в базах данных.

– Если для регистрации в сети устройство использует уникальный идентификатор, для контрафактных устройств ИКТ такого рода регистрация может быть запрещена. При этом необходимая информация поступает из базы данных устройств, авторизованных для работы на определенном рынке. Задача состоит в том, чтобы создать и поддерживать систему регистрации и базу данных, особенно в тех случаях, когда значительное количество устройств уже введено в эксплуатацию без подобных мер контроля.

– При этом не следует допускать злоупотреблений при использовании систем идентификации и регистрации, необходимо уважать права потребителей и не создавать дополнительных проблем пользователям устройств ИКТ. Кроме того, следует обеспечить защиту пользователей от произвольного отключения сетей.

– Возможность конфискации контрафактных устройств ИКТ зависит от физической проверки и в большинстве случаев требует вмешательства правоохранительных органов, которое проводится в рамках закона с учетом возможных юридических действий. Проблема заключается в установлении взаимодействия между различными организациями, определении правовой базы и степени ответственности за участие в обороте контрафактных устройств ИКТ.

– Не следует недооценивать также влияние на пользователей. Необходимо учитывать, что в некоторых странах, возможно, не разрешается отключать устройства и что жизнь пользователя может подвергаться риску.

8.4 Ограничение импорта, распространения и продажи новых контрафактных устройств ИКТ на рынке

В дополнение к действиям, направленным на изъятие уже используемых контрафактных устройств ИКТ, а также на изъятие этой продукции из запасов, необходимо принять меры, ограничивающие импорт, контрабанду, распространение и продажу новых контрафактных устройств на рынке.

Такой подход может способствовать сокращению общего наличия контрафактных устройств ИКТ на рынке в рамках финансовых и временных ограничений для администраций, которые решили предпринять эти действия и уменьшить влияние на конечных пользователей по сравнению с действиями, направленными на отключение контрафактных устройств ИКТ.

Как указано в пункте 8.2, эти меры также должны быть нацелены на источники появления контрафактных устройств ИКТ.

8.5 Определение различий между подлинными и контрафактными устройствами ИКТ

Для обеспечения эффективности действий по изъятию контрафактных устройств ИКТ на рынках и предотвращению появления новых устройств необходимо внедрить решения и критерии, позволяющие отличать подлинные устройства от контрафактных. При этом необходимо действовать с особой тщательностью даже при рассмотрении клонированных уникальных идентификаторов, с тем чтобы заградительные меры принимались в основном с использованием автоматизированных систем или в ручном режиме для ограниченного количества устройств ИКТ.

При определении различий между подлинными и контрафактными устройствами ИКТ необходимо учитывать нижеследующие аспекты.

– Целью производителей контрафакта является создание продукта, очень близкого к подлинному оригинальному продукту.

– Производитель контрафакта может активно пытаться вводить в заблуждение инспекторов, предоставляя фальшивую или украденную подлинную документацию, аппаратное и программное обеспечение в качестве части контрафактной продукции.

– Некоторые элементы контрафактного изделия могут быть взяты из подлинного продукта и его аксессуаров, включая в частности программное обеспечение, уникальные идентификаторы, детали корпуса, разводку печатных плат (ПП) и набор микросхем.

– В подлинных продуктах регулярно обновляется микропрограммное и программное обеспечение, прежде всего по соображениям безопасности. Это относится также к приложениям и некоторым аксессуарам. Таким образом определение характерного признака подлинного продукта может представлять непростую задачу.

– Зачастую для того чтобы отличить подлинное устройство, визуального осмотра недостаточно. Может потребоваться дополнительная техническая экспертиза, а также вспомогательные или лабораторные испытания.

8.6 Ограничение влияния на производителей подлинных устройств ИКТ

Решения, используемые для борьбы с контрафактными устройствами, должны свести к минимуму влияние на производителей подлинных устройств ИКТ и сосредоточить внимание на контрафактных устройствах ИКТ, их производителях и распространителях.

В связи с этим следует избегать схем, при которых производители подлинных устройств должны нести дополнительные расходы при производстве и реализации легальной продукции. Эти расходы могут сыграть на руку производителям контрафакта, которые привлекают покупателей более низкими ценами на свою продукцию.

8.7 Уменьшение влияния на конечных пользователей при изъятии контрафактных устройств ИКТ с рынка

Любое решение, принимаемое в целях изъятия или отключения контрафактных устройств ИКТ, должно тщательно продумываться в части влияния на конечных пользователей. Если для достижения одной и той же цели существует несколько путей, следует выбирать тот, который в наименьшей степени затрагивает потребителя.

Таким образом, необходимо учитывать нижеследующие аспекты:

– отключение устройств ИКТ в некоторых странах может быть запрещено;

– контакт с пользователем через устройство до его отключения не всегда возможен (например, для устройств, передающих только данные или СМС, при переадресации вызовов, для систем интерактивного голосового ответа (IVR) и в других случаях, когда контакт с пользователем отсутствует);

– блокировка может быть критичной для контрафактных устройств ИКТ, работающих с важными приложениями (например, медицинские приложения, финансовые услуги и т. д.);

– обеспечение надлежащего соблюдения прав пользователей, при этом все необходимые действия будут проводиться в соответствии с национальным законодательством.

8.8 Информирование потребителей

Потребители должны быть информированы по вопросам, связанным с покупкой и дальнейшим использованием контрафактных устройств ИКТ, включая в частности потенциальные риски для здоровья и низкое качество обслуживания.

Следует учитывать тот факт, что потребители часто принимают решение о покупке контрафактной продукции, ориентируясь на уровень цен и пренебрегая возможными проблемами в будущем. Поэтому очень важно информировать их о негативных последствиях использования контрафактных устройств ИКТ и преимуществах подлинных устройств.

8.9 Недопущение технических барьеров в торговле (ТБТ)

Следует позаботиться о том, чтобы не допустить возникновения препятствий легальному импорту и использованию подлинного оборудования ИКТ или технического барьера в торговле (ТБТ), определяемого Соглашением Всемирной торговой организации (ВТО) по торговым аспектам прав интеллектуальной собственности (ТРИПС) [b-TRIPS Agreement].

Речь может идти об использовании белых списков, которые по ошибке или в результате неправильного планирования могут помешать законным легальным пользователям, включая путешественников и туристов, использовать продукцию ИКТ. Такие требования по регистрации устройств могут непреднамеренно создать технические барьеры в торговле.

9 Концептуальные требования

При реализации мер по борьбе с контрафактными устройствами ИКТ уполномоченные органы стран должны учитывать нижеследующие требования.

9.1 Идентификация и меры принудительного характера против производителей и распространителей контрафактных устройств

В рамках борьбы с использованием контрафактных устройств ИКТ, поставляемых на рынок или ввозимых в страну, необходимо сформировать механизм отслеживания источника и удаления с рынка производителей и распространителей этой продукции.

Поскольку перед продажей контрафактные устройства ИКТ часто пересекают границы разных стран, то для выполнения этого требования необходимо установить тесное сотрудничество между заинтересованными сторонами, участвующими в данном процессе, а также между соответствующими сторонами в других странах, вовлеченных в процесс.

Как указано в пункте 8.2, требуется осуществлять идентификацию и принимать меры принудительного характера против производителей и распространителей контрафакта в странах происхождения.

9.2 Консультации с отраслевыми и потребительскими группами

Перед тем как принимать какие-либо меры по исправлению ситуации, необходимо установить связь со всеми заинтересованными сторонами, такими как сетевые операторы, отраслевые и потребительские группы; при этом следует учитывать отраслевые инициативы и достигнутые соглашения об эффективных и рациональных действиях, которые в минимальной степени затронут права конечных пользователей.

Кроме того, потребители могут быть информированы о своих обязанностях и правах в отношении использования и приобретения устройств ИКТ, а борьба с контрафактными устройствами ИКТ может уменьшить негативное воздействие на все заинтересованные стороны. Необходимо приложить все усилия, чтобы избежать дестабилизации и свести к минимуму возможные недоразумения. Вся предоставленная информация должна быть четко изложена и понятна конечным пользователям.

Требуется также осуществлять действия, направленные на повышение готовности и доступности устройств и снабжение потребителей информацией о преимуществах использования легальных устройств и негативных последствиях, связанных с использованием контрафактной продукции.

9.3 Надежный уникальный идентификатор

Подлинные устройства ИКТ требуют наличия уникальных и постоянных идентификаторов, безопасных (в том смысле, что они не могут быть изменены неавторизованными объектами), уникальных для каждого устройства и присваиваемых уполномоченным лицом или объектом.

Производителям рекомендуется хранить уникальный идентификатор в защищенных элементах оборудования и принимать максимальные меры безопасности для обнаружения несанкционированного доступа к уникальному идентификатору и, как следствие, блокирования устройства до восстановления исходного идентификатора.

Объекту, распределяющему идентификаторы, рекомендуется внедрить механизм, обеспечивающий корректное и безопасное использование этих уникальных идентификаторов.

9.4 Централизованная справочная база данных

Рекомендуется развернуть централизованную справочную базу данных авторизованного оборудования на определенном рынке, основанную на уникальных идентификаторах, что позволит проводить эффективную дифференциацию между подлинными и контрафактными устройствами ИКТ.

При создании этой базы данных следует учитывать нижеследующие аспекты.

– К централизованной базе данных должны иметь доступ надлежащие заинтересованные организации страны, в частности таможенные, полицейские правоохранительные и регулирующие органы. Эти организации должны быть информированы о транзите соответствующих товаров, что позволит им пресекать ввоз, распространение и продажу контрафактных устройств ИКТ на рынке и отслеживать производителей и распространителей контрафакта.

– Централизованная база данных должна стать краеугольным камнем в решении задачи по удалению с рынка уже используемых контрафактных устройств ИКТ.

– Существующие на рынке специальные базы данных могут предоставлять информацию по продукции внутри страны. Некоторые из этих баз данных являются натуральными подмножествами либо даже тем или иным образом связаны с глобальной базой данных.

9.5 Введение режима оценки соответствия

Для эффективного развертывания централизованной национальной справочной базы данных авторизованного оборудования необходимо использовать существующую (или создать новую) надежную схему оценки соответствия (CAS) на основе логотипов и знаков одобрения типа, а также других уникальных идентификаторов, созданных производителями подлинной продукции. Это упростит для всех заинтересованных сторон (например, таможенных органов, потребителей и производителей) дифференциацию между подлинными и контрафактными устройствами.

– Некоторые национальные администрации, региональные и международные организации, частные компании и целый ряд участников рынка ИКТ уже ввели эффективный режим оценки соответствия на местах. Как правило, если речь идет об использовании ИКТ в глобальном масштабе, устройства должны отвечать требованиям комплекса международно признанных стандартов и проходить процедуры оценки соответствия (например, в организациях, признанных МСЭ, – CASC, ISO/CASCO, IECEE CB, GSMA, ФКС, Министерстве инноваций, науки и экономического развития Канады, ANATEL, GCF, PTCRB, ARIB и т. д.).

– Эти организации обладают значительным объемом данных, связанных с контролем продукции, например информация о предприятиях, ответственных за производство и продажу таких продуктов; наборы стандартов и национальных регулярных органов (например, распределение спектра); а также данные о происхождении продукции.

– Существует несколько путей в направлении создания упорядоченного рынка ИКТ. Один из примеров: в соответствии с задачей 4 Программы МСЭ в области C&I были разработаны различные руководящие указания. Портал программы МСЭ в области C&I размещен по адресу https://www.itu.int/ru/ITU-T/C-I/Pages/default.aspx.

9.6 Тесное сотрудничество с таможенными органами и соответствующими национальными организациями

Для эффективного ограничения распространения, импорта и продажи новых контрафактных устройств ИКТ на рынке необходимо установить тесное сотрудничество между органами, ответственными за работу централизованной национальной справочной базы данных, таможенными органами и между таможнями отдельных стран.

– Поскольку таможенные органы и другие соответствующие уполномоченные национальные организации по защите прав потребителей играют важнейшую роль в перехвате контрафактной продукции, в их распоряжение должны быть предоставлены инструменты для выявления контрафактных устройств ИКТ, такие как централизованная национальная справочная база данных.

– В борьбе с незаконной торговлей устройствами ИКТ, включая контрафактные, контрабандные и похищенные устройства, могут использоваться механизмы аутентификации данных отдельного устройства, что позволяет проверять, является ли оно подлинным, если это разрешено законодательством и регуляторными положениями данной страны.

– Должны быть разработаны и полностью задействованы процедуры принятия принудительных мер и связи между различными организациями. Речь может идти об обмене соответствующей информацией, например содержащейся в национальной базе данных устройств ИКТ, в соответствии с национальными, региональными или международными стандартами.

– Рекомендуется, чтобы таможенные органы использовали межправительственную онлайновую платформу для совместного использования информации о продуктах и предупреждений, которые помогают выявлять контрафактное оборудование. Такой платформой является база данных IPM Всемирной таможенной организации [b-WCO-IPM].

9.7 Предоставление информации конечным пользователям перед принятием мер по исправлению ситуации

Требуется информировать потребителей о рисках, связанных с приобретением контрафактных устройств ИКТ, а также о том, что использование поддельных продуктов может быть небезопасным, а их эксплуатационные характеристики будут хуже, чем у подлинных устройств.

Кроме того, потребителям следует четко разъяснять основания для запрета контрафактных устройств ИКТ (такие как угроза безопасности и более низкое качество обслуживания, связанный с этим рост количества жалоб от клиентов, угроза возникновения помех, нарушение прав интеллектуальной собственности (ПИС) и т. д.). Должны проясняться любые возможные спорные и неточные сведения по процедурам, которые могут вызвать негативные последствия на рынке.

При разработке технологических решений для идентификации контрафактных устройств ИКТ рекомендуется предоставлять потребителям инструмент для проверки подлинности продукта.

9.8 Поддержка со стороны действующих национальных нормативно-правовых баз

Перед реализацией тех или иных ограничительных мер по борьбе с контрафактными устройствами ИКТ требуется обеспечить поддержку со стороны действующей национальной нормативно-правовой базы, а именно:

– ограничение активации контрафактных устройств ИКТ в сетях электросвязи;

– ограничение ввоза, оборота и продажи контрафактных устройств ИКТ и аксессуаров на рынке, которые не соответствуют законодательной и нормативной базами страны;

– выработка необходимых решений, касающихся дифференциации между подлинными и контрафактными продуктами для органов власти, потребителей и каналов сбыта;

– усиление мер безопасности, препятствующих производству контрафактной и прочей нелегальной продукции;

– формирование правовой основы для борьбы с подделкой уникальных идентификаторов.

При рассмотрении этого требования следует уделить должное внимание существующим национальным законодательным и нормативным базам, в которых уже могут быть учтены рассматриваемые аспекты.

9.9 Соображения относительно продукции, уже используемой на рынке

Перед принятием тех или иных радикальных мер в отношении контрафактных устройств ИКТ на рынке рекомендуется учитывать необходимость защиты пользователей этой продукции. Это должно смягчить негативные последствия для тех пользователей этих устройств, которые не осведомлены о национальных законодательных или регуляторных положениях или требованиях, связанных с приобретением и использованием контрафактной продукции ИКТ.

Блокирование действующих устройств ИКТ может оказать серьезное и непредсказуемое воздействие на сети различных типов, на конечных пользователей и инфраструктуру. В этом случае одним из решений является применение переходных механизмов, таких как блокирование вначале только новых пользовательских устройств и разрешение на продолжение работы устройств, уже действующих в сети. Однако в конечном счете пользователям все же придется приобретать подлинные устройства.

10 Возможные подходы к решению проблемы контрафактной продукции ИКТ

С учетом изложенных выше требований и на основе информации, представленной в исследованиях конкретных случаев, содержащихся в [b-ITU-T TR-Counterfeit], а также взятых из других источников, далее описываются некоторые подходы к борьбе с контрафактными устройствами ИКТ и соображения, которые следует принимать во внимание при реализации этих решений.

10.1 Запрещение использования недействительных и поддельных идентификаторов устройств

Если для регистрации в сети устройство использует уникальный идентификатор, для контрафактных устройств ИКТ такого рода регистрация может быть запрещена, для чего используется информация из базы данных устройств, авторизованных для работы на определенном рынке.

В подобных случаях, если устройство ИКТ фактически имеет надежный уникальный идентификатор, могут применяться решения, которые:

– блокируют оборудование с недействительными уникальными идентификаторами в своих сетях;

– блокируют использование оборудования, не принадлежащего ни к одному из типов, утвержденных регулятором;

– предотвращают незаконный импорт и продажу этих устройств.

При выборе подобного способа действий рекомендуется также повышать осведомленность потребителей об указанных требованиях. Кроме того, может потребоваться внесение соответствующих изменений в национальное законодательство, как указано в пункте 9.8, выше.

При принятии того или иного решения по борьбе с контрафактными устройствами ИКТ путем обнаружения и блокировки устройств с недействительными уникальными кодами идентификаторов появляются также дополнительные возможности:

– обеспечивать импорт или продажу исключительно легальных устройств, что приведет к увеличению выплат таможенных пошлин и налога на добавленную стоимость;

– бороться с кражей устройств путем регистрации уникальных кодов идентификаторов похищенного оборудования в черном списке по требованию уполномоченных органов;

– обеспечивать защиту потребителя от использования низкокачественного неавторизованного оборудования, которое может представлять опасность для здоровья человека, или же не обеспечивать надлежащее качество услуг (защита реализуется путем внедрения механизма простой проверки легальности оборудования до его покупки).

В процессе стандартизации необходимо соблюдать требования по защите персональных данных и не допускать негативного влияния на пользователей устройств ИКТ со стороны механизмов регистрации идентификаторов. Кроме того, следует обеспечивать защиту потребителей от произвольного отключения от сетей.

Более подробную информацию о возможной реализации решений для мобильных устройств можно найти в Приложении A.

10.2 Сертификация устройств ИКТ и надзор за рынком

Как указано в пункте 9.5, внедрение схемы оценки соответствия (CAS) может помочь при создании национальной справочной базы данных авторизованного оборудования, содержащей список уникальных идентификаторов и дополнительную информацию по устройствам (такую как знаки утверждения, технические и физические характеристики). Таким образом, все заинтересованные стороны (например, таможенные органы, потребители и производители) смогут идентифицировать одобренные устройства.

Кроме того, используя эту информацию, должностные лица таможни могли бы идентифицировать контрафактную продукцию путем введения надзора за рынком и других необходимых принудительных мер. Кроме того, импортеры, в отношении которых имеются сведения об игнорировании правил импорта, могут быть идентифицированы и помещены в особый список. Регуляторные органы могут уведомляться о поставках контрабандных устройств ИКТ, что позволит принять решение о проведении проверок, при которых должно гарантироваться соблюдение законодательства.

Задача системы надзора за рынком используемого оборудования электросвязи как неотъемлемой части политики CAS – обеспечить, чтобы продукция, присутствующая на рынке, не создавала электромагнитных помех, не наносила ущерба сетям электросвязи общего пользования и не угрожала здоровью, безопасности или другим аспектам защиты населения.

На практике надзор за рынком включает в себя любые необходимые действия (например, запрет, изъятие, снятие с продажи продукции), направленные на прекращение распространения устройств, которые не соответствуют требованиям, изложенным в законодательных и регуляторных положениях, на обеспечение соответствия продукции установленным нормам и на применение санкций.

Надзор за рынком жизненно важен для бесперебойного функционирования рынка электросвязи, а также для защиты потребителей и сотрудников от рисков, связанных с продуктами, не соответствующими нормам. Кроме того, надзор за рынком помогает защитить законопослушных предпринимателей от конкуренции со стороны недобросовестных участников рынка, которые игнорируют или пытаются обойти установленные правила.

Многие регуляторные органы во всем мире уже ввели конкретные законодательные требования по организации надзора за рынком. В регуляторных положениях четко излагаются обязанности органов, осуществляющих надзор за рынком, предусматривающие наличие у этих органов необходимых полномочий, ресурсов и информации для надлежащего выполнения своих функций [b-ITU-T-CI-Portal]. Регламентом установлена необходимость введения процедур рассмотрения жалоб, отслеживания конкретных инцидентов, проверки принятия соответствующих мер по исправлению ситуации и сбора научно-технической информации по вопросам безопасности. Кроме того, Государства – Члены МСЭ составляют, внедряют и периодически обновляют национальные программы надзора за рынком, а также регулярно (раз в несколько лет) рассматривают и оценивают собственную деятельность по надзору [b-ITU-D-CI-Guidelines].

В Регламенте ЕС № 765/2008 надзор за рынком определяется как действия, выполняемые уполномоченными органами, и меры, принимаемые ими в целях обеспечения того, чтобы продукция соответствовала требованиям, изложенным в действующем законодательстве, и не ставила под угрозу здоровье, безопасность или какой-либо другой аспект защиты интересов потребителей [b-EC-Regulation].

Таким образом, помимо действий, предпринимаемых в момент появления конкретного продукта на границе страны, рекомендуется проводить дополнительный надзор после поступления его на рынок, что поможет выявлять контрафактные товары и, как следствие, гарантировать, что продукт, продаваемый конечному пользователю, фактически соответствует продукту, представленному в процессе сертификации [b-ITU-D-Rep].

Европейская экономическая комиссия Организации Объединенных наций (ЕЭК ООН) рекомендует координировать процесс надзора за рынком на национальном уровне и таможенную деятельность, а также предоставлять правообладателям возможность информирования органов надзора за рынком о появлении контрафакта [b-UNECE].

10.3 Контроль жизненного цикла устройства

Желательно обеспечивать способность отличать оригинальное устройство ИКТ от клона без ущерба для прав пользователя. В таких клонах обычно используются идентификаторы или другие элементы, обеспечивающие уникальную идентификацию, для того чтобы выдать их за оригинальные устройства.

Одним из возможных решений, помогающим заинтересованным сторонам и гарантирующим подлинность продуктов, может стать развертывание системы контроля жизненного цикла устройства, основанной на уникальных идентификаторах и способной отслеживать устройства ИКТ с начального момента цикла его производства (включая происхождение компонентов, транспортную компанию и розничную торговую точку, в которой устройство будет выставлено на продажу) до момента доставки конечному пользователю.

Эта информация должна быть доступна всем заинтересованным сторонам, с тем чтобы даже в случае клонирования уникальных идентификаторов в контрафактном оборудовании органы власти и сами конечные пользователи смогли проверить подлинность этой информации. Например, если пользователь находится в магазине в какой-либо стране и при проверке уникального идентификатора инструмент показывает, что данный продукт должен продаваться в другом магазине или в другой стране, это должно послужить убедительным доказательством того, что даже несмотря на наличие действительного уникального идентификатора такой продукт является контрафактным.

При использовании данного решения необходимо соблюдать осторожность, если речь идет о перепродаже конечным пользователем бывших в употреблении продуктов. В этом случае национальное законодательство должно учитывать последствия в плане защиты личной информации при определении связи между пользователем и рассматриваемым устройством.

Следует учитывать, что продукт, идентифицированный при таком подходе, может являться не контрафактом, а подлинным продуктом, продаваемым на сером рынке. В таком случае для выявления контрафактного продукта потребуются дополнительные действия.

11 Базовое концептуальное решение

На рисунке 1 представлено предлагаемое концептуальное решение по борьбе с производством, оборотом и использованием контрафактных устройств ИКТ, основанное на общих элементах различных подходов, описанных в разделе 10.

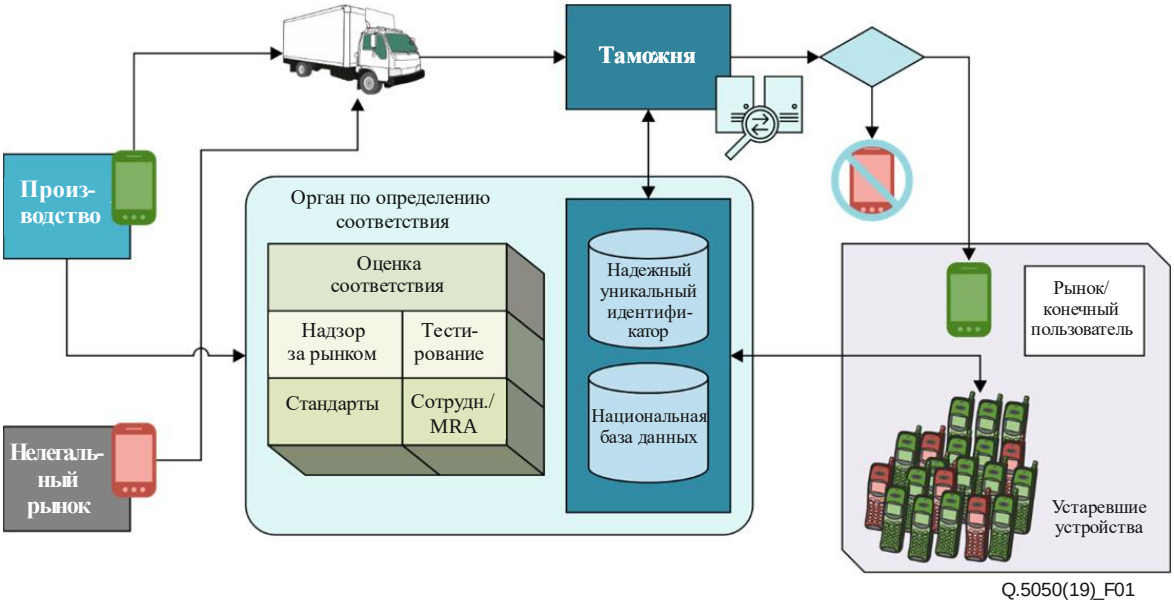

Рисунок 1 – Предлагаемое общее концептуальное решение

Следует организовать взаимодействие различных организаций, ведущих разнообразную деятельность и управляющих информационными системами, в целях контроля и получения информации, важной для выявления контрафактных и поддельных устройств и борьбы с их использованием.

Законопослушные коммерческие структуры позволяют проводить проверку соответствия поступающего в страну продукта нормам и имеют представителей, ответственных за оборудование.

При поступлении продукции в пункт контроля учреждение (например, таможня) проверяет все правовые аспекты таких устройств, включая соответствие устройств действующим регуляторным и сертификационным требованиям, таким как распределение радиочастот, безопасность, совместимость и т. д. Кроме того, в отношении устройств, включенных в белый список[1], также могут проводиться проверки, позволяющие убедиться в том, что импортируемым устройствам законно присвоены идентификаторы и что марка и модель проверяемого устройства соответствуют данным, записанным при выдаче идентификаторов.

В то же время неавторизованной продукции, в частности контрафактным устройствам, вход на рынок закрыт. Сотрудники организаций используют в работе действующий режим оценки соответствия, а также базу данных с информацией о том, что должно находиться в импортируемых контейнерах.

Такие инвентарные базы данных могут также использоваться при проведении действий принудительного характера в отношении оборудования, попадающего на рынок (как легального, так и контрафактного).

---

[1] Например, глобальная база данных TAC GSMA может использоваться в целях содействия при составления белого списка устройств, соответствующих требованиям 3GPP.

Приложение A

Решения для мобильных устройств

(Данное Приложение является неотъемлемой частью настоящей Рекомендации)

При работе с мобильными устройствами, соответствующими стандарту 3GPP, применяют решения по идентификации подлинных и легально импортируемых мобильных терминалов, основанные на системе регистрации международных идентификаторов мобильного оборудования (IMEI). В решениях по предотвращению распространения контрафактных мобильных устройств, основанных на IMEI, используются нижеследующие методы:

– блокировка в сетях мобильных устройств с недействительными номерами IMEI (например, не имеющих IMEI, с нулевыми IMEI, с IMEI, включающими строки нестандартного формата, с дублирующими IMEI, с IMEI, присвоенными неавторизованными организациями, а также с действительными IMEI, которые еще не присвоены авторизованной организацией[2]);

– выполнение других действий по информированию потребителей, принятие мер принудительного характера и соответствующие изменения законодательства на национальном уровне.

Для блокировки использования контрафактных мобильных устройств данная система может быть развернута на основе реестра действительных кодов IMEI (идентификатор, соответствующий стандартам, официально присваиваемый уполномоченной организацией, легально импортируемым устройствам, прошедшим одобрение типа или проверку на соответствие требованиям) мобильных устройств, которые активно используются в национальных сетях. Регистрация IMEI мобильных устройств обеспечивает, чтобы мобильные устройства соответствовали национальным регуляторным положениям, а в некоторых странах – чтобы они были импортированы легально.

- **Справочные базы данных**

Коды IMEI используются для создания базы данных с белым списком, серым списком и черным списком устройств. Белый список – это реестр устройств, разрешенных для использования в стране (например, устройств, легально импортированных или изготовленных в этой стране); серый список – это реестр устройств с неподтвержденным статусом (не внесенных ни в белый список, ни в черный список); черный список – это реестр устройств, обслуживание которых в сети электросвязи должно быть запрещено.

Необходимо провести предварительный анализ того, какие последствия в отношении сетей и пользователей может иметь применение белых, серых и черных списков, поскольку они могут ограничивать перемещение устройств между странами, а также оказывать влияние на иностранных посетителей и операторов сетей.

Серый список и черный список генерируются автоматически путем обработки данных из белого списка и данных, полученных от операторов, импортеров и таможенных органов.

- **Интеграция с сетью оператора**

Для обеспечения активного взаимодействия с системой регистрации операторам электросвязи необходимо поддерживать регистры идентификаторов оборудования (EIR), а также производить регулярную синхронизацию и автоматический обмен данными между EIR и базой данных кодов IMEI (например, на ежедневной основе).

При первом подключении и регистрации мобильного телефона в сети оператора код IMEI терминала пересылается оператором мобильной связи в базу данных. Рассматриваемая система показывает коды IMEI, которые не внесены в белый список, выявляет контрафактные мобильные устройства и регистрирует соответствующие коды IMEI в сером списке. Владелец соответствующего пользовательского устройства получает СМС-уведомление и должен подтвердить легальное происхождение устройства в течение указанного периода после даты внесения в серый список.

---

[2] Для проверки незаконно присвоенных или клонированных IMEI для устройств, совместимых с 3GPP, может использоваться глобальная база данных TAC GSMA.

Необходимо обеспечить надежность и безопасность системы регистрации и связанных с ней процессов. Доступ к базе данных обычно предоставляется регуляторным и таможенным органам, сетевым операторам и широкому кругу лиц с использованием соответствующих привилегий на доступ. Пользователи должны иметь доступ к этой базе данных в целях проверки того, разрешено ли мобильному устройству работать в стране (как правило, путем отправки СМС-сообщения или при помощи веб-страницы).

Важно отметить, что СМС следует рассматривать как незащищенное средство связи с клиентом, которое могут использовать мошенники, поэтому могут потребоваться дополнительные меры.

- **Обнаружение клонированных IMEI**

Поскольку возможна подделка уникальных идентификаторов некоторых устройств и существует вероятность того, что распространители контрафакта будут клонировать IMEI обычных устройств, чтобы избежать проверки системой, необходимо принять дополнительные меры для идентификации и борьбы с поддельными устройствами, имеющими клонированные легальные IMEI.

Одним из возможных решений является внедрение баз данных с дополнительной информацией о продукте, которая может быть полезна для проверки соответствия продукта, использующего идентификаторы, другим атрибутам. Указанные инструменты могут быть реализованы при помощи режима оценки соответствия, когда эта информация собирается в ходе процесса сертификации устройства и хранится в базе данных, доступной для всех заинтересованных сторон.

- **Дополнительные соображения**

Кроме того, решение для борьбы с контрафактными мобильными устройствами путем выявления и блокировки мобильных устройств с недействительными или поддельными кодами IMEI может оказаться полезным для:

– блокировки незаконного импорта этих устройств и, следовательно, обеспечения того, чтобы мобильные устройства импортировались и продавались на законных основаниях, благодаря чему могут увеличиться выплаты таможенных пошлин и налога на добавленную стоимость;

– борьбы с кражей мобильных телефонов путем внесения кодов IMEI украденных пользовательских устройств в черный список по запросу правоохранительных органов, благодаря чему такие кражи становятся бесполезными (аналогичная процедура может быть применена к блокировке телефонов по просьбе владельцев утерянных мобильных устройств);

– блокировки оборудования, тип которого не имеет одобрения регуляторного органа; эта мера обеспечивает защиту потребителей от использования мобильных устройств низкого качества, которые могут быть неавторизованными или опасными для здоровья, а также не обеспечивают надлежащее качество услуг подвижной связи (защита обеспечивается путем внедрения метода для простой проверки легальности мобильного телефона до его покупки).

Важно придерживаться подхода, согласованного на национальном уровне, поскольку контрафактные устройства ИКТ могут присутствовать в нескольких сетях, и в процессе обнаружения должна учитываться эффективность мер, которые необходимо принять во избежание нежелательных последствий для пользователей, дублирования действий или конфликтов между различными операторами подвижной связи.

Необходимо выполнять диагностику на ранних этапах (определение масштабов проблемы недействительных идентификаторов, клонирование и т. д.), планировать процесс обнаружения и контроля, распределять требуемые ресурсы (деньги, персонал, время) и анализировать воздействие на конечных пользователей в целях его снижения. Результаты должны обсуждаться со всеми заинтересованными сторонами, что позволит выполнить указанные выше решения.

Следует также учитывать, что в некоторых случаях подобные механизмы могут вызывать у легальных пользователей, включая путешественников и туристов, проблемы следующего характера.

– Иностранец, посещающий страну и использующий местную карту, содержащую модуль идентификации абонента (SIM-карту) в своем устройстве, может попасть в ловушку, связанную с белым списком, в результате чего не сможет пользоваться своим устройством.

– Приезжающий пользователь, находящийся в роуминге, который продолжает задействовать свое устройство в течение нескольких месяцев, также может быть несправедливо исключен из местного белого списка по истечении определенного периода.

– Сообщение о регистрации может быть отправлено приезжающему пользователю в стране, где он применяет местную SIM-карту, однако он может не говорить на местном языке и не прочитает сообщение. Таким образом данный пользователь не пройдет регистрацию, а его устройство будет занесено в черный список. Это может привести или i) к отключению приезжающего пользователя от локальной сети; или ii) к занесению его легального устройства в черный список в других странах в рамках договоренностей о совместном доступе к информации, несмотря на то что устройство является полностью легальным.

Таким образом, если механизмы недостаточно проработаны, они могут вызывать проблемы, и такие сценарии должны предотвращаться в процессе разработки. И наконец, данная функция не должна использоваться для произвольного отключения пользователей от сетей по другим причинам.

Дополнение I

Другие отраслевые решения

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

Отраслевые предприятия вносят значительный вклад в решение проблемы контрафактного оборудования и повышения надежности оборудования и доверия к компаниям. Благодаря отраслевым усилиям ведется разработка решений, позволяющих повысить безопасность цепочки поставок. Решение проблемы контрафактного оборудования не является единственной целью этих усилий. Отрасль также должна сотрудничать с правительственными организациями, в частности с правоохранительными и таможенными органами для принятия мер принудительного характера. Результаты этих усилий целесообразно рассматривать как инструментарий, который компании будут использовать исходя из необходимости и конкретных обстоятельств (например, продукции, рыночных условий и т. д.).

Следует отметить, что отраслевая деятельность по борьбе с контрафактными продуктами охватывает очень широкий спектр продукции с различными цепочками поставок, причем некоторые из них имеют разные потребности. Это подразумевает наличие сложных схем взаимодействия нескольких участников. Помимо вышеуказанной внешней деятельности компании ведут конфиденциальные служебные исследования и разработку способов борьбы с контрафактной продукцией.

Ниже приведен неполный обзор некоторых мер по повышению безопасности устройств, которые могут помешать изготовлению контрафактной продукции.

- **База данных IMEI GSMA**

IMEI представляет собой 15-значный номер, который используется для идентификации устройства в сети подвижной связи. Первые 8 цифр IMEI – это код распределения типов (TAC), идентифицирующий конкретную модель.

Ассоциация глобальной системы подвижной связи (GSMA) поддерживает глобальную базу данных, которая содержит информацию о конкретных TAC, которые присваиваются устройствам, совместимым с 3GPP. Эта база данных называется базой данных IMEI.

Эта база данных может использоваться следующим образом.

– Идентификация контрафактных устройств ИКТ может выполняться в сотрудничестве с производителем подлинного оборудования, который может быть идентифицирован при помощи списка из базы данных TAC GSMA.

– Доступ к базе данных TAC GSMA может предоставляться государственным организациям, таким как министерства, регуляторные, таможенные и правоохранительные органы, для получения информации о происхождении и технических характеристиках мобильных устройств. Эта информация может использоваться для выявления нарушений и идентификации производителя устройства, который не может подтвердить, что его устройство является подлинным.

– Подлинность производимых мобильных устройств и их IMEI могут быть проверены при помощи базы данных TAC GSMA. Таможенные и правоохранительные органы могут использовать справочную службу GSMA для проверки серийного номера сертификата TAC, предоставленного производителем. Это второй серийный номер, связанный с каждым TAC. Несоответствие этих идентификаторов говорит о том или ином виде фальсификации идентификатора.

– Регуляторные органы могут использовать базу данных TAC GSMA для обеспечения того, чтобы характеристики мобильных устройств, тестируемых для оценки соответствия, совпадали с характеристиками модели, указанными в базе данных.

База данных IMEI GSMA: https://imeidb.gsma.com/imei/index

Услуги IMEI GSMA: https://www.gsma.com/services/tac-allocation/the-imei-database/

- **Система идентификации, регистрации и блокировки устройств**

Система идентификации, регистрации и блокировки устройств (DIRBS) – это серверная программная платформа, предназначенная для борьбы с контрафактными, нелегальными и украденными мобильными устройствами в стране. Программная платформа DIRBS доступна в качестве открытого источника и предназначена для оказания помощи государственным учреждениям, регуляторным органам и другим структурам в их усилиях по борьбе с ненадлежащим использованием контрафактных, нелегальных и украденных устройств в сотовых сетях. Платформа соответствует рекомендациям Международного союза электросвязи по обращению с нелегальными и не имеющими одобрения типа устройствами в стране.

DIRBS состоит из базы данных об устройствах на национальном уровне, которая взаимодействует на разных уровнях с операторами, местными производителями, импортерами, потребителями, таможенными и правоохранительными органами, а также глобальной базой данных IMEI GSMA. Платформа DIRBS состоит из механизма анализа и связанных с ним подсистем, которые обеспечивают информацию для разрешения блокировки контрафактных и фальсифицированных устройств; реальная блокировка определяется правилами, действующими в конкретной стране, и осуществляется через механизмы регистра идентификаторов оборудования (EIR) оператора.

Более подробная информация представлена по адресу www.qualcomm.com/dirbs.

- **Компания Trusted Computing Group**

Компания Trusted Computing Group (TCG – Группа по доверенным вычислениям) – некоммерческая организация, созданная для разработки, определения и продвижения открытых, независимых от поставщиков глобальных отраслевых стандартов, поддерживающих основанный на аппаратных средствах доверительный подход для функционально совместимых доверенных вычислительных платформ.

Наряду с другими стандартами TCG разработала спецификацию для модуля доверенной платформы (TPM), актуальную для данной области:

http://www.trustedcomputinggroup.org/resources/tpm_main_specification

http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

Как отмечено на вышеупомянутом веб-сайте, TPM представляет собой компьютерную микросхему (микроконтроллер), в защищенном режиме хранящую артефакты, используемые для аутентификации платформы (ПК или ноутбука). Эти артефакты могут включать в себя пароли, сертификаты или ключи шифрования.

Данный механизм позволяет проводить как локальную, так и удаленную аттестацию, которая облегчает доверительное отношение к установлению подлинности оборудования.

TCG также создала рабочую группу Embedded Systems для решения проблем защиты встроенных систем, включая интернет вещей (IoT):

http://www.trustedcomputinggroup.org/developers/embedded_systems

- **Глобальная платформа**

Глобальная платформа разработала стандарты для доверенной среды исполнения (TEE), принятой в современных мобильных устройствах в качестве метода безопасного хранения и исполнения конфиденциальных кодов и других средств обеспечения безопасности.

Более подробная информация представлена по адресу https://www.globalplatform.org/specificationsdevice.asp.

- **ОТК1/ПК27 ИСО/МЭК**

Сфера деятельности ПК27 имеет большое значение для деятельности отрасли, связанной с безопасностью и смягчением последствий использования контрафактной продукции, а также для разработки стандартов защиты информации и ИКТ. В нее входят общие методы, технологии и руководящие указания для решения вопросов обеспечения безопасности и защиты личной информации.

Наряду с прочими документами ПК27 опубликовал стандарты, касающиеся контрафактного оборудования, такие как:

– [b-ISO/IEC 15408]: *Information technology – Security techniques – Evaluation criteria for IT security" (Common Criteria)*;

– [b-ISO/IEC 27034] *Information Technology – Security Techniques – Application Security*;

– [b-ISO/IEC 27036-3]: *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*;

– [b-ISO/IEC 20243]: *Information Technology – Open Trusted Technology Provider TM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*.

Более подробная информация представлена по адресу http://www.din.de/en/meta/jtc1sc27.

• **Форум Open Group Trusted Technology Forum**

Форум Open Group Trusted Technology Forum (OTTF) проводит разработку глобальной программы и структуры целостности цепочек поставок в целях предоставления покупателям ИТ-продуктов широкого выбора аккредитованных технических партнеров и поставщиков. Следует отметить, что указанный выше стандарт [b-ISO/IEC 20243] был впервые разработан форумом Open Group.

Более подробная информация представлена по адресу http://www.opengroup.org/getinvolved/forums/trusted.

• **Институт инженеров по электротехнике и радиоэлектронике**

Институт инженеров по электротехнике и радиоэлектронике (IEEE) разработал стандарт для идентификации безопасных устройств и метод криптографической привязки идентификатора к устройству, например IEEE 802.1ar: Standard for Local and Metropolitan Area Networks: Secure Device Identity.

Как указано на веб-сайте IEEE: "Данный стандарт определяет идентификаторы безопасных устройств (DevID), предназначенные для использования в качестве учетных данных для аутентификации совместимых безопасных устройств с помощью расширяемого протокола аутентификации (EAP) и других протоколов аутентификации и обеспечения безопасности отраслевого стандарта. Стандартизованный идентификатор устройства облегчает аутентификацию совместимых безопасных устройств и упрощает ввод в эксплуатацию безопасных устройств и управление ими".

Более подробная информация представлена по адресу http://www.ieee802.org/1/pages/802.1ar.html.

• **Другие виды отраслевой деятельности, связанные с контрафактной продукцией**

ICC – Бюро по борьбе с контрафактной продукцией

http://www.iccwbo.org/products-and-services/fighting-commercial-crime/counterfeiting-intelligence-bureau/

ICC – Бизнес в борьбе с контрафактом и пиратством (BASCAP)

http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/Welcome-to-BASCAP/

Библиография

[b-ITU-T-CI-Portal] На портале МСЭ по вопросам соответствия и функциональной совместимости в рамках задачи 4 представлена обновленная информация о нормативно-правовых базах стран в этой области. http://www.itu.int/en/ITU-T/C-I/Pages/default.aspx.

[b-ITU-T TR-Counterfeit] Технический отчет "Контрафактные устройства ИКТ" (2015 год.)

[b-IEEE 802.1] IEEE 802.1 (2009), *Standard for Local and Metropolitan Area Networks: Secure Device Identity.* http://www.ieee802.org/1/pages/802.1ar.html

[b-ISO/IEC 15408-1] ISO/IEC 15408-1:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.*

[b-ISO/IEC 17000] ISO/IEC 17000:2004, *Conformity assessment – Vocabulary and general principles.*

[b-ISO/IEC 20243] ISO/IEC 20243:2015, *Information Technology – Open Trusted Technology Provider TM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products.*

[b-ISO/IEC 27034] ISO/IEC 27034:2011, *Information technology – Security techniques – Application security.*

[b-ISO/IEC 27036-3] ISO/IEC 27036-3:2013, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security.*

[b-EC-Regulation] Market Surveillance Regulation EC no. 765/2008.

[b-Gartner] https://www.gartner.com/it-glossary/gray-market

[b-ITU-D-CI-Guidelines] ITU Guidelines on Establishing conformity and interoperability regimes: Complete Guidelines (2015), ITU. http://www.itu.int/en/ITU-D/Technology/Documents/ConformanceInteroperability/publications/Establishing_Conformity_and_interoperability_Regimes-E.pdf.

[b-ITU-D-Rep] Заключительный отчет по Вопросу 4/2. Вопрос 4/2: Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость. Исследовательские комиссии МСЭ-.D, 2017 год. https://www.itu.int/pub/D-STG-SG02.04.1-2017

[b-OECD] 2017 OECD report "Trade in Counterfeit ICT Goods".

[b-TRIPS Agreement] Торговые аспекты прав интеллектуальной собственности; приложение к Марракешскому соглашению о создании Всемирной торговой организации, подписанному в Марракеше, Марокко, в апреле 1994 года.

[b-UNECE] Рекомендация M. Использование инфраструктуры надзора за рынком в качестве дополнительного инструмента защиты потребителей и пользователей от контрафактной продукции. http://www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_M.pdf.

[b-WCO-IPM] IPM Всемирной таможенной организации. http://www.wcoipm.org/.

[b-WTO-TBT] Всемирная торговая организация – Соглашение ВТО о технических барьерах в торговле.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие 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	Оконечное оборудование, субъективные и объективные методы оценки
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 протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии,
Женева, 2019 год