Международный союз электросвязи

МСЭ-Т Технический отчет МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(21 ноября 2014 г.)

Контрафактное оборудование ИКТ

Краткое содержание

Контрафакция повсеместно признается в качестве одной из значительных и растущих социально-экономических проблем. В настоящем Техническом отчете представлена базовая информация о природе вопросов, связанных с контрафакцией оборудования информационно-коммуникационных технологий (ИКТ), приводится обзор международных конвенций, регулирующих этот вид нарушения прав интеллектуальной собственности, и деятельности организаций, обеспечивающих соблюдение этих прав, а также дается описание целого ряда средств борьбы с торговлей контрафактными продуктами. Кроме того, в Приложении А описан ряд национальных и региональных инициатив, направленных на борьбу с контрафакцией мобильных устройств.

Ключевые слова

Контрафактный, некачественный.

Регистрационный номер

QSTR-COUNTERFEIT.

Журнал регистрации изменений

Настоящий отчет является версией 1 Технического отчета МСЭ-Т "*Контрафактное оборудование ИКТ*", утвержденного на собрании Рабочей группы 3 (РГ3) 11-й Исследовательской комиссии МСЭ-Т, которое проходило в Женеве 21 ноября 2014 года.

Редактор: Кит Мейнуэринг
ИСООН
Тел.: +46 76 107 6877
Эл. почта: keith.mainwaring@ukrainesystems.com

Содержание

			Стр.
1		Введение: контрафакция продуктов – растущая проблема	6
2		Что такое контрафакция?	8
3		Воздействие контрафактного оборудования ИКТ и его компонентов	8
	3.1	Примеры контрафактного оборудования ИКТ	9
4		Конвенции по правам интеллектуальной собственности (ПИС)	12
	4.1	Парижская конвенция по охране промышленной собственности и Бернская конвенция по охране литературных и художественных произведений	12
	4.2	Аспекты прав интеллектуальной собственности, связанные с торговлей (ТРИПС), Всемирной торговой организации (ВТО)	12
5		Обеспечение ПИС	14
	5.1	Всемирная организация интеллектуальной собственности (ВОИС)	14
	5.2	Всемирная торговая организация – Совет по ТРИПС	14
	5.3	Управление ООН по контролю над наркотиками и предупреждению преступности (УНП ООН)	14
	5.4	Всемирная таможенная организация (ВТАО)	15
	5.5	Европейский союз	16
	5.6	Интерпол	16
	5.7	Европейская экономическая комиссия Организации Объединенных Наций (ЕЭК ООН)	16
	5.8	Национальные инициативы (несколько примеров)	17
6		Промышленные форумы по борьбе с контрафакцией	17
	6.1	Международная торговая палата (МТП)	17
	6.2	Международная коалиция по борьбе с контрафакцией (IACC)	18
	6.3	Форум производителей мобильного оборудования (MMF)	18
	6.4	Международная ассоциация дилеров по продаже услуг и компьютеров и Североамериканская ассоциация дилеров в области электросвязи (AscdiNatd)	18
	6.5	Альянс за сокращение "серого" рынка и контрафакции (AGMA)	18
	6.6	Рабочая группа по борьбе с контрафакцией Британской ассоциации производителей электротехнического и смежного оборудования (BEAMA)	18
	6.7	UKEA (Альянс электронной промышленности Соединенного Королевства)	19
	6.8	Группа по борьбе с контрафакцией (ACG)	19
	6.9	UNIFAB − Союз производителей	19
	6.10	Международная инициатива в области производства электронного оборудования (iNEMI)	19
7		Меры по борьбе с контрафактным оборудованием	19
	7.1	Введение	19
	7.2	Злоупотребление идентификаторами и знаками утверждения типа	22
	7.3	Международный идентификатор аппаратуры подвижной связи (IMEI)	22
	7.4	Уникальные идентификаторы	25
	7.5	Автоматическая идентификация и сбор данных (AIDC)	28

7.6 Конфиденциальная печать и голографическая маркировка 33
7.7 Управление цепочкой поставок..... 33
7.8 Тестирование..... 34
7.9 Базы данных 35
7.10 Изучение рынка 35

8 Организации по стандартам 35

9 Руководящие указания по борьбе с контрафакцией 36

10 Выводы..... 38

11 Участие МСЭ..... 40

12 Справочные материалы 43

Приложение А: Системы для определения контрафактных мобильных устройств 51
А.1: Примеры мер, принятых национальными администрациями и регуляторными органами..... 51
А.2: Примеры совместных мер, принятых на региональных уровнях 68

Список рисунков

Стр.

Рисунок 1: Пример защищенной метки, требуемой Anatel и определенной в ее резолюции 481/2007 20

Рисунок 2: Экосистема оценки соответствия 21

Рисунок 3: Процедура, известная под названием tropicalização (по-португальски "подготовка для работы в тропических условиях") 22

Рисунок 4: Формат IMEI 23

Рисунок 5: Формат uCode 27

Рисунок 6. Функциональная архитектура для доступа к мультимедийной информации, инициируемого посредством идентификации на основе маркеров (Рекомендация МСЭ-Т H.621) 28

Рисунок 7: Примеры линейных штрих-кодов 28

Рисунок 8: Примеры матричных (двумерных) штрих-кодов 29

Рисунок 9: Формат маркера ID стандарта 15963 ИСО/МЭК 30

Рисунок 10: Классы эмитентов уникальных TID 30

Рисунок 11:Пример эмблемы RFID, указанной в стандарте 29160 ИСО/МЭК 31

Рисунок 12: Обзор стандартов EPCglobal [59] 32

Рисунок 13: Элементы системы управления безопасностью стандарта ИСО 28000. 33

Рисунок 14: Защита прав интеллектуальной собственности (на основе комплекта материалов, подготовленного Групой Соединенного Королевства по преступности, связанной с IP [75]) 38

Рисунок A.1: Решение в области центральной базы данных EIR IMEI в Египте 54

Рисунок A.2: Структура центрального регистра идентификации оборудования [на основе ежегодного отчета о деятельности за 2010 год: https://www.icta.mu/mediaoffice/publi.htm] 59

Рисунок A.3: Функции AISMTRU 63

Рисунок A.4: Общая база данных EIR и IMEI 64

Рисунок A.5: Сервер синхронизации 65

Рисунок A.6: Система всесторонней защиты информации (CIPS) AISMTRU 66

Рисунок A.7: Последствия внедрения AISMTRU на Украине 67

Технический отчет МСЭ-Т

Контрафактное оборудование ИКТ

Краткое содержание

Контрафакция повсеместно признается в качестве одной из значительных и растущих социально-экономических проблем. В настоящем Техническом отчете представлена базовая информация о природе вопросов, связанных с контрафакцией оборудования информационно-коммуникационных технологий (ИКТ), приводится обзор международных конвенций, регулирующих этот вид нарушения прав интеллектуальной собственности, и деятельности организаций, обеспечивающих соблюдение этих прав, а также дается описание целого ряда средств борьбы с торговлей контрафактными продуктами. Кроме того, в Приложении A описан ряд национальных и региональных инициатив, направленных на борьбу с контрафакцией мобильных устройств.

1 Введение: контрафакция продуктов − растущая проблема

Накапливается все больше свидетельств тому, что распространение контрафактных продуктов, хотя его очень сложно измерить, представляет собой растущую проблему с точки зрения как масштабов, так и диапазона затрагиваемых продуктов. В 2008 году ОЭСР [1] опубликовала отчет, в котором на основе произведенных таможней конфискаций общий объем международной торговли контрафактными и пиратскими товарами (не включая цифровые продукты или продукты, произведенные и потребляемые на внутреннем рынке) в 2005 году оценивался более чем в 200 млрд. долл. США. Эта оценка обновлялась на основе роста и изменяющейся структуры международной торговли с немногим более 100 млрд. долл. США в 2000 году до 250 млрд. долл. США в 2007 году, что составляет 1,95% мировой торговли [2]. Некоторые оценки даже выше: Бюро по борьбе с контрафактной продукцией Международной торговой палаты (МТП) оценивает, что на контрафакцию приходится 5−7% мировой торговли в объеме 600 млрд. долл. США в год [3].

Группа МТП "Бизнес в борьбе с контрафактом и пиратством" (BASCAP) поручила провести исследование [4], чтобы дополнить приведенную ОЭСР картину экономического и социального воздействия контрафакции и пиратства. В настоящем отчете общая экономическая стоимость контрафактных и пиратских продуктов в мире оценивается в размере 650 млрд. долл. США в год, при этом на международную торговлю приходится более половины этой стоимости (от 285 млрд. долл. США до 360 млрд. долл. США), на внутреннее производство и потребление − от 140 млрд. долл. США до 215 млрд. долл. США, а на цифровой контент (музыка, фильмы и программное обеспечение) − от 30 млрд. долл. США до 75 млрд. долл. США. Кроме того, по оценкам, контрафакция и пиратство обходятся правительствам и потребителям стран "большой двадцатки" более чем в 125 млрд. долл. США ежегодно (в связи с такими факторами, как уменьшенные налоговые поступления и увеличенные расходы на внедрение контрмер и на медицинский контроль), а также приводят к потере примерно 2,5 млн. потенциальных рабочих мест.

Национальные таможенные органы Европейского союза (ЕС) зарегистрировали за 2005−2010 годы трехкратный рост поступающих в ЕС контрафактных товаров. Статистические данные, опубликованные Европейской комиссией в июле 2011 года, показывают огромную тенденцию к росту количества поставок с подозрением на нарушение прав интеллектуальной собственности (ПИС). Таможенные органы зарегистрировали в 2010 году около 80 тыс. таких случаев, а с 2009 года эта цифра практически удвоилась. На внешних границах ЕС было задержано более 103 млн. поддельных продуктов. http://trade.ec.europa.eu/doclib/docs/2012/january/tradoc_149003.pdf

Контрафакция охватывает огромный диапазон продуктов − продукты питания и напитки, фармацевтические продукты, электрооборудование и автомобильные детали, все виды потребительских товаров и даже материальные средства в целом. Контрафакция распространяется на компьютерные компоненты (мониторы, корпуса, жесткие диски), компьютерное оборудование, маршрутизаторы, веб-камеры, пульты дистанционного управления, мобильные телефоны, телевизоры (ТВ), проигрывающие устройства компактных дисков (CD) и универсальных цифровых дисков (DVD), громкоговорители, камеры, наушники, адаптеры универсальной последовательной шины (USB), программное обеспечение, сертификаты, сертификационные знаки и данные (такие как биометрические данные).

Кроме того, для цифрового пиратства и в качестве рынка для контрафактных товаров все чаще используется интернет. Все факторы, которые делают интернет привлекательным ресурсом для розничных продавцов, особенно тех из них, которые нацелены на узкие рынки (глобальный охват рынка, легкость создания, перемещения и закрытия веб-сайтов, которые могут быть сделаны весьма привлекательными и убедительными, и дешевая рассылка электронной почты), наряду с возможностью сохранять анонимность, приводят к тому, что интернет становится привлекательным для продавцов контрафактных товаров. А огромное количество сайтов в интернете делают весьма сложным для владельцев прав интеллектуальной собственности и правоприменительных органов определение незаконных операций. Назойливая электронная почта, сайты по электронной торговле и аукционам − все они используются в попытках продать контрафактные товары.

В том что касается отрасли ИКТ, по оценкам, приведенным в отчете KPMG и AGMA, от 8% до 10% всех продаваемых в мире товаров отрасли информационных технологий (ИТ) являются контрафактными, а в 2007 году контрафакция привела к потерям доходов в отрасли ИТ в размере 100 млрд. долл. США. Одна лишь компания Hewlett-Packard провела в период между 2005 и 2009 годами более 4620 расследований в 55 странах, что привело к конфискации контрафактных печатных средств более чем на 795 млн. долл. США [6]. В 2011 году на бытовую электронику приходилось 22% конфискованных таможней США товаров, при этом стоимость товаров увеличилась на 16% по сравнению с 2010 годом. Около трети товаров этой категории − мобильные телефоны [5].

В 2011 году мировой рынок контрафактных мобильных телефонов оценивался в размере 250,4 млн. телефонов (http://press.ihs.com/press-release/design-supply-chain/cellphone-gray-market-goes-legit-sales-continue-decline). Это соответствует примерно 16% из общего количества проданных в 2011 году 1546 млн. радиотелефонных трубок [8]. Эти данные аналогичны оценке степени проникновения контрафактной продукции на рынок мобильных телефонов, приведенной в подготовленном в 2011 году для Европейской комиссии исследовании интернационализации и фрагментации цепочек создания стоимости и безопасности поставок, согласно которой на контрафактные мобильные телефоны приходится 15−20% мирового рынка в аспекте проданных единиц продукции и около 9 млрд. долл. США доходов.

В добавок к производству контрафактных устройств, контрафактные электронные компоненты включаются в цепочки поставок законной продукции. Использование контрафактных электронных компонентов в военном оборудовании США вызвало сенсацию в конце 2011 года, когда в Сенатской комиссии по делам вооруженных сил заслушивался вопрос о контрафактных электронных компонентах в цепочках поставок Министерства обороны [9]. По оценкам исследования, проведенного Бюро промышленности и безопасности Министерства торговли [10], было около 1800 случаев включения контрафактных электронных компонентов в цепочки поставок контрактов на производство военной продукции, охватывающих более миллиона компонентов. Кроме того, было обнаружено, что количество инцидентов возросло с 3868 в 2005 году до 9356 в 2008 году. В результате этого слушания в Закон о полномочиях в сфере национальной обороны (NDAA) 2012 года включено руководство по борьбе с контрафактными компонентами, включая проведение дополнительных проверок импортированных электронных компонентов, а также на подрядчиков возложена полная ответственность за обнаружение поддельных компонентов и исправление любых случаев, когда поддельные компоненты попали в продукты [11].

Проведенное ОЭСР в 2008 году исследование показало, что большая часть контрафактных продуктов происходит из одной азиатской страны (на которую приходится 69,7% конфискованных контрафактных продуктов).

Настоящий Технический отчет предназначен для представления базовой информации о проблеме контрафакции и путях ее решения, при этом акцент делается на контрафакции оборудования ИКТ и на инструментах ИКТ, которые могут использоваться для смягчения этой проблемы.

Помимо контрафактных устройств также наблюдается распространение оборудования и аксессуаров ИКТ, которые обычно называют "некачественными" или "неразрешенными". Хотя и не имеется общепринятого стандартного определения этих терминов, в таких устройствах часто используются компоненты низкого качества и в большинстве случаев они не соответствуют применимым национальным юридическим требованиям, касающимся сертификации, утверждения, распространения и продажи мобильных устройств. Такие устройства не всегда сопряжены с нарушением прав интеллектуальной собственности производителей устройств, и поэтому они не подпадают под принятое определение "контрафакции"; следовательно, они не попадают в сферу

охвата настоящего Технического отчета, который посвящен контрафактным устройствам. "Некачественные" устройства создают и представляют собой определенный набор проблем и средств их решения, что требует отдельного рассмотрения.

2 Что такое контрафакция?

В Соглашении ВТО по аспектам прав интеллектуальной собственности, связанным с торговлей (ТРИПС), контрафактные товары с товарным знаком определяются как "любые товары, включая упаковку, на которых самовольно обозначен товарный знак, который идентичен товарному знаку, зарегистрированному в установленном порядке для таких товаров, или который по его основным аспектам нельзя отличить от такого товарного знака и который вследствие этого нарушает права владельца данного товарного знака согласно законодательству страны импорта" (сноска 14 к Статье 51). Поэтому термин "контрафакция" используется в Соглашении ТРИПС только в сфере товарных знаков. Он относится к контрафактной продукции, которая определяется более точно, чем нарушения, связанные с товарным знаком, на основе того, что товарный знак идентичен или практически неотличим от оригинала. Данный текст не касается намерений, с которым использовался контрафактный товарный знак. В этом тексте контрафактный продукт определяется в аспекте того, насколько точно повторяется знак, используемый для зарегистрированного продукта и применяемый к таким же товарам, как и товары, для которых зарегистрирован товарный знак. На практике, такая контрафактная продукция обычно включала бы случаи буквального копирования знака с намерением создать видимость того, что обозначен подлинный продукт. Такие случаи обычно подразумевают намерение обмануть, поскольку введение в заблуждение относительно подлинного продукта и его копии является преднамеренным.

В этой же сноске к Соглашению ТРИПС пиратские товары, охраняемые авторским правом, определяются как "любые товары, которые являются копиями, произведенными без согласия правообладателя или лица, должным образом уполномоченного правообладателем, в стране производства и которые произведены прямо или косвенно на основе изделия, изготовление копии которого являлось бы нарушением авторского права или связанного с ним права согласно законодательству страны импорта". Таким образом, в Соглашении ТРИПС термин "пиратство" относится к нарушению авторского права и связанных с ним прав.

3 Воздействие контрафактного оборудования ИКТ и его компонентов

Контрафактное оборудование ИКТ оказывает на общество особое воздействие, которого может и не быть для других видов нарушений прав интеллектуальной собственности. Например, контрафактные продукты как правило официально не проверяются и не утверждаются в соответствии с какими-либо нормативными требованиями, которые могут быть применимы. Использование контрафактных продуктов может оказаться очень опасным. Например, сообщалось о смертельных случаях из-за взрывов контрафактных аккумуляторных батарей, о случаях поражения электротоком и пожарах, причиняемых зарядными устройствами, а задокументированные образцы таких устройств содержали высокие уровни опасных веществ, таких как свинец и кадмий.

В отчете ОЭСР за 2008 год содержались оценки социально-экономических последствий и последствий для правообладателей, потребителей и правительств:

- В том что касается социально-экономических последствий, контрафакция вполне может иметь отрицательные последствия для инноваций, уровней иностранных прямых инвестиций, роста экономики и уровней занятости, а также может перенаправлять ресурсы в сети организованной преступной деятельности.
- Контрафакция, очевидно, будет оказывать экономическое воздействие на правообладателей, поскольку могут быть затронуты объем продаж и роялти, цены, ценность и репутация торговой марки, стоимость и масштаб операций.
- Потребители могут посчитать, что контрафактные товары имеют низкое качество и представляют собой серьезные риски для здоровья и безопасности.
- Правительства не будут получать достаточно налогов и, возможно, столкнутся с проблемами коррупции, а также им потребуется тратить дополнительные ресурсы на борьбу с деятельностью, связанной с контрафакцией.

3.1 Примеры контрафактного оборудования ИКТ

Ниже приводятся основные примеры воздействия контрафактного оборудования ИКТ:

3.1.1 Мобильные телефоны

Контрафактные мобильные телефоны и аксессуары оказывают отрицательное воздействие на общество, например следующим образом:[1]

- снижают качество услуг служб подвижной телефонной связи, таким образом воздействуя на впечатления потребителей и предприятий;
- создают угрозу безопасности для потребителей в связи с использованием неисправных или непригодных компонентов или материалов;
- приводят к угрозам, связанным с кибербезопасностью;
- ставят под угрозу конфиденциальность данных потребителей;
- наносят ущерб безопасности цифровых транзакций;
- позволяют избегать уплаты применимых налогов и сборов и, таким образом, отрицательно воздействуют на налоговые поступления правительств;
- наносят вред наиболее уязвимым в финансовом отношении потребителям, не предоставляя им никаких гарантий и другим образом нарушая требования закона о защите прав потребителей;
- создают риски для окружающей среды и здоровья потребителей в связи с использованием опасных веществ при производстве таких устройств;
- способствуют торговле наркотиками, терроризму и другим видам национальной и международной преступной деятельности;
- причиняют вред экономике, принимая во внимание искажение рыночного равновесия, которое причиняют недобросовестная конкуренция и мошенническая практика; и
- наносят ущерб товарным знакам компаний, производящих подлинные продукты.

Исследование, проведенное Технологическим институтом Nokia (INdT) − независимой научно-исследовательской и опытно-конструкторской организацией − подтвердило низкое качество контрафактных телефонов и потенциальное отрицательное воздействие, которое они оказывают на потребителей, операторов электросвязи и местную экономику. В ходе исследования были изучены 44 контрафактных и некачественных сотовых телефона, а также было проведено их сравнение с подлинным и официально утвержденным оборудованием. Исследование показывает, что в случае контрафактных телефонов не удаются 26% попыток вызовов, а 24% установленных соединений отбрасываются. Кроме того, в тех местах, где подлинный телефон может отлично работать, контрафактные телефоны нельзя будет использовать из-за плохого качества передачи по сравнению с исходными телефонами. Кроме того, имеются проблемы с передачей вызовов между сотами (способностью поддерживать вызов при перемещении между сотами), при этом время передачи вызовов на 41% дольше по сравнению с исходными телефонами и при передаче отбрасываются 34% вызовов. См. рисунки, приведенные в Приложении 1 Руководства для правительств "Контрафактный/некачественный мобильный телефон", разработанного Форумом производителей мобильного оборудования (MMF) (http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf).

Кроме того, контрафактные мобильные телефоны создают значительные риски для здоровья и безопасности. Такие устройства могут содержать химические вещества, уровень которых превышает установленные нормы безопасности, и намного сложнее организовать их сбор с помощью программ утилизации электронных отходов. Это особенно сказывается на развивающихся странах, которые обладают ограниченными возможностями по экологически безопасной переработке или совсем их не имеют и где множество контрафактных мобильных устройств. Решение проблемы контрафактных устройств путем запрета на них еще более усугубляет эту проблему для развивающихся стран.

---

[1] Приведенная информация основана на Руководстве MMF для правительств "Контрафактный/некачественный мобильный телефон" (http://www.mmfai.org/public/docs/eng/MMF%5FCounterfeitPhones%5FEN%2Epdf)

Контрафактные продукты в связи с низким качеством сборки и использованием низкокачественных компонентов содержат опасные вещества, которые запрещены во многих странах в рамках правил ограничения содержания опасных веществ (RoHS) или аналогичного национального законодательства.

Другое исследование по опасным веществам, проведенное недавно Технологическим институтом Nokia (INdT), расположенным в Бразилии, показывает потенциальные опасности от контрафактных телефонов. В частности, задача исследования состояла в оценке того, соответствуют ли контрафактные телефоны правилам RoHS, а также Директиве ЕС об ограничении использования некоторых опасных веществ в электрическом и электронном оборудовании. Этой Директивой ограничивается использование шести опасных материалов в различных видах электрического и электронного оборудования.

Исследование, которое проводилось с использованием метода испытания согласно стандарту МЭК 62321 [75], включало тестирование пяти контрафактных телефонов и 158 частей, включая крышки, дисплеи, интегральные схемы (IC), клавиатуру и другие компоненты устройств, предназначенных для монтажа на поверхности (SMD). В рамках проведенного INdT исследования обнаружено наличие двух опасных веществ (свинца и кадмия) как во внутренних, так и во внешних компонентах в концентрации, намного превышающей максимальные значения, разрешенные согласно правилам RoHS. В Руководстве MMF для правительств "Контрафактный/некачественный мобильный телефон" (http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf) на рисунке A показан чрезмерный уровень свинца и кадмия, которые были обнаружены во внутренних и внешних компонентах протестированных мобильных телефонов.

Исследования, проведенные в других странах, подтвердили наличие в контрафактных мобильных телефонах опасных веществ. Центр по материалам для электронных технологий (C-MET), расположенный в Хайдарабаде, Индия, провел исследование для тестирования соответствия правилам RoHS мобильных радиотелефонных трубок, поступающих на индийский рынок. Для этого исследования C-MET выбрал для тестирования 15 широко распространенных моделей мобильных телефонов. Телефоны были выбраны на основе их популярности и наличия на индийском рынке, а тесты проводились с использованием процедур стандарта МЭК 62321 (2008 г.).

Результаты показали, что во всех контрафактных мобильных телефонах было обнаружено чрезвычайно высокое процентное содержание опасных веществ, особенно свинца. В некоторых случаях содержание свинца в 35−40 раз превышало приемлемые на международном уровне пределы. Многие важнейшие компоненты, такие как слот карты памяти, слот модуля идентификации абонента (SIM), камера и др., с которыми непосредственно физически контактируют потребители, показали наихудшие результаты с точки зрения содержания опасных материалов, что несомненно повышает риск для потребителей по сравнению тем, когда компоненты находятся внутри устройства. В отличие от этого было обнаружено, что протестированные мобильные телефоны мировых и других признанных марок соответствуют пределам RoHS и поэтому безопасны для использования потребителями. В Руководстве MMF для правительств "Контрафактный/некачественный мобильный телефон" (http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf) на рисунке B кратком виде представлены результаты этого исследования, а на рисунке C наглядно показаны места, где были обнаружены высокие концентрации свинца.

Кроме того, использование телефонов с дублированными/поддельными/отсутствующими номерами международного идентификатора аппаратуры подвижной связи (IMEI) может представлять угрозы для национальной и личной безопасности, поскольку их сложно отследить по сети.

Наконец, в качестве примера доходов, которые могут быть потеряны в результате торговли контрафактными мобильными устройствами, Управление по борьбе с контрафакцией Кении утверждает, что из-за рынка контрафактных мобильных устройств страна потеряла порядка 38,5 млн. долл. США [39]. Внедрение Автоматизированной информационной системы учета мобильных терминалов на Украине (AISMTRU) в 2009 году привело к тому, что в период 2010−2012 годов было получено дополнительно 500 млн. долл. США доходов от уплаты таможенных пошлин на импорт мобильных терминалов. До внедрения в 2009 году этой системы только 5−7% используемых на Украине мобильных устройств импортировались легально, тогда как сейчас легально импортируется 92−95% [40].

3.1.2 Аксессуары и компоненты для продуктов ИКТ

Нередко поступающие в продажу аксессуары для продуктов ИКТ являются контрафактными. В случае мобильных телефонов, а также других продуктов ИКТ, это элементы питания, зарядные устройства и наушники. В случае принтеров контрафактными часто являются картриджи с чернилами. В случае цифровых камер, среди других поддельных аксессуаров, таких как сетевые шнуры и карты памяти, используются поддельные объективы, которые должным образом зарегистрированы вместе с корпусом камеры. Такие поддельные компоненты даже доходят до уровня микросхем. Случайная или намеренная замена поддельными электронными компонентами может причинять пользователям серьезные проблемы, когда они используются в медицинском оборудовании или в других важнейших для безопасности продуктах ИКТ. В 2013 году на проходившей в Париже конференции CarteS были конфискованы незаконные копии бесконтактных смарт-карт MIFARE (http://www.react.org/news-a-events/item/567-mifare).

Контрафактные элементы питания широко распространены по всему миру и вызывают особую обеспокоенность. Они являются причиной целого ряда пожаров. Контрафактные элементы питания могут быть различных видов: от щелочных батареек AA до перезаряжаемых литиево-ионных аккумуляторных батарей, которые включаются во многие различные виды продуктов, в первую очередь мобильные телефоны.

Контрафактные элементы питания были причиной ряда смертельных случаев (hhttp://www.bloomberg.com/apps/news?pid=newsarchive&sid=aLWvmmrHx9F0). В связи с этим отчетом отмечалось, что контрафактные элементы питания широко распространены в более бедных районах, с учетом того, что в них более высокий уровень использования радиотелефонных трубок и, следовательно, чаще требуется замена элементов питания.

Аналогичные инциденты отмечались в странах по всему миру. Все большую обеспокоенность вызывает то, что такие элементы питания являются причиной возникновения проблем на воздушных судах, согласно ряду сообщений об инцидентах. В феврале 2014 года Джоф Лич из Управления гражданской авиации Соединенного Королевства сказал, что обеспокоен "дешевыми скопированными элементами питания, которые продаются из сомнительных онлайновых источников и могли бы приводить к неисправностям, имеющим драматические последствия" (http://www.bbc.co.uk/news/business-25733346).

В 2004 году, давая показания в Судебном комитете Сената Соединенных Штатов Америки, представитель компании Gillette объяснил, что в рамках продолжавшейся одну неделю операции среди многих других контрафактных продуктов был изъят миллион поддельных батареек Duracell (http://www.judiciary.senate.gov/hearings/testimony.cfm?renderforprint=1&id=4f1e0899533f7680e78d03281ff674b8&wit_id=4f1e0899533f7680e78d03281ff674b8-2-2).

Наушники вызывают обеспокоенность в связи с тем, что низкое качество контрафактных наушников может не только плохо воздействовать на уши, но и представлять потенциальный риск возгорания. В 2013 году сообщалось о том, что официальными лицами было конфисковано поддельных наушников на общую сумму 15 млн. фунтов стерлингов (http://www.express.co.uk/news/uk/387869/Designer-headphones-top-16m-deluge-of-fake-goods).

3.1.3 Приемопередающие радиоустановки

Компания Motorola Solutions Inc. предостерегла потребителей от приобретения контрафактных приемопередающих радиоустановок, которые были обнаружены в 2013 году во Вьетнаме. Такие контрафактные приемопередающие радиоустановки могут быть опасными для пользователей; это не просто копии моделей приемопередающих радиоустановок компании Motorola, но на них также незаконно проставлены логотип Motorola и номера моделей, поэтому потребителям сложно их отличать (hhttp://nz.finance.yahoo.com/news/motorola-solutions-counterfeit-two-way-030000020.html).

3.1.4 Цифровые камеры

Цифровые камеры − это часть длинного списка продуктов ИКТ, которые являются контрафакцией. Как и в случае других продуктов, их очень сложно отличить, и оптовые и розничные продавцы и готовые помочь пользователи иногда составляют руководства, чтобы помочь потребителям определять подделки (http://www.ebay.co.uk/gds/How-to-Identify-a-Fake-Nikon-Camera-/10000000177984982/g.html). Для потребителей могут быть очень высокими связанные с

безопасностью и конфиденциальностью риски от таких контрафактных устройств, как веб-камеры. В этих продуктах не только программное обеспечение изначально плохого или неудовлетворительного качества, но и пользователи зачастую не получают обновлений для систем безопасности или последующей поддержки, что делает их подверженными киберрискам.

3.1.5 Персональные и планшетные компьютеры

Популярность некоторых видов компьютеров и планшетов привела к широкому распространению их контрафактного производства. В некоторых случаях такие продукты фактически являются "ловушками" и даже не содержат печатной платы (http://www.cnn.com/2013/03/22/tech/mobile/fake-ipads-walmart/). В тех случаях, когда речь не идет об электронике, в таких продуктах иногда предустанавливается вредоносное программное обеспечение, включенное в контрафактные версии операционных систем (http://www.computerworld.com/s/article/9231277/Microsoft_finds_new_computers_in_China_preinstalled_with_malware).

3.1.6 Электронные детские игрушки

В 2014 году большинство детских игрушек включало электронные устройства того или иного вида. Начиная от поддельных игровых приставок и портативных игровых устройств до игрушек для маленьких детей − все они могут причинять физический вред детям. Риски для безопасности представляют, например, незаземленные блоки питания, которые создают риск поражения электротоком (http://www.theguardian.com/money/2011/dec/07/christmas-shopping-counterfeit-toys).

4 Конвенции по правам интеллектуальной собственности (ПИС)

В ряде международных соглашений и конвенций установлены материально-правовые нормы для защиты ПИС в рамках национального законодательства, а также допустимые исключения и ограничения, и определены необходимые процедуры, которые обязуются вводить национальные правительства для того, чтобы правообладатели могли предпринимать эффективные меры против любых действий, нарушающих их права.

4.1 Парижская конвенция по охране промышленной собственности и Бернская конвенция по охране литературных и художественных произведений

Всемирная организация интеллектуальной собственности (ВОИС) курирует многосторонние договоры, касающиеся интеллектуальной собственности. Основополагающими договорами являются Парижская конвенция по охране промышленной собственности и Бернская конвенция по охране литературных и художественных произведений.

Парижская конвенция была принята в 1883 году и несколько раз существенно пересматривалась. Ее цель состоит в том, чтобы защищать "патенты на изобретения, полезные модели, промышленные образцы, товарные знаки, знаки обслуживания, фирменные наименования и указания происхождения или наименования места происхождения, а также пресечение недобросовестной конкуренции" [18]. В том что касается контрафакции, в Конвенции требуется, чтобы договаривающиеся государства принимали меры против "прямого или косвенного использования ложных указаний о происхождении продуктов или подлинности личности изготовителя, промышленника или торговца".

4.2 Аспекты прав интеллектуальной собственности, связанные с торговлей (ТРИПС), Всемирной торговой организации (ВТО)

Всемирная торговая организация (ВТО) курирует Соглашение ТРИПС, в котором установлены минимальные стандарты, применимые ко всем членам ВТО в связи как с материально-правовой защитой, так и обеспечением ПИС. Таким образом, Соглашением ТРИПС в многостороннее соглашение впервые вводится всесторонний набор положений по обеспечению его соблюдения. Любые разногласия в связи с этим между членами ВТО должны регулироваться согласно Договоренностям ВТО о правилах и процедурах, регулирующих разрешение споров.

Положения ТРИПС по обеспечению соблюдения имеют две основные задачи: предоставление правообладателям эффективных средств обеспечения соблюдения, а также обеспечение того, чтобы правоприменительные процедуры были сбалансированными и пропорциональными и не препятствовали законной торговле. Эти положения разделены на пять разделов. В первом разделе

изложены общие задачи, которым должны отвечать все правоприменительные процедуры. Они направлены в первую очередь на обеспечение их эффективности и на выполнение некоторых основных принципов надлежащих правовых процедур. Следующие разделы посвящены гражданско-правовым и административным процедурам и средствам защиты, обеспечительным мерам, специальным требованиям, касающимся мер пограничного контроля, и уголовному судопроизводству.

В Соглашении проводится различие между правонарушающими действиями в целом, к которым должны применяться существующие гражданско-правовые или административные процедуры и средства защиты, и контрафакцией и пиратством − наиболее явными и очевидными формами правонарушающей деятельности, в отношении которых обязательны некоторые дополнительные процедуры и средства защиты, а именно меры пограничного контроля и уголовное судопроизводство. Для этих целей контрафактные товары в общем определяются как товары, подразумевающие буквальное копирование товарных знаков, а пиратские товары − как товары с нарушением права на воспроизведение согласно авторскому или связанному с ним праву.

Более подробно, обязательства членов ВТО являются следующими:

a) Гражданско-правовые и административные процедуры: Правообладатель должен иметь возможность возбуждать гражданско-правовые, судебные или, на выборочной основе, административные процедуры против нарушителя ПИС. Такие процедуры должны быть справедливыми и соразмерными. Установлены некоторые правила в области доказывания. Кроме того, требуется, чтобы члены ВТО предоставляли судебным органам полномочия присуждать три вида средств защиты: судебные приказы, возмещение убытков и другие средства защиты. В качестве мер по предупреждению неправомерного использования, обязательства распространяются также на возмещение ущерба ответчика, когда правообладатель злоупотреблял правоприменительными процедурами.

b) Обеспечительные меры: Временные судебные запреты являются важным инструментом до разрешения спора в рамках судебного разбирательства. В связи с этим судебные органы имеют полномочия предписывать неотложные и эффективные правоприменительные меры, чтобы предпринимать действия против предполагаемых нарушений. Такие меры направлены на то, чтобы предупредить случаи нарушения ПИС и сохранить соответствующие доказательства, касающиеся предполагаемого нарушения. Как и в других разделах, касающихся обеспечения соблюдения, представлены некоторые процедурные требования и меры по предупреждению неправомерного использования.

c) Меры пограничного контроля: Дают возможность правообладателю сотрудничать с таможенными управлениями в целях конфискации контрафактной продукции на границе и предупреждения оборота таких товаров. Эти меры обязательны для контрафактных товарных знаков и пиратских товаров, охраняемых авторским правом, при этом члены ВТО могут также применять их к случаям нарушения других ПИС, к контрафактной продукции, предназначенной для экспорта, товарам в пути, незначительным объемам импорта и параллельному импорту. К мерам пограничного контроля применяются некоторые процедурные требования и меры по предупреждению неправомерного использования, аналогичные применимым к обеспечительным мерам. В том что касается средств защиты, компетентные органы должны иметь полномочия предписывать уничтожение или иное изъятие контрафактной продукции вне каналов торговли.

d) Уголовное судопроизводство: Его необходимо внедрить для рассмотрения дел, связанных с преднамеренным использованием контрафактного товарного знака или с пиратством в сфере авторского права в промышленных масштабах. Применение уголовного судопроизводства в отношении других случаев нарушений ПИС не обязательно. В том что касается средств защиты, то в Соглашении указывается, что санкции должны включать содержание под стражей и/или денежные штрафы и, в соответствующих случаях, также конфискацию, штрафы и уничтожение контрафактной продукции и материалов и оборудования, которые использовались для ее производства.

В отношении членов ВТО из числа наименее развитых стран в настоящее время действуют меры переходного характера, согласно которым они освобождаются от обязательства применять защитные и правоприменительные нормы, установленные Соглашением ТРИПС, в целом до июля 2021 года, а также от выполнения положений, касающихся защиты и обеспечения соблюдения патентов и закрытых данных в фармацевтическом секторе, до января 2016 года. Задача состоит, среди прочего, в том, чтобы дать им возможность создать конкурентную технологическую базу.

5 Обеспечение ПИС

Несмотря на то что международные договоры, касающиеся защиты прав интеллектуальной собственности, действуют уже более сотни лет, только лишь недавно на международных форумах был рассмотрен вопрос об обеспечении соблюдения. Это произошло благодаря тем основам, которые были созданы Соглашением ТРИПС, а также в связи с социально-экономическими последствиями нарушений ПИС. Теперь вопрос обеспечения ПИС стоит в повестке дня многих международных организаций, в том числе ВОИС, Всемирной таможенной организации (ВТАО) и Интерпола, Европейского союза и многих стран.

5.1 Всемирная организация интеллектуальной собственности (ВОИС)

Всемирная организация интеллектуальной собственности (ВОИС) создала в 2002 году Консультативный комитет по защите прав (ККЗП) для координации деятельности с другими международными организациями и частным сектором в целях борьбы с контрафакцией и пиратством. Он организует программы профессиональной подготовки и оказывает техническую помощь.

ВОИС также сотрудничает с Программой Организации Объединенных Наций по окружающей среде (ЮНЕП) и другими организациями, такими как Экономическая и социальная комиссия Организации Объединенных Наций для Азии и Тихого океана (ЭСКАТО ООН) в целях повышения уровня осведомленности о проблемах, связанных с утилизацией и удалением растущих объемов контрафактных продуктов (http://www.wipo.int/wipo_magazine/en/2012/06/article_0007.html, http://www.unep.org/ozonaction/News/Features/2012/SoutheastAsiaexploressynergies/tabid/104354/Default.aspx, http://www.unescap.org/events/wipoescapunep-workshop-environmentally-safe-disposal-ip-infringing-goods).

5.2 Всемирная торговая организация – Совет по ТРИПС

Совет по ТРИПС − это один из трех секторальных советов, действующих в рамках Генерального совета ВТО. Он отвечает за применение Соглашения ТРИПС и, в частности, за мониторинг действия этого Соглашения и соблюдения членами своих обязательств в рамках Соглашения ТРИПС. Совет проводит официальные собрания в Женеве три раза в год, а также, при необходимости, неофициальные собрания. Эти собрания представляют собой форум для обсуждения и консультаций по любому вопросу, связанному с Соглашением ТРИПС, а также для прояснения или толкования положений Соглашения. Вопрос обеспечения ПИС обсуждался на специальной основе в Совете ТРИПС несколько раз, а последний раз в 2012 году.

5.3 Управление ООН по контролю над наркотиками и предупреждению преступности (УНП ООН)

УНП ООН является депозитарием Конвенции Организации Объединенных Наций против транснациональной организованной преступности, которая представляет собой всемирную платформу сотрудничества по борьбе со всеми формами организованной преступности. В настоящее время сторонами Конвенции являются 167 стран, которые приняли на себя обязательство бороться с организованной преступностью с помощью сотрудничества и обеспечения того, чтобы национальное законодательство имело надлежащую структуру.

УНП ООН два раза в год проводит собрания Сторон Конвенции Организации Объединенных Наций против транснациональной организованной преступности. На этих собраниях собираются вместе представители правительств со всего мира для содействия выполнению Конвенции и обзора ее выполнения, с тем чтобы обеспечить более эффективные подходы к борьбе с транснациональной организованной преступностью. Последнее собрание проходило в октябре 2012 года.

Управление ООН по контролю над наркотиками и предупреждению преступности сосредоточило внимание на связи между торговлей контрафактными товарами и транснациональной организованной преступностью (http://www.unodc.org/counterfeit/). В январе 2014 года УНП ООН начало кампанию под названием "Контрафакт: не приобретай продукцию преступников" в целях повышения осведомленности среди потребителей о незаконном обороте контрафактной продукции, который составляет 250 млрд. долл. в год. Кампания "Контрафакт: не приобретай продукцию преступников" информирует потребителей о том, что покупка контрафактных товаров может финансировать

организованные преступные группы, подвергает риску здоровье и безопасность потребителей, а также усугубляет другие этические и экологические проблемы.

УНП ООН также противодействует потоку незаконных товаров, таких как контрафактные продукты и наркотики, с помощью программ технической помощи. УНП ООН и Всемирная таможенная организация в 2006 году приступили к осуществлению Программы по контролю за контейнерными перевозками (CCP). В результате этой программы было конфисковано 487 контейнеров, содержавших фальсифицированные и контрабандные товары, а также 195 контейнеров с наркотиками. (https://www.unodc.org/unodc/en/frontpage/2014/January/counterfeit-dont-buy-into-organized-crime---unodc-launches-new-outreach-campaign-on-250-billion-a-year-counterfeit-business.html, https://www.unodc.org/unodc/en/frontpage/2012/July/criminals-rake-in-250-billion-per-year-in-counterfeit-goods-that-pose-health-security-risks-to-unsuspecting-public.html)

5.4 Всемирная таможенная организация (ВТАО)

ВТАО − межправительственная организация в составе 179 таможенных управлений, которая возглавляет, руководит и поддерживает деятельность своих членов в целях защиты законной торговли и содействия ей, получения доходов, защиты общества и создания потенциала. Поскольку таможенные управления отвечают за защиту национальных границ от незаконного потока контрафактных и пиратских товаров, ВТАО возглавляет обсуждения, посвященные предпринимаемым на глобальном уровне мерам по борьбе с такими преступлениями. Это подразумевает поддержку мер по борьбе с контрафакцией и пиратством с помощью совершенствования методов по обеспечению соблюдения и содействия обмену информацией между таможнями, а также таможнями и частным сектором.

Основная задача Программы ВТАО в области ПИС и здоровья и безопасности состоит в том, чтобы привлечь к контрафактным продуктам внимание таможенников и отраслей промышленности во всем мире и обеспечить их бдительность в связи с такими продуктами. ВТАО, одним из важнейших приоритетов которой является защита здоровья и безопасности потребителей, активно осуществляет широкомасштабные меры по созданию потенциала и разработке различных инструментов по обеспечению соблюдения.

Сознавая важность сотрудничества с частным сектором, ВТАО очень тесно работает с членами из отрасли и отраслевыми ассоциациями, с тем чтобы оценить их потребности и сложности, связанные с борьбой с этим явлением. ВТАО на регулярной основе приглашает правообладателей участвовать в различных проводимых ею мероприятиях по борьбе с контрафакцией, таких как операции на местах, региональные или национальные семинары, и разработала онлайновый инструмент − интерфейс для членов из частного сектора (IPM), чтобы предоставить таможенникам средство обнаружения контрафактных и пиратских продуктов и связи с участниками экономической деятельности в реальном времени.

Одной из важнейших частей инициатив ВТАО, направленных на борьбу с контрафакцией, являются крупномасштабные операции, при которых многие таможенные управления одновременно повышают уровень обеспечения соблюдения законов, связанных с контрафактными продуктами, с тем чтобы количественно и качественно оценить воздействие контрафактной деятельности в мире. Только лишь в 2003 году таможенные управления конфисковали более 1,1 млрд. контрафактных продуктов в рамках операции в Африканском регионе и операции в регионе Латинской Америки.

Кроме того, ВТАО разработала глобальный инструмент онлайнового обнаружения − IPM, предназначенный для рядовых сотрудников таможни, который помогает различать подлинные продукты и их поддельные копии. Со времени внедрения этого инструмента в 2010 году, IPM стал реальным узлом связи между таможенниками на местах и частным сектором, помогающим им обмениваться важнейшей информацией в реальном времени в целях конфискации контрафактных товаров.

Теперь, с недавним внедрением мобильного IPM, таможенники могут получать доступ к IPM через свои мобильные устройства и извлекать всю необходимую информацию, которая содержится в базе данных. Эта новая версия дает возможность использовать мобильные устройства для сканирования шрих-кодов отраслевого стандарта GS1, которые проставлены на миллионах продуктов, что позволяет затрачивать меньше времени на поиск в базе данных продуктов. Кроме того, сканирование штрих-кодов даст возможность автоматически соединяться с любыми службами аутентификации,

которые связаны с контролируемым продуктом. Этот новый элемент, известный под названием IPM Connected, представляет собой глобальную сеть поставщиков средств защиты (SFP), сопряженную с IPM. С учетом растущей сети SFP, число правообладателей, желающих присоединиться к IPM, также растет, при этом в настоящее время данная система включает более 700 торговых марок, охватывая самые разные отрасли промышленности − от фармацевтических и пищевых товаров и пестицидов до товаров повседневного спроса и предметов роскоши [16].

5.5 Европейский союз

Проблема контрафакции изучалась в Европейском союзе в рамках целого ряда инициатив, начиная от разработки нормативных положений, касающихся работы таможенных органов, до подготовки директивы по обеспечению прав интеллектуальной собственности. Комиссия приступила к проведению общих консультаций по этой теме, выпустив в октябре 1998 года "Зеленый документ".

Работа таможенных органов ранее определялась в Постановлении Совета (ЕС) № 3295/94 "Утверждение мер по запрещению выпуска в свободное обращение, экспорта, реэкспорта или помещения под отлагательную процедуру контрафактных и пиратских товаров"; но это положение было отменено и заменено Постановлением Совета № 1383/2003 от 22 июля 2003 года о таможенных действиях против товаров, подозреваемых в нарушении отдельных прав интеллектуальной собственности, а также о мерах, принимаемых против товаров, нарушающих такие права.

Директива 2004/48/ЕС по обеспечению прав интеллектуальной собственности (под обычным названием IPRED) предназначена для согласования средств, обеспечивающих соблюдение прав интеллектуальной собственности в государствах − членах ЕС. Эта директива применяется ко всем видам интеллектуальной собственности как в физической, так и в цифровой среде. IPRED была весьма противоречивой в том, что первоначальное предложение содержало положения по уголовным санкциям, которые впоследствии были исключены, а также поскольку в ней требовалось внести изменения в национальное право, с тем чтобы суд мог обязать поставщика услуг интернета раскрыть правообладателю идентичность потребителя (на основе использованного адреса протокола Интернет).

Совет Европейского союза принял резолюцию по всестороннему европейскому плану борьбы с контрафакцией и пиратством (25 сентября 2008 г.), который привел к созданию Обсерватории ЕС по контрафакции и пиратству, предназначенной для сбора большего количества данных о контрафакции и пиратстве, содействия более активному сотрудничеству и обмена информацией по передовому опыту в области обеспечения соблюдения (https://oami.europa.eu/ohimportal/en/web/observatory/home).

ЕС согласовал и активно обсуждает со многими странами двусторонние торговые соглашения, такие как Трансатлантическое торговое и инвестиционное партнерство (TTIP) с США (http://ec.europa.eu/trade/policy/in-focus/ttip/).

Европейская комиссия опубликовала в июле 2014 года документ "Торговля, рост и интеллектуальная собственность − Стратегия защиты и обеспечения прав интеллектуальной собственности в третьих странах" (http://ec.europa.eu/transparency/regdoc/rep/1/2014/EN/1-2014-389-EN-F1-1.Pdf) и план действий, содержащийся в документе COM (2014) 392/2.

5.6 Интерпол

Интерпол − Международная организация уголовной полиции, насчитывающая 190 государств-членов, создала в 2002 году Группу по расследованию преступлений в области интеллектуальной собственности. Эта Группа поддерживает региональные и глобальные операции по конфискации контрафактных товаров, организует с помощью Международного колледжа следователей по уголовным делам в области IP (IIPCIC) учебные курсы и создала базу данных по международным преступлениям в сфере интеллектуальной собственности.

5.7 Европейская экономическая комиссия Организации Объединенных Наций (ЕЭК ООН)

Рабочая группа ЕЭК ООН по политике в области стандартизации и сотрудничества по вопросам нормативного регулирования (РГ.6) создала консультативную группу по надзору за рынком (группу MARS), целью которой является содействие государствам-членам в координации их усилий, направленных на уменьшение проблемы, связанной с контрафактными товарами. Группа разработала

Рекомендацию M. "Использование инфраструктуры надзора за рынком в качестве дополнительного инструмента защиты потребителей и пользователей от контрафактной продукции" [18].

5.8 Национальные инициативы (несколько примеров)

5.8.1 Франция

CNAC (*Comité National Anti Contrefaçon*) − Национальный комитет Франции по борьбе с контрафакцией (http://www.industrie.gouv.fr/enjeux/pi/cnac.php),

и INPI (*Institut National pour la Propriété Industrielle*) − Национальный институт промышленной собственности (http://www.inpi.fr/fr/connaitre-la-pi/lutte-anti-contrefacon.html). Кроме того, в деятельности по борьбе с контрафакцией участвует Министерство экономики и финансов (*Ministère de l'économie et des finances*) (http://www.economie.gouv.fr/signature-deux-nouvelles-chartes-lutte-contre-contrefacon-sur-internet).

5.8.2 Управление Соединенного Королевства по вопросам интеллектуальной собственности

Управление правительства Соединенного Королевства по вопросам интеллектуальной собственности создало в 2004 году Группу по противодействию преступлениям в сфере интеллектуальной собственности (ИС). Она готовит ежегодные отчеты по преступлениям в сфере ИС и опубликовала комплект материалов по цепочке поставок [19]. В Соединенном Королевстве также есть министр по вопросам интеллектуальной собственности.

5.8.3 Агентство Кении по борьбе с контрафакцией

Парламент Кении принял в 2008 году Закон по борьбе с контрафакцией (№ 13). Этим законом запрещается торговля контрафактными товарами и создается Агентство по борьбе с контрафакцией [20].

5.8.4 Объединенная комиссия США и Китая по коммерции и торговле

США и Китай создали Объединенную комиссию по коммерции и торговле. На ее 24-м собрании в декабре 2013 года Национальная ведущая группа Китая по борьбе с нарушениями ПИС и с производством и продажей контрафактных и некачественных товаров обязалась принять в 2014 году план действий, включающий повышение уровня информированности общественности, а также требования по соблюдению всех законов и нормативных положений, касающихся мер защиты и обеспечения ПИС (www.commerce.gov/news/fact-sheets/2013/12/20/fact-sheet-24th-us-china-joint-commission-commerce-and-trade-fact-sheet).

6 Промышленные форумы по борьбе с контрафакцией

Реакцией промышленных предприятий на проблему контрафакции стало создание форумов, представляющих их интересы. Такие форумы предоставляют информацию о степени распространения этой проблемы, предлагают пути смягчения воздействия контрафакции и подталкивают правительства и международные организации к принятию мер для борьбы с контрафакцией.

6.1 Международная торговая палата (МТП)

МТП представляет мировые коммерческие организации. Ее членами являются тысячи компаний и ассоциаций примерно из 120 стран. Она действует в интересах коммерческих кругов, выступая с заявлениями перед правительствами и межправительственными организациями. МТП была учреждена в 1919 году, а в 1923 году сама создала Международный арбитражный суд МТП.

В 1985 году МТП создала Бюро по борьбе с контрафактной продукцией, а недавно − Группу "Бизнес в борьбе с контрафактом и пиратством" (BASCAP).

Бюро МТП по борьбе с контрафактной продукцией ведет базу данных на основе исследований конкретных ситуаций и, кроме того, обеспечивает следственные функции.

Группа BASCAP продолжила изучение экономического и социального воздействия контрафакции и пиратства, которое было начато ОЭСР [4], и создала центр обмена информацией, сгруппированной

по странам [21] и секторам [22], а также разработала справочник по защите торговых марок [23] и мировой справочник с контактной информацией [24].

Кроме того, МТП публикует "Дорожную карту по интеллектуальной собственности" [25].

6.2 Международная коалиция по борьбе с контрафактной продукцией (IACC)

IACC [26] была создана в 1979 году, и ее членами являются представители всех отраслей промышленности. Ее целью является борьба с контрафакцией и пиратством с помощью содействия внедрению нормативных положений по борьбе с контрафакцией.

6.3 Форум производителей мобильного оборудования (MMF)

Форум производителей мобильного оборудования ведет веб-сайт (spotafakephone.com), на котором приводится информация по контрафактным мобильным телефонам и элементам питания.

6.4 Международная ассоциация дилеров по продаже услуг и компьютеров и Североамериканская ассоциация дилеров в области электросвязи (AscdiNatd)

AscdiNatd разработала программу борьбы с контрафакцией, которая включает политику в области борьбы с контрафакцией, предназначенную для принятия компаниями-членами, и информационные ресурсы по контрафакции, включая информацию, полученную от компаний HP и Cisco [27].

6.5 Альянс за сокращение "серого" рынка и контрафакции (AGMA)

AGMA был создан в 2001 году компаниями 3Com, Cisco Systems, Hewlett-Packard, Nortel и Xerox в целях борьбы с торговлей контрафактными высокотехнологичными продуктами.

6.6 Рабочая группа по борьбе с контрафакцией Британской ассоциации производителей электротехнического и смежного оборудования (BEAMA)

BEAMA − независимая экспертная база знаний и форум для электротехнической отрасли Соединенного Королевства и всей Европы. В Ассоциации представлены более 300 компаний-производителей из электротехнического сектора, и она обладает существенным влиянием на международном уровне, а также в большой политике, политике в области стандартизации и коммерции.

Рабочая группа BEAMA по борьбе с контрафакцией (ACWG) была создана в 2000 году. Ее задача состоит в принятии мер против производителей контрафактного электрооборудования и против торговых компаний, продающих их на многих международных рынках, в том числе Европы, Ближнего Востока и Африки. Членами этой Рабочей группы, как и у BEAMA, являются многие ведущие промышленные ассоциации из секторов, которые занимаются монтажом, распределением, тестированием и сертификацией, а также правоохранительной деятельностью. Достигнуто признание на глобальном уровне ее активной работы, и она сотрудничает с торговыми ассоциациями и правоохранительными органами всего мира.

Создана база данных по контрафакции для использования отраслью электроэнергетических установок, которая предоставляется официальным органам всего мира, с тем чтобы они могли отслеживать положение на местных рынках.

Деятельность Рабочей группы освещается в отраслевых журналах, на презентациях, благодаря участию в конференциях и с помощью публикации руководств и плакатов, предназначенных для повышения уровня осведомленности об этой быстро растущей угрозе, которая может причинять ущерб безопасности потребителей и целостности бизнеса.

Рабочая группа отвечает за управление проектами действий по борьбе с контрафакцией, сбор и распространение информации по вопросам, связанным с ПИС, и отвечает на вопросы правительств и других сторон от имени Ассоциации. Она также предоставляет консультации и информацию любой компании или ассоциации, у которых имеются проблемы, связанные с ПИС.

В настоящее время ее деятельность включает проекты в Китае, ОАЭ, Соединенном Королевстве, Нигерии и Ираке, а также всесторонние программы наблюдения за веб-сайтами и портами.

В Соединенном Королевстве BEAMA работает со многими ведущими отраслевыми органами в целях повышения уровня осведомленности и борьбы с контрафактными и несоответствующими требованиям продуктами, и специально для этой цели был создан отраслевой портал www.counterfeit-kills.co.uk.

6.7 UKEA (Альянс электронной промышленности Соединенного Королевства)

UKEA − консорциум торговых ассоциаций Соединенного Королевства, представляющих сектор электронного оборудования. Цель Альянса состоит в координации проводимых в секторе обсуждений вопросов и в связи с правительством. UKEA создал Форум по борьбе с контрафакцией [28], который публикует информацию по проблемам, связанным с контрафактными электронными компонентами, по поставщикам возможных решений и по передовому опыту.

6.8 Группа по борьбе с контрафактным производством (ACG)

ACG − торговая ассоциация Соединенного Королевства, созданная в 1980 году, члены которой относились в основном к автомобильной промышленности, но теперь в ней представлены большинство отраслей промышленности.

6.9 UNIFAB − Союз производителей

Союз производителей − французская организация, занимающаяся борьбой с контрафакцией с помощью повышения уровня осведомленности общественности (помимо прочей деятельности, открыт Музей контрафакции), предоставления информации предприятиям и лоббистской деятельности (http://www.unifab.com/en/).

6.10 Международная инициатива в области производства электронного оборудования (iNEMI)

Инициатива iNEMI разработала проект "Контрафактные компоненты − Методика оценки и разработка показателей" (http://www.inemi.org/project-page/counterfeit-components-assessment-methodology-and-metric-development).

7 Меры по борьбе с контрафактным оборудованием

7.1 Введение

С контрафактным оборудованием можно бороться, маркируя товары таким образом, чтобы их можно было аутентифицировать путем строгого контролирования жизненного цикла продуктов. На продукты можно наносить метки, которые сложно подделать, и присвоенные серийные номера, которые можно использовать для того, чтобы удостовериться в подлинности товара (например, с помощью доступа в базу данных).

Отдельным товарам могут быть присвоены уникальные идентификаторы. Примером системы, которая используется для борьбы с контрафакцией, является проверка происхождения с помощью мобильных средств (mPedigree), которая используется для борьбы с фармацевтической контрафактной продукцией в Африке. Эта система позволяет потребителям проверять, являются ли лекарственные продукты подлинными или контрафактными и потенциально опасными, с помощью передачи (бесплатной) коротких сообщений (SMS) в реестр фармацевтической продукции.

Требуется строгий контроль за цепочками поставок и, возможно, полными жизненными циклами продуктов, при этом не менее необходимы тестирование, оценка и сертификация, чтобы обеспечить безопасность продукта и сохранение соответствующего качества. Кроме того, сотрудникам таможен необходимо предоставить инструменты для определения контрафактных продуктов, а также могут применяться механизмы надзора за рынком.

Идентификаторы можно наносить на объект прямым текстом или же они могут быть закодированы на "идентификационном (ID) маркере", таком как штрих-код, маркер радиочастотной идентификации (RFID), смарт-карта или инфракрасный маркер, с тем чтобы их можно было считывать автоматически. При идентификации объекта можно выделить три уровня. Первый из них − это

уровень непосредственного идентификатора, на котором объекты получают уникальную идентификацию, например проставляется электронный код продукта (EPC). Второй уровень − это уровень кодирования, поскольку непосредственный идентификатор может кодироваться в различных форматах. И, наконец, физическая реализация, когда кодированный идентификатор наносится, например, на маркер RFID.

Для обеспечения того, чтобы идентификаторы были уникальными для конкретных приложений на глобальном уровне, они должны управляться организованным образом с помощью своего рода процедуры распределения. Например, Ассоциация GSM (GSMA) занимается международными идентификаторами аппаратуры подвижной связи (IMEI) для глобальной системы подвижной связи (GSM), универсальной системы подвижной электросвязи (UMTS) и устройств с долгосрочным развитием (LTE); Отраслевая ассоциация в области электросвязи распределяет идентификаторы оборудования подвижной связи (MEID) для устройств с многостанционным доступом с кодовым разделением (CDMA), а GS1 занимается штрих-кодовыми идентификаторами. ИСО управляет рядом доменов идентификаторов, а также действует в качестве высшего органа, включающего системы идентификаторов других организаций, таких как GS1.

Другой пример − маркировка оборудования для указания того, что оно было утверждено для продажи на рынках страны. Например, компания Anatel требует, чтобы зарядные устройства и элементы питания для мобильных телефонов обозначались защищенной меткой, определенной в ее резолюции 481/2007[2] (см. рисунок 1).

Рисунок 1 – Пример защищенной метки, требуемой Anatel и определенной в ее резолюции 481/2007

Такой подход использовался в отрасли по производству оборудования электросвязи в течение многих лет и был успешно внедрен некоторыми странами/регионами[3] (например, ФКС[4], Anatel[5], ЕС[6]).

Сотрудники таможен должны иметь возможность определять контрафактные продукты, а также случаи надзора за рынком и другие правоприменительные меры, которые могут быть применены. Кроме того, можно идентифицировать импортеров, в отношении которых имеются сведения о пренебрежении контролем за импортом, и включать их в специальный список. При импорте оборудования ИКТ мошенничающими импортерами регуляторные органы могут быть уведомлены о том, что может быть принято решение о проведении инспекций, а затем следует гарантировать обеспечение соблюдения соответствующих требований (см. рисунок 2).

---

2 https://translate.google.com/translate?sl=pt&tl=en&js=y&prev=_t&hl=fr&ie=UTF-8&u=legislacao.anatel.gov.br%2Fresolu%C3%A7%C3%B5es%2F2007%2F192-resolu%C3%A7%C3%A3o-481&edit-text=

3 При использовании некоторых систем оценки соответствия для такого подхода могут потребоваться сертификация, заявление о соответствии и/или применение соглашений о взаимном признании (MRA).

4 https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=30744&switch=P

5 https://grandeseventos.anatel.gov.br/en/frequently-asked-questions.html#pergunta1

6 http://exporthelp.europa.eu/thdapp/display.htm?page=rt%2frt_TechnicalRequirements.html&docType=main&languageId=en

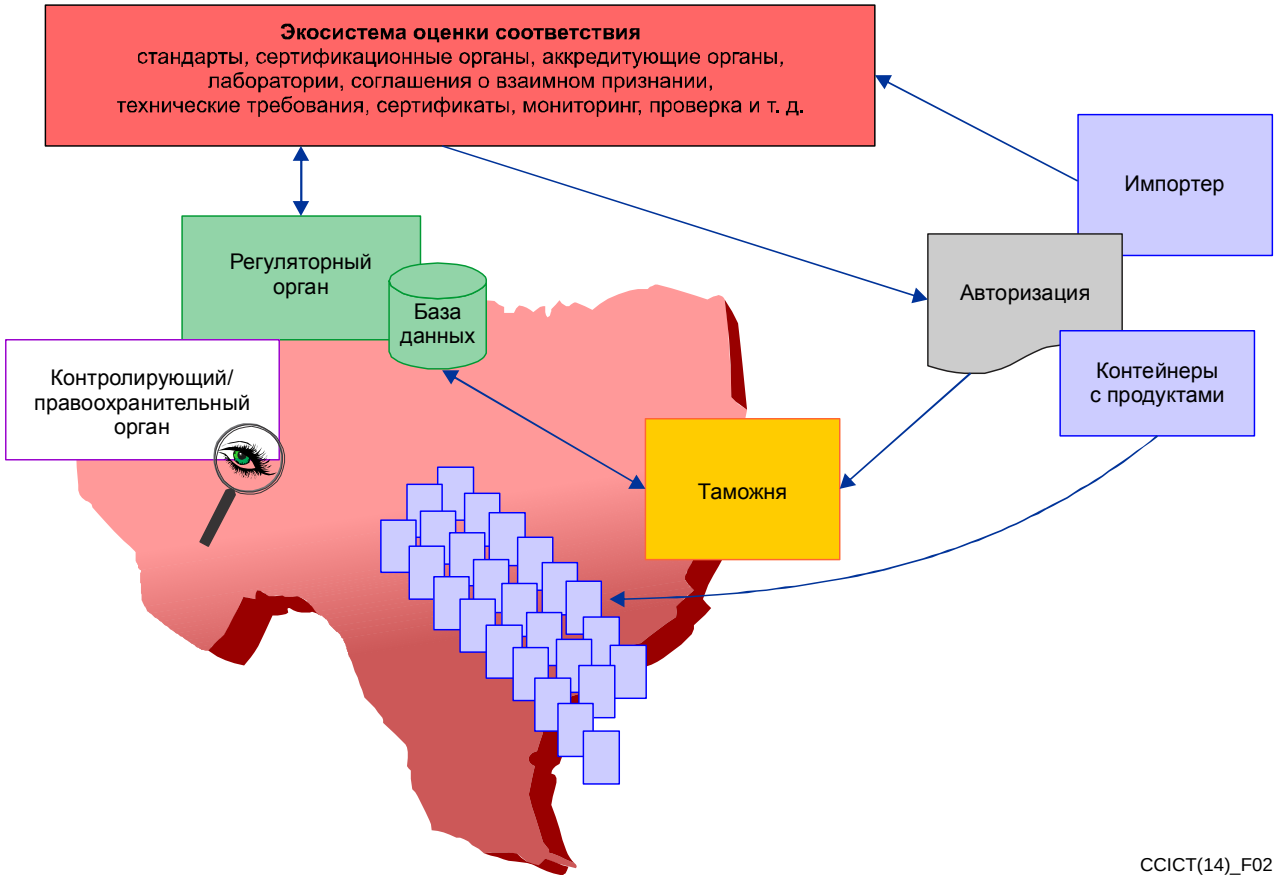


Рисунок 2 – Экосистема оценки соответствия

Следует отметить, что фактически контрафактные продукты могут соответствовать указанным требованиям, быть функционально совместимыми с подлинными продуктами и поэтому проходить проверку на соответствие и функциональную совместимость. Поэтому, чтобы точно определять контрафактные продукты и отличать их от подлинных продуктов, может потребоваться оценка продукта владельцем товарного знака.

Сектор ИКТ отличается широким присутствием международных конкурентов, что способствует постоянным инновациям. Это желательное условие, но в то же самое время рынок открыт для производителей/продавцов, которые не настроены следовать устоявшимся международным, региональным или национальным правилам.

Проблема асимметричной информации более ярко выражена в развивающихся странах, где недостаточно разрабатываются или не разрабатываются вообще процедуры технологической оценки и оценки на соответствие. Типичные проблемы, которые часто возникают при управлении системой оценки на соответствие, связаны с отсутствием заслуживающей доверия и доступной для анализа информации, например как в следующих случаях: i) определение происхождения или ответственного по закону агента для продуктов; ii) места расположения производственных предприятий; iii) сертификационные органы; и iv) компетентные лаборатории с законными свидетельствами об аккредитации. В некоторых случаях импортеры без каких-либо технических знаний и возможности предоставить помощь, могут представлять иностранные компании, которые привлекали для исполнения работ их инженерно-технические и производственные подразделения, перемещенные в другие страны (например, схемы с привлечением внешних подрядчиков). Хотя такие процессы могут обеспечивать экономию в процессе производства, ухудшаются качество и подотчетность при производстве оборудования электросвязи/ИКТ.

Кроме того, можно было бы утверждать, что условия для производства низкокачественного оборудования создают интересы личной выгоды, корысть, отсутствие норм и/или слабое обеспечение их соблюдения. В ряде случаев в связи с отсутствием надлежащего процесса оценки соответствия на конкретном целевом рынке одна и та же торговая марка или модель оснащается и продается с

различными электронными компонентами, некоторые хорошего качества, некоторые − плохого, и поставляется в определенные направления в зависимости от относительно низкого качества. Как один из примеров такой фальсификации оборудования, предназначенного для продажи в странах к югу от экватора, можно привести процедуру, известную под названием tropicalização (по-португальски "подготовка для работы в тропических условиях") (см. рисунок 3).

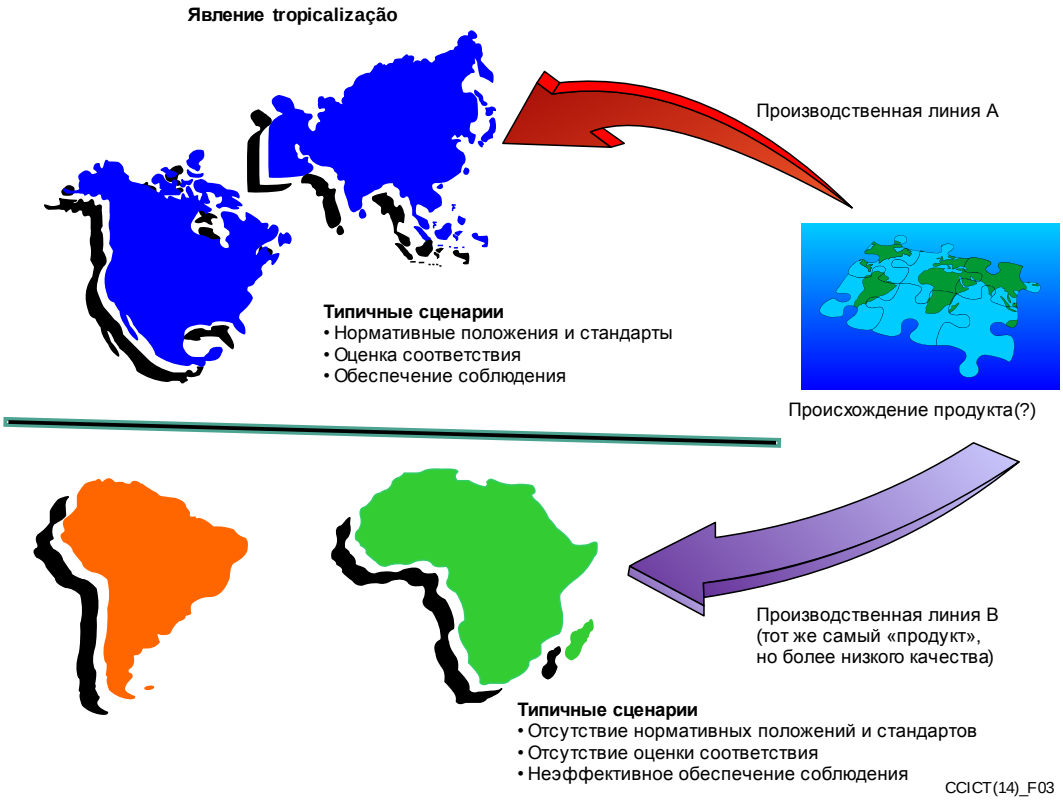


Рисунок 3 – Процедура, известная под названием tropicalização (по-португальски "подготовка для работы в тропических условиях")

7.2 Злоупотребление идентификаторами и знаками утверждения типа

Все идентификаторы, создаваемые подлинными производителями товаров, могут использоваться и используются контрафакторами с нарушениями для достижения своих целей заставить потребителей и органы власти поверить в то, что их продукт является подлинным. Эта проблема стоит перед многими отраслями, не только ИКТ. Читателю следует не забывать о том, что любой механизм идентификации и связанная с ним безопасность будут целью для контрафакторов и преступников. Знаки и пиктограммы утверждения типа, а также электронные идентификаторы часто умышленно повреждаются, чтобы избежать проверок на границе со стороны таможенных и правоохранительных органов. Это создает практические проблемы для производителей, потребителей, сотрудников таможен и правоохранительных органов, которым трудно отличить поддельные идентификационные знаки от подлинных, даже перед рассмотрением самого продукта.

7.3 Международный идентификатор аппаратуры подвижной связи (IMEI)

Как уже отмечалось, мобильные телефоны были особенно привлекательной целью для контрафакторов, и в ответ на это Форум производителей мобильного оборудования (MMF) создал веб-сайт, где приводится информация для потребителей о том, как определять контрафактные телефоны и элементы питания (http://spotafakephone.com). Они рекомендуют быть в курсе внешнего вида, функциональных возможностей, наличия и цен подлинных товаров, а также проверять номер международного идентификатора аппаратуры подвижной связи (IMEI). IMEI − это уникальный идентификатор для каждого мобильного телефона, а контрафактные товары часто не имеют IMEI или имеют поддельный номер. Одна из проблем для производителей, сетевых операторов и органов власти состоит в том, что контрафакторы так наладили свое производство, что иногда добиваются в

рамках своей стратегии в области контрафакции соблюдения допустимых областей, действующих у существующих производителей. Это также может использоваться в качестве одного из методов, чтобы избегать систем проверки IMEI.

Распределением IMEI руководит GSMA, с тем чтобы обеспечить уникальность таких идентификаторов. Применяется иерархическая схема распределения, при которой GSMA присваивает двузначные идентификаторы представляющим доклады органам, которые затем распределяют IMEI и серийный номер оборудования. Представляющие доклады органы, в настоящее время уполномоченные распределять IMEI: CTIA (Ассоциация беспроводной связи), BABT (Британский комитет по утверждениям для электросвязи), TAF (Форум по тестированию и утверждению оконечного оборудования электросвязи) (Китай) и MSAI (Альянс Индии в области стандартов подвижной связи).

Формат IMEI, действующий с 1 января 2003 года, приводится ниже на рисунке 4 [37]:

Код распределения типа (TAC)	Серийный номер	Контрольная цифра
NNXXXX YY	ZZZZZZ	A

TAC	Код распределения типа, известный ранее под названием код утверждения типа.
NN	Идентификатор представляющего доклад органа.
XXXXYY	Идентификатор типа мобильного оборудования (ME), определенный представляющим доклад органом.
ZZZZZZ	Распределяется представляющим доклад органом, но присваивается производителем для каждого ME.
A	Контрольная цифра, определяемая как функция от всех других цифр IMEI.

Рисунок 4 – Формат IMEI

GSMA регистрирует для каждого устройства, обозначаемого ее IMEI, дополнительную информацию, такую как название производителя и номер модели, и технические характеристики, такие как поддерживаемые полосы частот и класс мощности.

GSMA ведет IMEI DB (базу данных IMEI) [38], ранее известную как центральный регистр идентификации оборудования (CEIR). IMEI DB содержит "белый список" оборудования, которое считается подходящим для использования во всем мире, а "черный список" IMEI, относящихся к устройствам, которые не считаются подходящими для использования в связи с тем, что они были потеряны, украдены или являются бракованными и представляют собой угрозу для целостности сети. Следует отметить, что "белый список" IMEI DB − это список кодов TAC, а не полных IMEI, и данные могут свободно получать имеющие на это право стороны, включая национальные регуляторные органы, правоохранительные учреждения и таможенные органы. В дополнение к IMEI DB отдельные сетевые операторы могут ввести собственные регистры идентификации оборудования (EIR), в которые они могут загрузить "белый список", что позволяет операторам контролировать, какие устройства могут поступать в их сети (http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/accessing-the-imei-database/).

В первую очередь IMEI DB предназначена для использования операторами, с тем чтобы они могли идентифицировать используемые в их сетях устройства и определять их характеристики, а также для блокирования украденных радиотелефонных трубок. Кроме того, IMEI DB может использоваться для обнаружения контрафактных устройств, что помогает предотвращать легализацию таких устройств, сдерживать преступность и содействовать привлечению к уголовной ответственности.

Вместе с тем в связи с внедрением IMEI отмечался ряд проблем. Сообщалось о случаях оборудования, не имеющего IMEI, с полностью нулевым IMEI, дублированными IMEI и IMEI, распределенными не уполномоченными на это организациями. Некоторые из таких устройств с недействительными или не являющимися уникальными IMEI являются контрафакцией, а другие − подлинные, но не соответствующие процедуре GSMA по распределению IMEI в связи с неправильным пониманием со стороны производителей. Например, по оценкам, в Индии

насчитывается 30 млн. радиотелефонных трубок GSM без IMEI, и альянс MSAI был уполномочен GSMA предложить программу временной амнистии, предусматривающую проставление подлинных IMEI (программа внедрения подлинных IMEI (GII)), с тем чтобы можно было уникальным образом идентифицировать каждое устройство.

В качестве примера дублированных IMEI можно отметить случай обнаружения в Австралии 6500 радиотелефонных трубокs с IMEI 135790246811220. В том что касается незарегистрированных IMEI, сетевой оператор в Уганде сообщил о том, что количество кодов TAC в его сети, которые не зарегистрированы в IMEI DB, превышает количество TAC, распределенных GSMA и зарегистрированных в IMEI DB.

Поэтому имеются веские причины обеспечивать санкционированное использование IMEI и распределение IMEI в соответствии с процессом GSMA. IMEI DB − это один из инструментов обнаружения контрафактных мобильных телефонов, и, в качестве одного из примеров, Кения запретила с конца сентября 2012 года доступ к мобильным телефонам с недействительными IMEI, при том что по оценкам поддельными радиотелефонными трубками пользуются 2,3 млн. абонентов. В Приложении A дана более подробная информация по этим примерам и приводятся другие случаи, когда IMEI использовались в качестве основы для определения контрафактных мобильных телефонов. Поскольку некоторые национальные меры, направленные на решение вопроса контрафактных мобильных устройств, основаны на использовании IMEI, важно, чтобы процедура распределения IMEI и база данных IMEI были защищенными и надежными, а также чтобы IMEI в устройствах надежно кодировались.

Один из вариантов состоит в том, что от операторов требуется блокировать устройства с дублированными и недействительными IMEI, поскольку такие устройства, чтобы они могли работать, должны аутентифицироваться в сети. Возможно, на настоящее время самым эффективным инструментом решения проблемы является блокирование этих устройств при их первом подключении.

Но имеется несколько препятствий для блокирования IMEI. Первое из них состоит в том, что GSMA ведет не полный "белый список" IMEI, а только "белый список" кодов TAC. Во-вторых, IMEI с законных устройств имитировались на контрафактных и некачественных устройствах, что затрудняет процесс блокирования. И, наконец, любое связанное с блокированием решение должно предотвращать или запрещать копирование других имитированных IMEI на рассматриваемых устройствах.

Несмотря на проблемы с блокированием, на рынке имеются подходящие решения. В то же самое время важно избегать смешения уникальных национальных решений, что просто перенесет эту проблему за национальные границы. С учетом того, что IMEI распределяются GSMA и что IMEI DB ведется GSMA, представляется логичным, что Ассоциации тем или иным образом следовало бы участвовать в национальных инициативах, чтобы использовать полный набор имеющихся списков и другие технические меры.

Но с учетом того, что, по оценкам, количество контрафактных устройств просто огромно, одно лишь блокирование рабочих терминалов оказало бы тяжелое и непредвиденное воздействие на сети и конечных пользователей. И этот факт нельзя игнорировать.

В связи с этим важно учитывать, что в развивающихся странах с низким уровнем социально-экономического развития мобильные телефоны являются основным средством связи и участия в информационном обществе[7]. К сожалению, это происходит с использованием значительного количества более дешевых контрафактных устройств.

По этой причине к такому изменению должно быть готово все общество. Необходимо изучить, рассмотреть и запланировать оптимальные подходы. Например, потребителям необходимо четко объяснить причины запрета контрафактных устройств (риски безопасности, более низкое качество обслуживания и, как следствие, рост количества жалоб, риска помех и нарушений ПИС).

---

[7] Инициатива МСЭ "Обеспечение развития с помощью мобильных средств": http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Pages/default.aspx.

Поэтому если регуляторные органы и правительства решат ввести меры по блокированию оконечных устройств, важно принять переходную политику, например сначала блокировать только новые оконечные устройства и позволить продолжать работу тех устройств, которые уже находятся в сети. Но в конечном счете пользователям придется перейти на подлинные оконечные устройства, так как предполагаемый жизненный цикл мобильных оконечных устройств составляет 18 месяцев[8].

7.4 Уникальные идентификаторы

Электронные коды продукта (EPC) впервые были разработаны Центром автоматической идентификации Массачусетского технологического института, созданным в 1999 году, которым сейчас руководит EPCglobal − дочерняя структура GS1, которая определила наиболее часто используемые спецификации для глобальных систем цепочек поставок. Кроме того, Международная организация по стандартизации (ИСО) и Единый идентификационный центр (Япония) определили идентификаторы для ряда приложений.

GS1 определяет следующие девять "идентификационных ключей" для идентификации товаров, местоположений предприятий, транспортных упаковок, имущества, услуг, типов документов, поставок и партий товаров:

- GTIN − глобальный номер товара
- GLN − глобальный номер предприятия
- SSCC – серийный код транспортной упаковки
- GRAI – глобальный идентификатор возвратного имущества
- GIAI – глобальный идентификатор индивидуального имущества
- GSRN – глобальный номер услуги
- GDTI – глобальный идентификатор типа документа
- GSIN – глобальный идентификационный номер поставки
- GINC – глобальный идентификационный номер партии товара

GTIN используется для идентификации категорий объектов, тогда как GLN, SSCC, GIAI и GSRN идентифицируют отдельные объекты; GRAI и GDTI могут применяться для идентификации категорий объектов или отдельных товаров в зависимости от отсутствия или присутствия серийного номера. GINC и GSIN идентифицируют логические группировки, а не физические объекты. Такие идентификационные ключи предназначены для реализации с использованием штрих-кодов. Существует зависимость между этими кодами и кодами EPC, определенными EPCglobal для использования с RFID. GTIN в схеме EPC расширен путем добавления серийного номера, с тем чтобы уникальным образом идентифицировать объект. Другие ключи, используемые для идентификации отдельных объектов, имеют непосредственный эквивалент кода EPC. Определены следующие EPC [41]:

- Общий идентификатор (GID)
  - urn:epc:id:gid:ManagerNumber.ObjectClass.SerialNumber
- Сериализованный глобальный номер товара (SGTIN)
  - urn:epc:id:sgtin:CompanyPrefix.ItemReference.SerialNumber
- Серийный код транспортной упаковки (SSCC)
  - urn:epc:id:sscc:CompanyPrefix.SerialReference
- Глобальный номер предприятия с расширением или без расширения (SGLN)
  - urn:epc:id:sgln:CompanyPrefix.LocationReference.Extension
- Глобальный идентификатор возвратного имущества (GRAI)
  - urn:epc:id:grai:CompanyPrefix.AssetType.SerialNumber
- Глобальный идентификатор индивидуального имущества (GIAI)

[8] http://www.epa.gov/osw/education/pdfs/life-cell.pdf: "Сотовые телефоны используются в среднем только 18 месяцев, прежде чем будут заменены, даже хотя они могут работать гораздо дольше".

    - urn:epc:id:giai:CompanyPrefix.IndividulAssetReference
- Глобальный идентификатор типа документа (GDTI)
    - urn:epc:id:gdti:CompanyPrefix.DocumentType.SerialNumber
- Глобальный номер услуги (GSRN)
    - urn:epc:id:gsrn:CompanyPrefix.ServiceReference
- Министерство обороны США (DoD)
    - urn:epc:id:usdod:CAGEOrDODAAC.SerialNumber
- Идентификатор авиакосмической и оборонной промышленности (ADI)
    - urn:epc:id:adi:CAGEOrDODAAC.OriginalPartNumber.Serial

В стандарте ИСО/МЭК 15459 [42] определяются уникальные идентификаторы для отслеживания цепочек поставок, которые могут быть представлены в таких средствах автоматической идентификации и сбора данных (AIDC), как штрих-коды и RFID.

В частях 1, 4, 5, 6 и 8 стандарта ИСО/МЭК 15459 указаны уникальные строки символов для идентификации транспортных единиц, отдельных товаров, возвратных транспортных единиц, группировок продуктов и транспортных единиц, соответственно. В каждом случае уникальный идентификатор сгруппирован по классам, с тем чтобы содействовать эффективному управлению идентификаторами для данного класса объекта.

В части 2 указаны процедурные требования к распределению уникальных идентификаторов для приложений управления товарами и излагаются обязанности органа регистрации и агентств по выдаче. Эти процедуры не применяются к товарам, для которых ИСО уже назначила агентства по ведению и органы регистрации для обеспечения идентификационных схем. Поэтому они не применяются к:

- грузовым контейнерам, поскольку их уникальное кодирование указано в ИСО 6346 [43];
- автотранспортным средствам, поскольку их уникальная идентификация указана в ИСО 3779 [44];
- автомобильным радиоприемникам, поскольку их уникальная идентификация указана в ИСО 10486 [45]; и
- схемам ISBN [46] и ISSN [47].

В части 3 излагаются общие правила, применимые к уникальным идентификаторам для управления товарами, которое требуется для обеспечения полной совместимости между классами уникальных идентификаторов.

Техническому комитету 246 ИСО поручена разработка стандартных инструментов борьбы с контрафакцией. Комитет разрабатывает стандарт по критериям качества для решений по аутентификации в целях борьбы с производством контрафактных товаров [48].

В дополнение к ИСО и EPCglobal, Единый идентификационный центр в Японии определил общий идентификатор под названием "ucode" [49], который не только предназначен для идентификации физических объектов, но и может использоваться для идентификации мест и цифровой информации (см. рисунок 5). Длина базовых ucodes − 128 битов (но может быть увеличена кратно 128 битам), и они могут включать другие идентификаторы, такие как ISBN, адреса протокола Интернет (IP) или телефонные номера по Рекомендации МСЭ-Т E.164 [76]. Как правило, ucode − это номер, которому необходимо придать смысловое содержание в реляционной базе данных. Любое лицо или организация может получить ucode в Едином идентификационном центре, который действует для этих номеров в качестве регистрационного органа.

Версия (4 бита)	TLDc (16 битов)	cc (4 бита)	SLDc (изменяется)	ic (изменяется)
TLDc: код домена верхнего уровня (присваивается Единым идентификационным центром) cc: код класса (указывает границу между SLDc и ic) SLDc: код домена второго уровня ic: идентификационный код для отдельных объектов				

Рисунок 5 – Формат ucode

МСЭ-Т работает над системами оценки мультимедийной информации, инициируемой посредством идентификации вещей на основе маркеров. В рамках этой работы составляется описание различных схем идентификации, которые могли бы использоваться для такой идентификации. Единый идентификационный центр представил свою схему ucode, согласно которой ucode будет присваиваться идентификатору объекта (OID), зарегистрированному по ветви {joint-iso-itu-t(2) tag-based(27)} в соответствии с Рекомендацией МСЭ-Т X.668 [50]. При описанной ранее схеме уникального идентификатора ИСО/МЭК идентификатор объекта присваивается по ветви {iso(1)} дерева идентификатора объекта. Это приводит к тому, что при схемах идентификации ИСО/МЭК (включая EPCglobal) и Единого идентификационного центра идентификаторы объектов присваиваются либо по ветви **{iso}** (ИСО и EPCglobal), либо по ветви **{joint-iso-itu-t}** (Единый идентификационный центр), и позволяет совместное существование различных схем идентификации с разными регистрационными органами. Для маркеров RFID идентификатор объекта (OID) и ID будут кодироваться так, как это определено в стандарте ИСО/МЭК 15962 [77].

ПРИМЕЧАНИЕ. – Термины "объект" или "идентификатор объекта" здесь не используются применительно к "вещи" в целом, а применяются в соответствии с определением, приведенным в ИСО/МЭК 15961 [78]: "четко определенные часть информации, определение или спецификация, для которых требуется название, чтобы установить их использование при связи". Идентификатор объекта определяет такой объект однозначным образом. Идентификаторы объектов организованы согласно иерархической структуре, при этом корни дерева или верхние "дуги" обозначают организацию, которая отвечает за определение информации. Верхние "дуги" представляют МСЭ-Т, ИСО и совместно ИСО−МСЭ-Т. Им присвоены цифровые значения 0, 1 и 2, соответственно. Дуге "на основе маркеров" в совместном дереве ИСО−МСЭ-Т присвоено цифровое значение 27.

Данные, связанные с объектом, могут храниться на маркере вместе с идентификатором, если у маркера достаточный объем памяти. А другие возможные средства найти информацию, связанную с идентификатором, состоят в использовании механизма разрешения идентификатора.

Можно предусмотреть для RFID весьма разнообразные услуги и приложения, поскольку становится возможным предоставлять информацию, связанную с идентификатором маркера, в различных формах (текст, звук или изображение). Например, в музее идентификатор на маркере, прикрепленном к картине, может использоваться для поиска дополнительной информации об этой картине и ее авторе. В продовольственном магазине идентификатор на упаковке продукта может использоваться, чтобы удостовериться, что продукт питания можно безопасно употреблять и что он не является частью выборочной партии, при проверке которой было обнаружено, что она тем или иным образом заражена. Доступ к обеспечиваемой идентификатором информации может также быть полезен в медицине/фармацевтике, сельском хозяйстве, библиотеках, розничной торговле и управлении цепочкой поставок. В Рекомендации МСЭ-Т F.771 [55] описывается ряд услуг, которые могли бы основываться на использовании информации, связанной с маркированными объектами, и требованиях для этих услуг.

Модель оценки информации, связанной с маркированным объектом, описывается в Рекомендации МСЭ-Т H.621 [52] (см. рисунок 6). В рамках этой модели функция обнаружения мультимедийной информации может направить идентификатор, полученный от считывающего устройства маркера ID, функции разрешения ID, тем самым получая указатель (такой как универсальный указатель ресурса − URL) на соответствующего управляющего мультимедийной информацией. В результате становится возможным получить доступ к информации, связанной с маркером ID. Поскольку ожидается, что число идентификаторов будет очень большим, вероятно, функция разрешения ID будет распространяться по древовидной структуре.

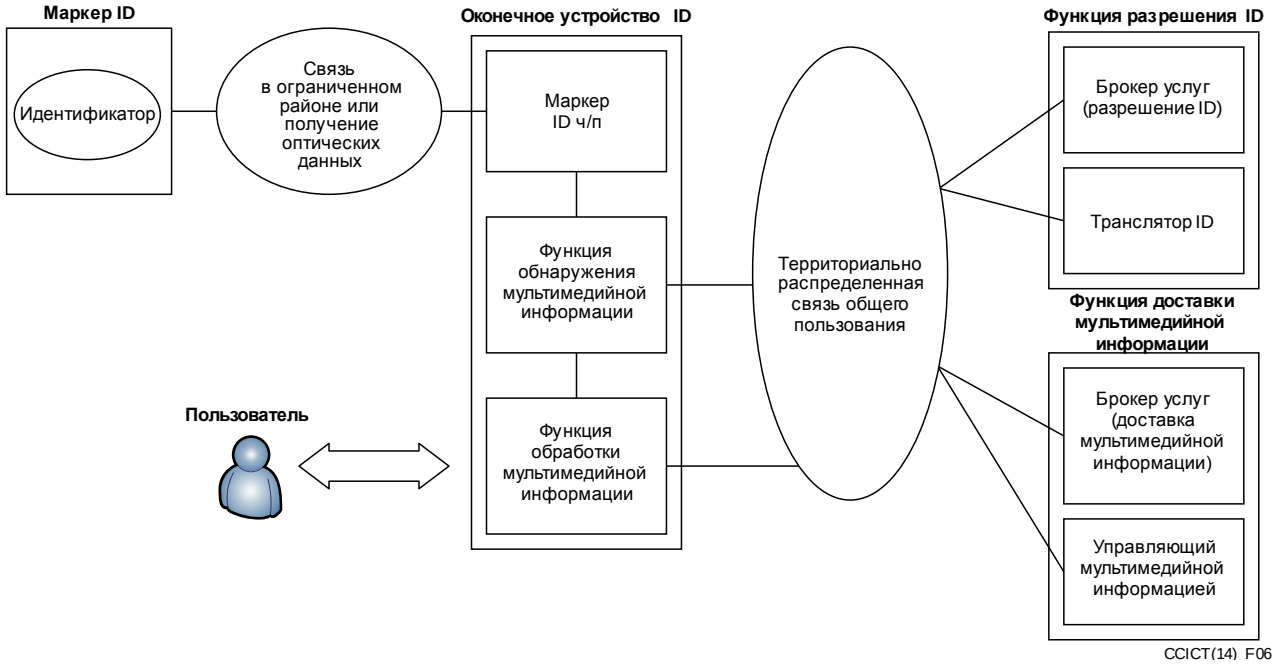


Рисунок 6 – Функциональная архитектура для доступа к мультимедийной информации, инициируемого посредством идентификации на основе маркеров (Рекомендация МСЭ-Т H.621)

Функция разрешения ID может быть основана на использовании системы наименований доменов (DNS) интернета, которая обычно обеспечивает адрес протокола Интернет (IP), соответствующий универсальному указателю ресурса (URL). В услуге по присвоению наименований объектам (ONS), описанной EPCglobal, для нахождения информации, связанной с кодами электронных продуктов, используются механизмы DNS.

Кроме того, в Рекомендации МСЭ-Т X.1255 [79] (https://www.itu.int/rec/T-REC-X.1255-201309-I/en) представлена структура обнаружения информации по управлению определением идентичности, которая признана в резолюции Полномочной конференции МСЭ "Борьба с контрафактными устройствами электросвязи/информационно-коммуникационных технологий".

7.5 Автоматическая идентификация и сбор данных (AIDC)

7.5.1 Штрих-коды

Штрих-коды часто используются для идентификации продуктов. Они могут быть различной формы − от штрих-кодов универсального товарного кода (UPC), которые хорошо известны в супермаркетах, до матричных (двумерных) штрих-кодов. Они могут легко подделываться и копироваться контрафакторами.

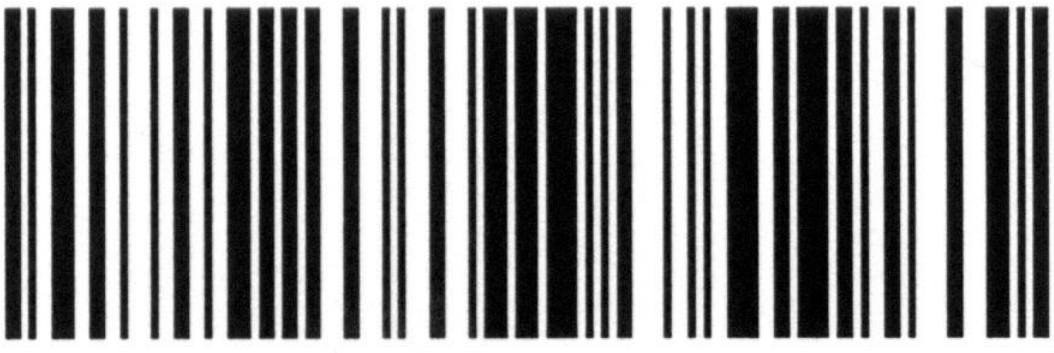


Рисунок 7 – Примеры линейных штрих-кодов

Примеры линейных штрих-кодов приведены на рисунке 7:

- UPC ИСО/МЭК 15420 [80]
- Код штрих-кода 39 ИСО/МЭК 16388 [81]
- Код штрих-кода 128 ИСО/МЭК 15417 [82]

Рисунок 8 – Примеры матричных (двумерных) штрих-кодов

Примеры матричных (двумерных) штрих-кодов приведены на рисунке 8:

- Codablock F ИСО/МЭК 15417+
- PDF 417 ИСО/МЭК 15438 [83]
- Maxicode ИСО/МЭК 16023 [84]
- Код QR ИСО/МЭК 18004 [85]
- Матричные данные ИСО/МЭК 16022 [86]

Штрих-коды могут использоваться для кодирования серийного номера. Например, DIN 66401 [87] определяет уникальный идентификационный знак (UIM), состоящий из матричного символа (ИСО/МЭК 16022 или ИСО/МЭК 18004) и уникального идентификатора данных (в соответствии с ANSI MH10.8.2 [88] и "+" символ согласно ANSI/HIBC 2.3 [89]). Это стандарт приложения для маркировки небольших элементов, например в сфере электроники или здравоохранения. Такие штрих-коды особо подходят для непосредственной чернильно-струйной или лазерной маркировки, а также для распечатки этикеток.

Требования к этикетированию и непосредственной маркировке продуктов с применением линейных и двумерных штрих-кодов указаны в стандарте ИСО 28219 [53]. Требования к дизайну этикеток с линейными и двумерными штрих-кодами для упаковки продуктов указаны в стандарте ИСО 22742 [54], а этикеток для поставки, перевозки и получения − в ИСО 15394 [55].

7.5.2 RFID

RFID дает возможность маркировать объекты и хранить на этих маркерах информацию, которую можно считывать с использованием технологии беспроводной связи малого радиуса действия. Спецификации для RFID охватывают идентификацию объектов, характеристики радиоинтерфейса и протоколы передачи данных.

В стандарте ИСО/МЭК 15963 [56] описываются способы присвоения маркерам радиочастот (РЧ) уникальных идентификаторов. Маркеры РЧ имеют идентификатор, распределенный производителем интегральной схемы − маркер ID. Маркер ID (TID) может использоваться в качестве уникального идентификатора элемента (UII), когда маркер прикрепляется к какому-либо элементу, или же UII может храниться в отдельной части памяти на маркере. В этом случае UII может быть кодом EPC, как это отмечается EPCglobal.

На рисунке 9 показан формат маркера ID стандарта ИСО/МЭК 15963.

Класс распределения (AC)	Регистрационный номер эмитента TID	Серийный номер
8 битов	Размер задается значением AC	Размер задается значениями AC и TID эмитента

Рисунок 9 – Формат маркера ID стандарта ИСО/МЭК 15963

Класс распределения указывает орган, присваивающий номера − эмитента TID. Производители карт интегральных схем могут быть зарегистрированы для присвоения уникальных идентификаторов согласно схеме ИСО/МЭК 7816-6 [90] или схеме Национального комитета по стандартам для информационных технологий (INCITS) Американского национального института стандартов, и таким же образом производители маркеров для транспортных контейнеров и транспортных приложений могут быть зарегистрированы согласно процедурам ИСО 14816 [91]. Идентификаторы EPCglobal включаются в схему ИСО/МЭК 15963 как класс GS1.

На рисунке 10 показаны пять классов эмитентов TID:

Значение AC	Класс	Размер идентификатора эмитента TID	Размер серийного номера	Регистрационный орган (регистрационный номер эмитента TID)
000xxxxx	INCITS 256	См. ANSI INCITS 256 [92] и 371.1 [93]	См. ANSI INCITS 256 и 371.1	autoid.org
11100000	ИСО/МЭК 7816-6	8 битов	48 битов	APACS (Платежное управление Соединенного Королевства)
11100001	ИСО 14816	См. NEN	См. NEN	NEN (Нидерландский институт по стандартизации)
11100010	GS1	См. ИСО/МЭК 18000-6 тип C [94] и ИСО/МЭК 18000-3 вид 3 [95]	См. ИСО/МЭК 18000-6 тип C и 18000-3 вид 3	GS1
11100011	ИСО/МЭК 7816-6	8 битов	48 битов	APACS (включает объем памяти и расширенный заголовок TID)
Все другие значения	Зарезервировано			Зарезервировано

Рисунок 10 – Классы эмитентов уникальных TID

Вначале RFID применялись для идентификации животных. В 1994 году ИСО завершила разработку стандарта, которым определяется структура идентификационного кода RFID для животных (ИСО 11784 [96]). В дополняющем стандарте ИСО 11785 [97] описано, как считывать эту информацию с маркера.

ИСО приступила к определению полного набора спецификаций для управления элементами: стандарты ИСО/МЭК 15961−15963 описывают общий протокол передачи данных и форматы идентификаторов, применяемые к серии стандартов ИСО/МЭК 18000 [98], где описываются радиоинтерфейсы на различных частотах. Для различных полос частот требуются отдельные спецификации, поскольку рабочая частота определяет характеристики возможности связи, например рабочий диапазон или то, влияет ли на передачу присутствие воды.

Стандарт ИСО/МЭК 29167-1 [57] определяет архитектуру для безопасности и управления файлами для стандартов ИСО/МЭК 18000, относящихся к радиоинтерфейсам. Определены механизмы безопасности, зависимые от приложений, и маркер может поддерживать все из них или какую-либо их группу. Запросчик маркера RFID может получать доступ к информации о механизмах безопасности, поддерживаемых маркером, а также к дополнительной информации, такой как алгоритм кодирования и применяемая длина ключа.

Руководства по внедрению для проектировщиков систем в целях оценки потенциальных угроз безопасности данных, обозначаемых маркером, и взаимодействию маркер-считывающее устройство, а также описания соответствующих контрмер для обеспечения безопасности данных маркера приводятся в стандарте ИСО/МЭК TR 24729-4 [58].

Приложения RFID для цепочки поставок (содержащие части, применимые к грузовым контейнерам, возвратным транспортным элементам, транспортным единицам, упаковке продуктов и маркировке продуктов) определены в стандартах ИСО 17363−17367 [99]−[103]; в ИСО 18185 [104] описано, как может использоваться RFID для отслеживания передвижений грузовых контейнеров. ИСО также разработала спецификации для проверки результатов деятельности и соответствия.

Приведенная в стандарте ИСО/МЭК 29160 [105] эмблема RFID может использоваться на продуктах в качестве метки для указания на то, что у них имеется маркер RFID (см. рисунок 11).

Рисунок 11 – Пример эмблемы RFID, указанной в стандарте ИСО/МЭК 29160

EPCglobal − дочерняя структура GS1, которая разрабатывает спецификации для использования кодов электронных продуктов, имеющих RFID. EPCglobal создала набор стандартов, включая спецификации для кодирования данных маркеров, для протоколов радиоинтерфейсов, протоколов считывающих устройств, а также информации и услуг по присвоению наименований объектам. На рисунке 12 представлен обзор набора стандартов EPCglobal.

Ниже представлены основные элементы набора стандартов:

- Стандарт данных маркера (TDS) EPC определяет количество схем идентификации и описывает, как эти данные кодируются на маркерах, а также как они кодируются в форме, подходящей для использования в системной сети EPC.
- Машиночитаемая версия форматов данных EPC приводится в стандарте перевода данных маркера (TDT) EPC. Она может использоваться для проверки идентификаторов EPC и перевода различных форм представления данных.
- Протоколы маркеров являются радиоинтерфейсами RFID. По интерфейсу "Gen 2" считывающее устройство посылает на маркер информацию с помощью модулирования радиочастотного сигнала в диапазоне 860−960 МГц. Маркеры являются пассивными в том смысле, что они получают энергию от сигнала, передаваемого считывающим устройством. Такой протокол радиоинтерфейса был включен в серию спецификаций ИСО/МЭК 18000 в части 6 как тип C. Высокочастотный радиоинтерфейс работает на частоте 13,65 МГц. Эта спецификация обратно совместима с ИСО/МЭК 15693 [106].
- Протокол считывающего устройства низкого уровня (LLRP) используется клиентом для контроля считывающего устройства на уровне работы протокола радиоинтерфейса и обеспечивает интерфейс между прикладным программным обеспечением и считывающими устройствами (протокол считывающего устройства (RP)).

- Считывающие устройства обнаруживают клиентов с использованием процедур, указанных в стандарте обнаружения, конфигурации и инициализации (DCI).
- Стандарт управления считывающим устройством (RM) используется для контролирования рабочего состояния считывающих устройств RFID. Он основан на использовании простого протокола управления сетью (SNMP), который определен Целевой группой по инженерным проблемам интернета (IETF).
- Стандарт событий прикладного уровня (ALE) предоставляет клиентам средство получения фильтрованных данных EPC. Этот интерфейс обеспечивает независимость между компонентами инфраструктуры, которые получают исходные данные EPC, компонентами, которые обрабатывают эти данные, и приложениями, которые используют эти данные.
- Стандарт информационных услуг EPC (EPCIS) дает возможность обмена данными EPC внутри предприятий и между предприятиями.
- Терминология профильного бизнеса (CBV) предназначена обеспечить, чтобы все стороны, которые обмениваются данными EPCIS, одинаково понимали значение этих данных.
- В стандарте услуги по присвоению наименований объектам (ONS) описывается, как может использоваться система наименований доменов (DNS) для получения информации, связанной с тем или иным конкретным кодом EPC.
- В стандарте профиля сертификатов EPCglobal описывается, как можно аутентифицировать объекты в глобальной сети EPC. Применяются система аутентификации из Рекомендации МСЭ-Т X.509 [60] и профили инфраструктуры открытых ключей интернета, определенные в стандартах IETF RFC 3280 [61] и IETF RFC 3279 [62].
- В стандарте определения происхождения указываются средства обработки электронных документов, касающихся "происхождения" лекарственных средств, для использования в приложениях цепочки поставок фармацевтических средств.

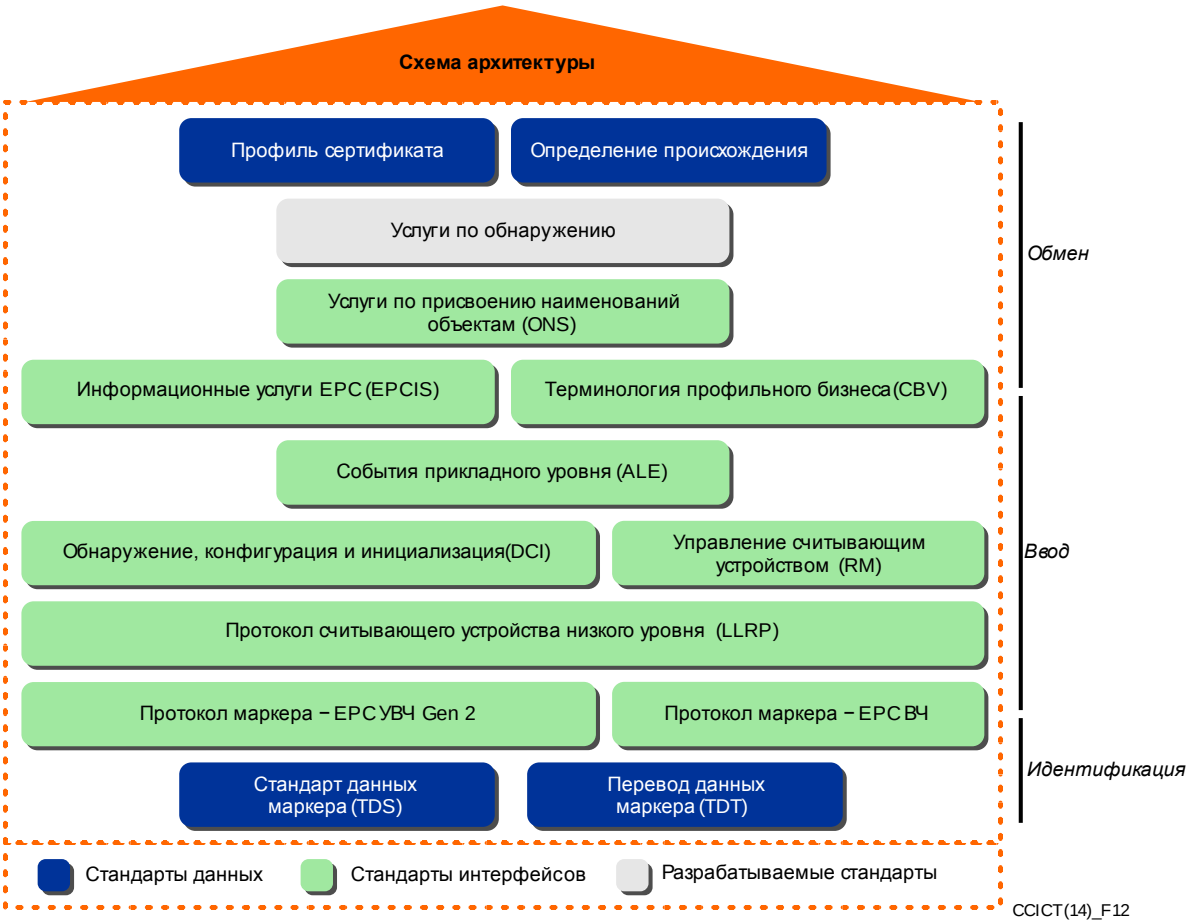


Рисунок 12 – Обзор стандартов EPCglobal [59]

7.6 Конфиденциальная печать и голографическая маркировка

Методы конфиденциальной печати могут использоваться для создания меток, защищающих от несанкционированного вскрытия, которые также могут дополняться голографическими изображениями, которые сложно подделать. Тем не менее следует отметить, что такие механизмы широко нарушаются и копируются контрафакторами.

7.7 Управление цепочкой поставок

Для борьбы с контрафактной деятельностью очень важно поддерживать безопасность цепочек поставок. В серии международных стандартов ИСО 28000 указываются требования по безопасному управлению цепочками поставок. Эти стандарты применимы к организациям любого размера, занимающимся производством, обслуживанием, хранением или воздушными, железнодорожными, автодорожными и морскими перевозками на любом этапе процесса производства или поставки. Имеются следующие стандарты:

- ISO 28000:2007, *Системы менеджмента безопасности цепи поставок. Технические условия*. [107]
- ISO 28001:2007, *Системы менеджмента безопасности цепи поставок. Наилучшие методы обеспечения безопасности в цепи поставок, оценки и планы. Требования и руководящие указания*. [108]
- ISO 28003:2007, *Системы менеджмента безопасности для цепи поставок. Требования к органам аудита и сертификации систем менеджмента безопасности цепи поставок*. [109]
- ISO 28004-1:2007, *Системы менеджмента безопасности цепи поставок. Руководство по внедрению ISO 28000. Часть 1. Общие принципы*. [110]
- ISO 28005-2:2011, *Системы менеджмента безопасности для цепи поставок. Электронный допуск в порт (EPC). Часть 2. Основные элементы данных*. [111]

Согласно ИСО 28000 от организаций требуется оценивать среду безопасности, в которой они работают, и определять, были ли внедрены надлежащие меры безопасности. На рисунке 13 показаны элементы системы управления безопасностью.

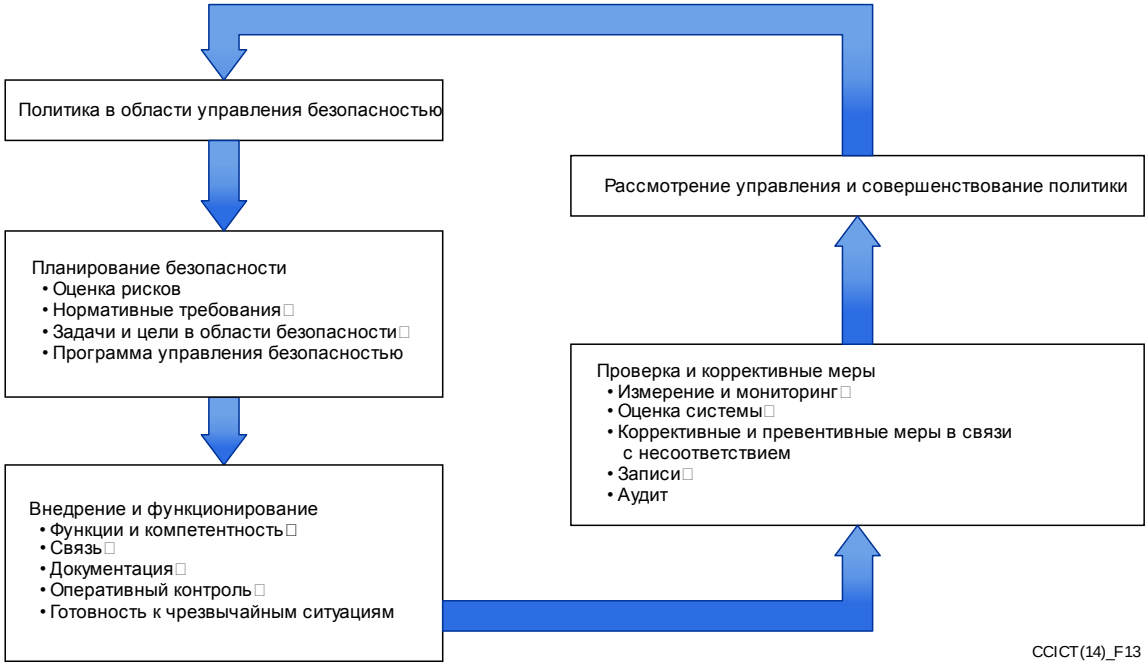


Рисунок 13 – Элементы системы управления безопасностью стандарта ИСО 28000

Рамочные стандарты безопасности Всемирной таможенной организации (ВТАО) [63] предназначены для обеспечения безопасности глобальных цепочек поставок и включают справочник с описанием факторов, которые указывают на высокий риск содержания в партиях грузов контрафактных товаров. Рамочные стандарты безопасности основаны на соглашениях между таможнями и на партнерствах

между таможнями и предприятиями, при этом преимущества предоставляются тем предприятиям, которые соблюдают стандарты безопасности цепочек поставок.

Технический комитет (ТК) 107 МЭК, сфера деятельности которого состоит в управлении процессами для отрасли авиационной электроники, разработал спецификацию, касающуюся недопущения использования контрафактных, фальсифицированных и переработанных электронных компонентов [64]. Кроме того, сейчас Комитет работает над спецификацией по управлению электронными компонентами из несетевых источников в целях недопущения того, чтобы контрафактные компоненты попадали в цепочку поставок [65].

SAE International (первоначально Общество автомобильных инженеров) разработало ряд спецификаций, предназначенных специально для того, чтобы предотвращать попадание контрафактных электронных компонентов в цепочки поставок аэрокосмической и автомобильной отраслей, которые часто упоминаются в электронной промышленности. SAE разработало два документа, которые предназначены для использования теми, кто принимает решения о закупках:

SAE AS5553 [112]: "Контрафактные электронные детали; предотвращение, обнаружение, смягчение последствий"; и

SAE ARP6178 [113]: "Контрафактные электронные детали; инструмент для оценка рисков сбытовых компаний"; и спецификация, предназначенная для использования сбытовыми компаниями: SAE AS6081 [114]: "Контрафактные электронные детали; протокол предотвращения, сбытовые компании". Кроме того, SAE разработало спецификацию по тестированию: SAE AS6171 [115]: "Стандарт для методов тестирования; контрафактные электронные детали".

ТК 107 МЭК тесно работает с SAE International в связи со стандартом SAE AS5553 с использованием соглашения о взаимодействии.

Большинство упомянутых ранее форумов, занимающихся проблемой контрафактных товаров, дают рекомендации или руководящие указания по управлению цепочкой поставок. В целом существуют требования, касающиеся возможности отслеживания, инспектирования и тестирования (которые осуществляются первой, второй или третьей сторонами). В 2011 году Группой Соединенного Королевства по преступности, связанной с IP, был разработан комплект материалов по цепочкам поставок.

7.8 Тестирование

Международная электротехническая комиссия (МЭК) управляет следующими схемами оценки соответствия (http://www.iec.ch/about/activities/conformity.htm):

- IECEE – Система схем оценки соответствия МЭК для электротехнического оборудования и компонентов;
- IECEx – Система МЭК для сертификации соответствия стандартам, относящимся к оборудованию, предназначенному для использования во взрывоопасной среде;
- IECQ – Система оценки качества МЭК для электронных компонентов.

Эти схемы оценки соответствия МЭК основаны на проводимой третьей стороной сертификации, и в них применяются онлайновые системы для предоставления информации по сертификатам, которые можно использовать для идентификации контрафактных продуктов.

Система IECEE управляет схемой сертификационного органа (CB), основанной на принципе взаимного признания ее членами результатов тестов для сертификации или утверждения на национальном уровне. Бюллетень CB (http://members.iecee.org/iecee/ieceemembers.nsf/cb_bulletin?OpenForm) представляет собой базу данных для пользователей схемы CB, которая обеспечивает следующую информацию:

- стандарты, принятые для использования в этой схеме;
- участвующие национальные сертификационные органы, в том числе категории продуктов и стандарты, для которых они были признаны; и
- национальные различия каждой страны-члена по каждому стандарту.

IECEE CBTC Online − это онлайновая регистрационная система сертификатов испытаний для национальных сертификационных органов, которая также предоставляет доступ для общественности.

Система IECEE создала целевую группу для изучения мер по борьбе с контрафакцией (CMC-WG 23 "Контрафакция").

Международная система сертификации IECEx включает следующие компоненты:

- Схема сертифицированного оборудования IECEx;
- Схема сертифицированных средств обслуживания IECEx;
- Система лицензирования знака соответствия IECEx;
- Сертификация компетенции персонала (CoPC) IECEx.

Система IECEx CoC Online обеспечивает информацию по сертификатам и лицензиям, выдаваемым в соответствии с этими схемами.

Система IECQ управляет планом управления электронными компонентами (ECMP) IECQ для авиационных систем и схемой IECQ управления процессами, связанными с опасными веществами (HSPM). Сертификаты представляются в онлайновой форме.

7.9 Базы данных

Базы данных известных контрафактных продуктов предоставляются для использования правоохранительным органам, которыми управляют ВТАО и Интерпол, а также потребителям. Бюро МТП по борьбе с контрафактной продукцией ведет базу данных примеров конкретных ситуаций.

7.10 Надзор за рынком

Надзор за рынком состоит в "деятельности, которую проводят, и мерах, которые принимают назначенные органы для обеспечения того, чтобы продукты соответствовали требованиям, установленным в соответствующих законодательных актах, и не представляли угрозы здоровью, безопасности или любому другому аспекту защиты общественных интересов" [66].

Контрафактные товары могут быть идентифицированы во время деятельности по надзору за рынком, и органы надзора за рынком можно было бы привлекать к усилиям по борьбе с торговлей контрафактными товарами. ЕЭК ООН рекомендует координировать надзор за национальным рынком и таможенную деятельность, а также предоставлять правообладателям возможность информировать о контрафакции органы надзора за рынком [67].

Некоторые страны требуют, чтобы выпускаемые на рынок продукты были зарегистрированы. Например, Организация по стандартам Нигерии недавно внедрила схему регистрации электронных продуктов, пытаясь ограничить продажу контрафактных продуктов.

8 Организации по стандартам

Основными международными организациями по стандартизации, которые занимаются темами, связанными с борьбой с контрафакцией, являются Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК).

В 2009 году ИСО создала технический комитет для разработки спецификаций для инструментов, предназначенных для борьбы с контрафакцией (ТК 246 ИСО). Этот комитет разработал спецификацию "Критерии эффективности для идентификационных растворов, используемых для борьбы с подделками материальных изделий" (ИСО 12931) [48]. Данная спецификация предназначена для повышения доверия потребителей, обеспечения большей защищенности цепочек поставок и помощи государственным органам в разработке превентивной, сдерживающей и карательной политики. ТК 246 ИСО более не действует, но работа в этой области продолжится в рамках ТК 247 ИСО.

Стандартизация в области обнаружения, предотвращения и контроля за мошенничеством, связанным с идентичностью, финансами, продуктами и с другими формами мошенничества в социально-экономической сфере, относятся к сфере охвата ТК 247 ИСО "Меры по предотвращению и контролю мошенничества". Этот комитет разработал руководящий стандарт ИСО по функциональной совместимости идентификаторов объектов для борьбы с контрафакцией − ИСО 16678 [116] "Руководящие указания по идентификации функционально совместимых объектов и соответствующим системам аутентификации для ограничения контрафакции и незаконной торговли".

Этот новый проект касается использования массовой сериализации для идентификации продуктов на основании базы данных, чтобы удостовериться в уровне аутентичности. Данный международный стандарт предназначен для того, чтобы можно было осуществлять надежную и безопасную идентификацию объекта в целях ограничения внедрения на рынок незаконных объектов. Серийно пронумерованные продукты можно аутентифицировать на всем протяжении цепочки производства и распределения, в том числе потребителю.

ИСО признала, что контрафакция и пиратство затрагивают огромный ассортимент потребительских товаров, включая одежду и обувь, лекарственные средства, автомобили и автомобильные детали, продовольствие и напитки, косметические средства, кинофильмы и музыку, электротехнические продукты, устройства безопасности и авиационные запасные части. Особую озабоченность потребителей вызывают риски для безопасности и здоровья, аспекты, связанные с качеством, удобство в использовании/пригодность к использованию по назначению, доступность, защита данных, потеря рабочих мест, вред экономике и связи с организованной преступностью (http://www.iso.org/iso/copolco_priority-programme_annual-report_2012.pdf).

Объединенный технический комитет ОТК 1/ПК 6 ИСО/МЭК работает над методами автоматической идентификации и сбора данных. У комитета имеются семь рабочих групп по следующим темам:

- РГ1 Носитель данных;
- РГ2 Структура данных;
- РГ4 Радиочастотная идентификация для управления объектами;
- РГ5 Системы определения местоположения в реальном времени;
- РГ6 Идентификация мобильных объектов и управление ими (MIIM);
- РГ7 Безопасность управления объектами.

Кроме того, в ТК 225 технологиями AIDC занимается Европейский комитет по стандартизации (CEN).

Многие национальные организации по стандартизации создали комитеты, аналогичные существующим в ИСО/МЭК. В качестве всего лишь одного примера можно привести Немецкий институт по стандартизации (DIN), который создал DIN NA 043-01-31 для работы по методам автоматической идентификации и сбора данных [68] и DIN NA 043-01-31-04 UA по радиочастотной идентификации для управления объектами

ТК 107 МЭК по управлению процессами для авиационного электронного оборудования работает над предотвращением контрафакции.

Кроме того, общество SAE International разрабатывает спецификации, с тем чтобы не допустить использование контрафактных электронных компонентов в высокотехнологичных отраслях, а GS1 разработала набор спецификаций по идентификации объектов и управлению цепочкой поставок.

9 Руководящие указания по борьбе с контрафакцией

Руководящие указания по борьбе с контрафакцией были представлены целым рядом организаций с различных сторон − с точек зрения производителей и сбытовых компаний, правительств и их правоохранительных органов, а также потребителей.

Форум по борьбе с контрафакцией предлагает передовой опыт для OEM (производителей исходного оборудования), сбытовых компаний и производителей компонентов [69]. Эти руководящие указания включают:

- снабжение напрямую от производителей или уполномоченных сбытовых компаний или, если это невозможно, из источника с "серого" рынка, созданного на местном уровне;
- требование представлять документальное подтверждение аутентичности, если используются источники с "серого" рынка;
- усиление координации при управлении жизненными циклами продуктов и компонентов;
- обеспечение того, чтобы сломанные и бракованные продукты уничтожались после использования; и

- повышение возможности отслеживания продукта с помощью использования уникальных идентификаторов и контроля документации.

Институт технологии компонентов (CTI) разработал Программу по предотвращению контрафактных компонентов (CCAP-101) [70] для сертификации независимых компаний, занимающихся сбытом электронных компонентов. Для сбытовых компаний указаны требования по обнаружению и недопущению поставок контрафактных компонентов своим клиентам. Может проводиться электрическое тестирование. Такая программа сертификации предназначена для того, чтобы выполнялись задачи спецификации SAE AS5553.

Аналогичным образом, Ассоциация независимых дистрибьюторов электронного оборудования (IDEA) разработала спецификацию для смягчения последствий и расследования контрафакции (IDEA-STD-1010A) [117], а также спецификацию по управлению качеством (IDEA-QMS-9090) [118].

Дорожная карта BTAO в области IP включает рекомендации в отношении действий предприятий и правительств по всем аспектам защиты интеллектуальной собственности, в том числе по борьбе с контрафакцией и пиратством. В частности, BTAO призывает правительства больше делать для усиления нормативных положений в области ПИС, так как "ресурсы правительств, выделяемые на борьбу с пиратством и контрафакцией, часто, к сожалению, недостаточны в сравнении с масштабом этой проблемы".

ОЭСР отметила, что рынок контрафактных и пиратских продуктов можно подразделить на "первичный рынок", на котором, по мнению потребителей, представлены подлинные продукты, и на "вторичный рынок", на котором покупатели заведомо приобретают контрафактные или пиратские продукты в поиске дешевых товаров. Тот, кто без угрызений совести покупает контрафактную рубашку или сумку, вполне может не захотеть покупать контрафактные лекарственные препараты или электрооборудование. На этих двух рынках требуются различные стратегии борьбы с контрафакцией, и поэтому необходимо знать, на каком рынке продается тот или иной конкретный продукт.

Вполне возможно эффективно бороться с контрафакцией продуктов на первичном рынке, например с помощью информационных кампаний, указывающих на опасности приобретения контрафактных продуктов, но в отношении продуктов на вторичном рынке может оказаться необходимым вводить более строгие наказания.

Комплект материалов по цепочкам поставок, разработанный Группой Соединенного Королевства по преступности, связанной с IP [71], направлен на повышение уровня информированности о проблеме контрафактных товаров, поступающих в цепочки поставок законного бизнеса, и в нем содержатся рекомендации по способам защиты объектов интеллектуальной собственности. На рисунке 14 схематично изображен процесс, с помощью которого компания может уменьшить риски попадания контрафактных товаров в ее цепочку поставок.

Рисунок 14 – Защита прав интеллектуальной собственности (на основе комплекта материалов, подготовленного Группой Соединенного Королевства по преступности, связанной с IP [71])

Форум MMF разработал Руководство для правительств, в котором предлагается ряд мер, в том числе:

- введение изменений в нормативно-правовую базу в целях ограничения активирования контрафактных устройств в сетях электросвязи;
- ограничение импорта мобильных устройств и аксессуаров, которые не соответствуют отраслевым стандартам или не одобрены/не соответствуют законодательной и нормативной базе страны;
- создание необходимых альянсов с участием отрасли и органов власти и разработка решений для подтверждения оригинальных продуктов органами власти, потребителями и каналами сбыта;
- разработка согласованных и новаторских технологических решений, которые ограничивают возможность активирования контрафактных мобильных устройств в сетях электросвязи; и
- поддержка стандартов, которые ведут к усилению средств защиты (таких как уникальные индивидуальные идентификационные номера), ограничивающих производство контрафактных и других незаконных продуктов.

Такой подход неизбежно ведет дальше опоры только лишь на традиционные правоприменительные меры, приводя к блокированию работы таких устройств в сетях. И все же обеспечение исполнения, информационно-пропагандистские кампании и надзор за рынком по-прежнему будут иметь важное значение, а производители мобильных телефонов будут продолжать работать с национальными органами, когда это возможно.

10 Выводы

Контрафакция представляет собой растущую проблему, которая затрагивает все более широкий диапазон продуктов. В секторе ИКТ контрафакция в особой степени направлена на мобильные телефоны, и ежегодно продается около 250 млн. контрафактных мобильных телефонов, что составляет 15−20% от мирового рынка. Помимо чисто экономического воздействия на производителей подлинных продуктов (обесценивание торговой марки, потеря доходов, нарушение авторских прав и товарного знака, недобросовестная конкуренция), уполномоченных дилеров и правительства (поскольку налоги не уплачиваются, возникают дополнительные затраты по обеспечению соответствия применимому национальному законодательству, необходимо реагировать на угрозы национальной безопасности, теряются возможности трудоустройства), существуют также угрозы для здоровья, безопасности и конфиденциальности потребителей, аспектов государственной безопасности, а также отрицательные последствия для сетевых операторов (в связи с более низким

качеством обслуживания (QoS), проблемами, связанными с потенциальными помехами и электромагнитной совместимостью (ЭМС), а также прерыванием связи в сети). Большинство таких контрафактных мобильных телефонов производятся в одной стране Азии, и именно из этой страны поступает большинство контрафактных электронных компонентов, полученных в результате переработки в неформальном секторе электронных отходов из развитых стран, как это было определено в ходе слушаний в Сенатской комиссии по делам вооруженных сил США, посвященных контрафактным электронным компонентам в цепочке поставок систем обороны [9]. Вполне очевидно, что требуется сделать гораздо больше для идентификации источников контрафактного оборудования и борьбы с ними, пока такое оборудование не экспортируется по всему миру.

В большинстве случаев уже имеются правовые инструменты для борьбы с контрафакцией, но правоприменение все еще обеспечивается слабо. В отчете ОЭСР за 2008 год сделан вывод о том, что "масштабы и последствия контрафакции и пиратства столь значительны, что они могут вынудить правительства, промышленность и потребителей к принятию жестких и длительных мер. В связи с этим важнейшее значение имеет более эффективное правоприменение, а также необходимость помощи со стороны общества в борьбе с контрафакцией и пиратством. Полезным будет укрепление сотрудничества между правительствами и отраслью, а также улучшение сбора данных".

Правительства стали более активно заниматься этим вопросом, и многие из них проводят кампании по повышению уровня информированности, разрабатывая рекомендации и более строго преследуя нарушителей, как это отмечалось недавно в Китае. Необходимо, чтобы правительства не только укрепляли свои нормативные положения в области ПИС, но и выполняли Базельскую конвенцию для обеспечения того, чтобы использованное и отслужившее свой срок оборудование перерабатывалось, не нанося ущерба окружающей среде, а не приводило к развитию неформальной контрафактной экономики. Следует повсеместно внедрять этические практики утилизации.

Возможно, правительства также захотят увязать деятельность по надзору за рынком с деятельностью таможенных органов, чтобы укрепить способность по обнаружению контрафактных продуктов. Конфискованное контрафактное оборудование ИКТ следует рассматривать в качестве электронных отходов и перерабатывать в соответствии со схемами экологически безопасной утилизации отходов.

Компании и отрасли промышленности, затронутые контрафакцией, организовали информационные кампании и лоббируют свои интересы. Хотя, как представляется, необходимо повысить уровень осведомленности по вопросам контрафакции. В США Законом о полномочиях в сфере национальной обороны (NDAA) 2012 года на подрядчиков возложена полная ответственность за обнаружение поддельных компонентов и исправление любых случаев, когда поддельные компоненты попали в продукты.

Потребителям также необходимо знать об опасностях приобретения контрафактного оборудования и о том, что такое оборудование может не быть безопасным в использовании и не работать так же хорошо, как подлинные товары. Очевидно, что многие национальные и международные органы, а также производители, розничные продавцы и СМИ регулярно освещают те проблемы, которые контрафактные продукты представляют для потребителей. Но по-прежнему потребители часто принимают практическое решение покупать контрафактные товары, несмотря на потенциальные последствия, по-видимому на основе цены.

С контрафакцией также можно было бы бороться с помощью управления жизненным циклом оборудования, и не только цепочкой поставок, но и этапами полного жизненного цикла оборудования, связанными с возвратом, повторным использованием и утилизацией. Для управления жизненным циклом необходимы средства для идентификации и аутентификации элементов, а также процессы их надежного отслеживания. Тем не менее, отслеживание должно быть надлежащим и достаточным, чтобы оно выполняло свои цели, поскольку технологии автоматической идентификации и сбора данных (AIDC), такие как RFID, действительно представляют существенные проблемы в области конфиденциальности, так как объекты потенциально могут быть увязаны с теми, кому они принадлежат. Следует внимательно подходить к тому, чтобы в процессе разработки стандартов уважалась частная жизнь потребителей и на пользователей продуктов ИКТ не оказывалось давление через механизмы регистрации идентификаторов. Кроме того, потребителей следует защищать от произвольного отключения от сетей.

Как отмечалось ранее, в борьбе с контрафакцией могут применяться технология AIDC и стандарты управления цепочкой поставок.

Для борьбы с контрафакцией требуется сотрудничество всех отраслей промышленности. Правоприменительные органы, такие как таможенные органы, можно было бы поддержать с помощью некоторых общих инструментов (например, по проверке поддельных паспортов и банкнот), а также целого ряда механизмов, относящихся к конкретным секторам и продуктам, и целенаправленных действий при сотрудничестве государственного и частного секторов.

Сейчас в секторе мобильных телефонов существует ряд систем, основанных на регистрации IMEI, которые управляются или планируются отдельными администрациями и регуляторными органами для идентификации подлинных и законно импортируемых мобильных терминалов. Кроме того, существует целый ряд региональных инициатив по обмену информацией о мобильных оконечных устройствах незаконного происхождения. Такие механизмы могут создавать проблемы и для законных пользователей. Например, иностранный пользователь, приезжающий в страну и затем использующий в своем устройстве местную SIM-карту, может попасться в ловушку "белого" списка, когда он не сможет пользоваться своим устройством. Такие механизмы могут приводить к проблемам, связанным со свободным перемещением товаров. В других секторах ИКТ такие механизмы не существуют в связи с самим характером продуктов и структурой отраслей.

Даже хотя некоторые страны и задействовали успешные решения, полагаясь на IMEI для сдерживания распространения контрафактных мобильных телефонов, другие страны, особенно развивающиеся, все еще сталкиваются с существенными проблемами в нахождении эффективных решений борьбы с контрафактными устройствами. В настоящее время имеющиеся в некоторых странах решения основаны на блокировании в своих сетях мобильных телефонов с недействительными номерами IMEI, блокировании использования оборудования типа, не одобренного регуляторным органом, блокировании незаконного импорта таких устройств или на осуществлении других действий, направленных на повышение уровня информированности потребителей, принятии правоприменительных мер и внесении соответствующих изменений в законодательство на национальном уровне.

Основные международные организации по стандартизации занимались рассмотрением тем, касающихся борьбы с контрафакцией. В настоящее время не имеется, например, Рекомендации МСЭ, позволяющей сравнивать различные существующие системы борьбы с контрафакцией, где описывалась бы необходимая структура и рассматривались на глобальном уровне рабочие характеристики и вопросы функциональной совместимости. МСЭ и другие соответствующие заинтересованные стороны должны играть ключевую роль в содействии координации между заинтересованными сторонами, чтобы определить пути решения проблемы контрафактных устройств на международном и региональном уровнях. Кроме того, МСЭ поручено содействовать своим членам в принятии необходимых мер для предотвращения или выявления случаев подделки и/или дублирования уникальных идентификаторов устройств.

В настоящем Техническом отчете рассматриваются темы, имеющие отношение только к борьбе с контрафакцией, например, что такое контрафакция, какое она оказывает воздействие, конвенции в области ПИС и обеспечение их выполнения, промышленные форумы по борьбе с контрафакцией и организации, занимающиеся вопросами контрафакции. МСЭ следует продолжить изучение этого вопроса, чтобы помочь регуляторным органам защитить потребителей, операторов и правительства от отрицательного воздействия контрафактных устройств.

11 Участие МСЭ

В своей Резолюции 177 Полномочная конференция МСЭ 2010 года (ПК-10) "*предлагает далее Государствам-Членам и Членам Секторов* учитывать нормативно-правовые базы других стран, касающиеся оборудования, которое оказывает отрицательное воздействие на качество инфраструктуры электросвязи этих стран, в частности признавая проблемы развивающихся стран, связанные с контрафактным оборудованием" [72].

В Резолюции 79 ВКРЭ-14 "Роль электросвязи/информационно-коммуникационных технологий в борьбе с контрафактными устройствами электросвязи/информационно-коммуникационных технологий и в решении этой проблемы" и в Резолюции COM5/4 ПК-14 "Борьба с контрафактными устройствами электросвязи/информационно-коммуникационных технологий" МСЭ поручается заниматься решением вопроса, связанного с контрафактным оборудованием ИКТ.

Этот вопрос изучается в рамках Вопроса 8 11-й Исследовательской комиссии (ИК11), и МСЭ провел в Женеве в ноябре 2014 года семинар-практикум на тему "Борьба с контрафактным и некачественным оборудованием ИКТ" (http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx).

16-я и 17-я Исследовательские комиссии МСЭ-Т разработали Рекомендации, касающиеся идентификации и аутентификации объектов.

5-я Исследовательская комиссия МСЭ-Т (ИК5) отвечает за изучение методик проектирования для уменьшения экологического воздействия использования ИКТ с помощью таких средств, как утилизация.

Директор БСЭ учредил специальную группу по ПИС (http://www.itu.int/en/ITU-T/ipr/Pages/adhoc.aspx) для изучения политики в области патентов, руководящих указаний в области авторских прав на программное обеспечение и торговых марок, а также других соответствующих вопросов. Эта группа проводит свои собрания, начиная с 1998 года. Кроме того, МСЭ и ВОИС совместно организовывали симпозиумы, например по многоязычным наименованиям доменов в 2001 году (http://www.itu.int/mlds/) и по разрешению споров, связанных с информационно-коммуникационными технологиями и интеллектуальной собственностью, в 2009 году (http://www.wipo.int/amc/en/events/workshops/2009/itu/index.html). МСЭ также организовал в 2012 году заседания круглого стола по патентам, чтобы обеспечить нейтральное место для встречи представителей отрасли, органов по стандартам и регуляторных органов в целях обсуждения вопроса о том, адекватно ли отвечают нынешняя патентная политика и действующая в отрасли практика потребностям различных заинтересованных сторон (http://www.itu.int/en/ITU-T/Workshops-and-Seminars/patent/Pages/default.aspx). До настоящего времени эта группа не занималась вопросом контрафакции.

МСЭ предстоит сыграть определенную роль в решении проблемы контрафактного оборудования ИКТ.

В отчете "Регулирование и защита потребителей в конвергентной среде" (март 2013 г.), подготовленном ИК1 Сектора развития электросвязи МСЭ (МСЭ-D) в рамках Резолюции 64 (Хайдарабад, 2010 г.) Всемирной конференции по развитию электросвязи МСЭ, в качестве одной из задач регуляторных органов упоминается защита новаторов, разработчиков и потребителей от контрафакции и пиратства, связанных с онлайновым (и все чаще трансграничным) предоставлением продуктов и услуг.

Согласно руководящим указаниям для развивающихся стран по созданию в различных регионах лабораторий по тестированию для оценки на соответствие, которые были опубликованы Сектором развития электросвязи МСЭ в мае 2012 года, Государства-Члены отметили, что контрафактное оборудование усугубляет проблемы, связанные с соответствием и функциональной совместимостью (http://www.itu.int/ITU-D/tech/ConformanceInteroperability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf). Отмечается, что "подозрения в выбросе на рынок некачественных продуктов, которые не прошли тестирование в других странах, является еще одной причиной беспокойства, наряду с импортом и широким использованием контрафактных продуктов. Одна из основных частей ответа на такую озабоченность состоит в наличии крепкого режима одобрения типа и лабораторий по тестированию, работающих на основе набора технических стандартов, режима тестирования и возможностей по тестированию для утверждения и мониторинга технологий связи, развернутых на рынке, которые подкрепляются надзором, аудитом и обеспечением применения. При отсутствии в стране или регионе разработанных технических требований, режима одобрения типа и лабораторий по тестированию рынок остается в существенной степени незащищенным". Тестирование и функциональная совместимость могут сильно ограничиваться, когда в продукте учтены многочисленные стандарты различных органов. Следует признать, что, хотя режим тестирования представляется привлекательным, одного лишь его вряд ли достаточно, чтобы реальным образом изменить ситуацию для борьбы с контрафакцией.

Следует отметить, что поскольку контрафакторы становятся все более искушенными, контрафактные продукты могут соответствовать установленным техническим требованиям и быть функционально совместимыми с подлинными продуктами. По существу, контрафактные продукты могут соответствовать набору надлежащих технических стандартов и проходить тест на соответствие и функциональную совместимость. В таком случае точно отличить контрафактные продукты от подлинных может только владелец товарного знака путем оценки продукта.

Проблема контрафактного оборудования ИКТ рассматривалась на Региональном семинаре-практикуме МСЭ по преодолению разрыва в стандартизации (ПРС) для Арабского и Африканского регионов (Алжир, 26−28 сентября 2011 г.), и была разработана директива для содействия обмену

информацией на региональном уровне путем создания базы данных, содержащей включенные в "черный" список контрафактные продукты (http://www.itu.int/ITU-T/newslog/ITU+Regional+Workshop+On+Bridging+The+Standardization+Gap+For+Arab+And+Africa+Regions+Interactive+Training+Session+And+Academia+Session.aspx).

В ходе информационной сессии по оценке соответствия и проверке на функциональную совместимость, проводившейся Консультативной группой по стандартизации электросвязи (КГСЭ) МСЭ-Т (Женева, 13 января 2012 г.), и Форума МСЭ по соответствию и функциональной совместимости для Арабского и Африканского регионов (Тунис, 5−7 ноября 2012 г.) подчеркивался сделанный в Арабском регионе вывод о том, что контрафактное оборудование представляет собой сложную проблему, особенно на рынке мобильных телефонов, а также подчеркивалась необходимость глобального сотрудничества в этой области (http://www.itu.int/ITU-D/tech/events/2012/CI_ARB_AFR_Tunis_November12/Presentations/Session5/CI%20Forum%202012_Tunis_AAlDin_S5_4.pdf), [http://www.itu.int/dms_pub/itu-t/oth/06/5B/T065B00000E0005PPTE.pptx].

Вопросы, касающиеся кражи мобильных устройств, "серого" рынка и контрафактных устройств, а также их воздействия на отрасль, операторов, правительства и пользователей, рассматривались на собрании ассоциаций регуляторных органов, которое было организовано Сектором развития электросвязи МСЭ (Шри-Ланка, Коломбо, 1 октября 2012 г.) в соответствии с Резолюцией 48 (Пересм. Хайдарабад, 2010 г.) "Укрепление сотрудничества регуляторных органов в области электросвязи", в которой МСЭ предлагается организовывать и координировать деятельность, а также содействовать деятельности, которая содействует обмену информацией между регуляторными органами и ассоциациями регуляторных органов по ключевым вопросам регулирования на международном и региональном уровнях. Представители десяти региональных ассоциаций регуляторных органов, включая ARCTEL-CPLP, AREGNET, ARTAC, EMERG, FRATEL, REGULATEL, OCCUR, FTRA, SATRC и АТСЭ, подчеркнули, что в связи с этим очень полезными могут быть действия на региональном уровне, такие как:

- обмен базами данных GSM и CDMA по "черным" спискам с помощью подписания двусторонних или многосторонних соглашений;
- соблюдение в отрасли рекомендаций по безопасности, направленных на предотвращение изменения программ дублирования IMEI или серийного идентификационного номера электронного оборудования производителя;
- создание регуляторных налоговых и/или таможенных механизмов, которые обеспечивают больший контроль применительно к импортируемым радиотелефонным трубкам, предотвращая вывоз или реэкспорт украденных мобильных оконечных устройств и/или их частей;
- проведение кампаний по повышению уровня информированности населения о важности сообщать о краже или потере мобильных оконечных устройств.

Многие региональные ассоциации изложили свой опыт в данной сфере и признали, что это важнейшая проблема, которую необходимо решать в сотрудничестве с отраслью и операторами. На собрании ассоциаций регуляторных органов была принята рекомендация о том, чтобы МСЭ в сотрудничестве с Ассоциацией GSM провели исследования по вопросам, касающимся кражи мобильных устройств, "серого" рынка и контрафактных устройств, и представили руководящие указания и рекомендации (http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/FinalReport_RA12.pdf).

12 Справочные материалы

[1] *The Economic Impact of Counterfeiting and Piracy*, OECD, June 2008.

[2] http://www.oecd.org/dataoecd/57/27/44088872.pdf

[3] http://www.icc-ccs.org/icc/cib

[4] *Estimating the global economic and social impacts of counterfeiting and piracy*. http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Global%20Impacts%20-%20Final.pdf

[5] Intellectual Property Rights Fiscal Year 2100 Seizure Statistics U.S. Customs and Border Protection. http://www.ice.gov/doclib/iprcenter/pdf/ipr-fy-2011-seizure-report.pdf

[6] hhttp://www.havocscope.com/counterfeit-hp-printing-supplies

[7] http://www.spotafakephone.com/

[8] IDC February 2012 http://www.idc.com/getdoc.jsp?containerId=prUS23297412

[9] http://www.levin.senate.gov/newsroom/press/release/background-memo-senate-armed-services-committee-hearing-on-counterfeit-electronic-parts-in-the-dod-supply-chain

[10] *Defence Industrial Base Assessment: Counterfeit Electronics*, January 2010 http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf

[11] http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf HR 1540 SEC. 818

[12] In *WIPO Intellectual Property Handbook* http://www.wipo.int/export/sites/www/about-ip/en/iprm/pdf/ip_handbook.pdf

[13] UK IP Toolkit 2009.

[14] http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html

[15] http://www.wipo.int/treaties/en/ip/washington

[16] www.wcoipm.org и

http://www.wcoomd.org/en/topics/enforcement-and-compliance/activities-and-programmes/ep_intellectual_property_rights.aspx

[17] http://www.canadainternational.gc.ca/g8/summit-sommet/2009/ipeg.aspx?view=d

[18] http://www.unece.org/trade/wp6/SectoralInitiatives/MARS/MARS.html

[19] http://www.ipo.gov.uk/ipenforce/ipenforce-resources.htm

[20] http://www.aca.or.ke

[21] http://www.iccwbo.org/bascap/id6169/index.html

[22] http://www.iccwbo.org/bascap/id7608/index.html

[23] http://www.pasdirectory.com

[24] http://www.iccwbo.org/bascap/id42204/index.html

[25] http://www.iccwbo.org/policy/ip/id2950/index.html

[26] https://iacc.org

[27] http://www.ascdi.com/asna/vendors/counterfit_task_force/default.aspx

[28] http://www.anticounterfeitingforum.org.uk

[29] http://archive.basel.int/convention/basics.html

[30] http://www.ier.org.tw/smm/6_PAS_141_2011_Reuse_Of_WEEE_And_UEEE.pdf

[31] http://www.bbc.co.uk/panorama/hi/front_page/newsid_9483000/9483148.stm

[32] http://www.bbc.co.uk/news/world-europe-10846395

[33] Recycling – From E-Waste to Resources, UNEP, 2009.

[34] Directive 2002/96/EC.

[35] BSI PAS141:2011, *Reuse of used and waste electrical and electronic equipment* (UEEE and WEEE). Process Management Specification (March 2011)
http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030245346

[36] http://www.numberingplans.com/?page=analysis&sub=imeinr

[37] IMEI Allocation and Approval Process, Version 7.0, GSMA, 31 October 2013.

[38] http://www.gsma.com/imei-database

[39] http://www.dailytrust.com.ng/index.php?option=com_content&view=article&id=160408:kenya-to-demobilise-all-fake-phones&catid=1:news&Itemid=2

[40] Annual Report of the National Commission for the State Regulation of Communications and Informatization for 2012. http://en.nkrzi.gov.ua/1324743665/

[41] GS1 EPC Tag Data Standard 1.6, 9 September 2011.
http://www.gs1.org/gsmp/kc/epcglobal/tds/tds_1_6-RatifiedStd-20110922.pdf

[42] ISO/IEC 15459, *Unique identifiers*.

Part 1:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 1: Individual transport units*.

Part 2:2006, *Information technology – Unique identifiers – Registration procedures*.

Part 3:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 3: Common rules*.

Part 4:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 4: Individual products and product packages*.

Part 5:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 5: Individual returnable transport items (RTIs)*.

Part 6:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 6: Groupings*.

Part 8:2009, *Information technology – Part 8: Grouping of transport units*.

[43] ISO 6346:1995, *Контейнеры грузовые. Кодирование, идентификация и маркировка*.

[44] ISO 3779:2009, *Транспорт дорожный. Идентификационный номер автомобилей (VIN). Содержание и структура*.

[45] ISO 10486:1992, *Автомобили легковые. Идентификационный номер автомобильного радиоприемника (CRIN)*.

[46] ISO 2108:2005, *Информация и документация. Международный стандартный книжный номер (ISBN)*.

[47] ISO 3297:2007, *Документация. Международный стандартный номер серийного издания (ISSN)*.

[48] ISO 12931:2012, *Критерии эффективности для идентификационных растворов, используемых для борьбы с подделками материальных изделий*.

[49] http://www.uidcenter.org/learning-about-ucode

[50] Recommendation ITU-T X.668 (2008) | ISO/IEC 9834-9:2008, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Registration of object identifier arcs for applications and services using tag-based identification*.

[51] Recommendation ITU-T F.771 (2008), *Service description and requirements for multimedia information access triggered by tag-based identification*.

[52] Recommendation ITU-T H.621 (2008), *Architecture of a system for multimedia information access triggered by tag-based identification*.

[53] ISO 28219:2009, Упаковка. Этикетирование и прямая маркировка изделий линейным штрих–кодом и двумерными символами.

[54] ISO 22742:2010, *Упаковка. Линейный штрих-код и двумерные обозначения на упаковке продукта*.

[55] ISO 15394:2009, *Упаковка. Штриховой код и двумерные символы, используемые на этикетках для отгрузки, транспортировки и получения груза*.

[56] ISO/IEC 15963:2009, *Информационные технологии. Идентификация радиочастоты для менеджмента объекта. Уникальная идентификация радиочастотных тегов*.

[57] ISO/IEC 29167-1:2014, *Information technology – Automatic identification and data capture techniques – Part 1: Security services for RFID air interfaces*.

[58] ISO/IEC TR 24729-4:2009, *Информационные технологии. Идентификация радиочастоты с целью управления изделием. Руководящие указания по внедрению. Часть 4. Безопасность теговых данных*.

[59] http://www.gs1.org/gsmp/kc/epcglobal

[60] Recommendation ITU-T X.509 (2012) | ISO/IEC 9594-8:2014, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[61] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[62] IETF RFC 3279 (2002), *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[63] http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/Procedures%20and%20Facilitation/safe_package/safe_package_I_2011.pdf

[64] IEC/TS 62668-1 ed2.0 (2014), *Process management for avionics – Counterfeiting prevention – Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components*.

[65] IEC/TS 62668-2 ed1.0 (2014), *Process management for avionics – Counterfeit prevention – Part 2: Managing electronic components from non-franchised sources*.

[66] На основе Регламента ЕС № 765/2008 по надзору за рынком, ст. 2 (17), http://www.unece.org/fileadmin/DAM/trade/wp6/documents/2009/WP6_2009_13e_final.pdf

[67] Recommendation M. on the: *Use of Market Surveillance Infrastructure as a Complementary Means to Protect Consumers and Users against Counterfeit Goods*. http://www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_M.pdf

[68] http://www.nia.din.de/gremien/NA+043-01-31+AA/en/54773446.html

[69] http://www.anticounterfeitingforum.org.uk/best_practice.aspx

[70] http://www.cti-us.com/CCAP.htm]

[71] http://www.ipo.gov.uk/ipctoolkit.pdf

[72] http://www.itu.int/ITU-D/tech/NGN/ConformanceInterop/PP10_Resolution177.pdf

[73] Establishing Conformity and Interoperability Regimes – Basic Guidelines (ITU, 2014).

[74] *Guidelines for developing countries on establishing conformity assessment test labs in different regions*, ITU, 2012: www.itu.int/ITU-D/tech/ConformanceInteroperability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf

[75] IEC 62321:2008, *Electrotechnical products – Determination of levels of six regulated substances (lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls, polybrominated diphenyl ethers)*.

[76] Рекомендация МСЭ-Т E.164 (2010), *Международный план нумерации электросвязи общего пользования*.

[77] ISO/IEC 15962:2013, *Информационные технологии. Распознавание радиочастот для управления элементом. Протокол данных: Правила кодирования данных и логические функции памяти*.

[78] ISO/IEC 15961:2004, *Информационные технологии. Распознавание радиочастот для управления элементом. Протокол данных: прикладной интерфейс*.

[79] Рекомендация МСЭ-Т X.1255 (2013), *Структура обнаружения информации по управлению определением идентичности*.

[80] ISO/IEC 15420:2009, *Информационные технологии. Методы автоматической идентификации и выделения данных. Спецификация символики штрихкода. EAN/UPC*.

[81] ISO/IEC 16388:2007, *Информационные технологии. Методы автоматической идентификации и выделения данных. Спецификации на символику штрихового кода. Код 39*.

[82] ISO/IEC 15417:2007, *Информационные технологии. Методы автоматической идентификации и выделения данных. Спецификация на символику штрихового кода. Код 128*.

[83] ISO/IEC 15438:2006, *Информационные технологии. Методы автоматической идентификации и выделения данных. Спецификации на символику штрихкода. PDF417*.

[84] ISO/IEC 16023:2000, *Информационные технологии. Международная спецификация символики. Максикод*.

[85] ISO/IEC 18004:2006, *Информационные технологии. Методы автоматической идентификации и выделения данных. Спецификация символики штрихового кода QR 2005*.

[86] ISO/IEC 16022:2006, *Информационные технологии. Методы автоматической идентификации и выделения данных. Спецификация символики штрихового кода матрицы данных*.

[87] DIN 66401 (2010), *Unique Identification Mark (UIM).*

[88] ANSI MH10.8.2-2010, *Data Identifier and Application Identifier Standard.*

[89] ANSI/HIBC 2.3-2009, *The Health Industry Bar Code (HIBC) Supplier.*

[90] ISO/IEC 7816-6:2004, *Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 6. Элементы межотраслевых данных для обмена информацией*.

[91] ISO 14816:2005, *Телематика для дорожного транспорта и транспортного движения. Идентификация автоматических транспортных средств и оборудования. Структура нумерации и данных*.

[92] ANSI INCITS 256-2007, *Radio Frequency Identification (RFID).*

[93] ANSI INCITS 371.1-2003, *Information technology - Real Time Locating Systems (RTLS) Part 1: 2.4 GHz Air Interface Protocol.*

[94] ISO/IEC 18000-6:2013, *Информационные технологии. Радиочастотная идентификация для управления элементом данных. Часть 6. Параметры для связи через радиоинтерфейс на частотах от 860 МГц до 960 МГц. Общие положения*.

[95] ISO/IEC 18000-3:2010, *Информационные технологии. Радиочастотная идентификация для управления элементом данных. Часть 3. Параметры для связи через радиоинтерфейс на частотах 13,56 МГц.*

[96] ISO 11784:1996, *Идентификация животных радиочастотным кодом. Структура кода*.

[97] ISO 11785:1996, *Идентификация животных по радиочастотным сигналам. Техническая концепция*.

[98] ISO/IEC 18000 (все части), *Информационные технологии. Радиочастотная идентификация для управления элементом данных*.

[99] ISO 17363:2013, *Применение RFID для управления поставками. Грузовые контейнеры*.

[100] ISO 17364:2013, *Прикладные программы цепи поставок RFID. Возвратные транспортные элементы и возвратные упаковочные элементы*.

[101] ISO 17365:2013, *Прикладные программы цепи поставок RFID. Транспортные единицы.*

[102] ISO 17366:2013, *Прикладные программы цепи поставок RFID. Упаковка продуктов.*

[103] ISO 17367:2013, *Прикладные программы цепи поставок RFID. Маркировка продуктов.*

[104] ISO 18185 (все части), *Контейнеры грузовые. Электронные печати*.

[105] ISO/IEC 29160:2012, Информационные технологии. Радиочастотная идентификация для управления предметом. Эмблема RFID.

[106] ISO/IEC 15693, *Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с радиосвязью через большой зазор*.

[107] ISO 28000:2007, *Системы менеджмента безопасности цепи поставок*.

[108] ISO 28001:2007, *Системы менеджмента безопасности цепи поставок. Наилучшие методы обеспечения безопасности в цепи поставок, оценки и планы. Требования и руководящие указания*.

[109] ISO 28003:2007, *Системы менеджмента безопасности для цепи поставок. Требования к органам аудита и сертификации систем менеджмента безопасности цепи поставок*.

[110] ISO 28004-1:2007, *Системы менеджмента безопасности цепи поставок. Руководство по внедрению ISO 28000. Часть 1. Основные принципы*.

[111] ISO 28005-2:2011, *Системы менеджмента безопасности для цепи поставок. Электронный допуск в порт (EPC). Часть 2. Основные элементы данных*.

[112] SAE AS5553 (2013), *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*.

[113] SAE ARP6178 (2011), *Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors*.

[114] SAE AS6081 (2012), *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors Counterfeit Electronic Parts; Avoidance Protocol, Distributors*.

[115] SAE AS6171 (2010), *Test Methods Standards; Counterfeit Electronic Parts*.

[116] ISO 16678:2014, *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*.

[117] IDEA-STD-1010A (2006), *Acceptability of Electronic Components Distributed in the Open Market*.

[118] IDEA-QMS-9090 (2013), *Quality Management System Standard*.

Глоссарий

AC	Allocation Class		Класс распределения
ADI	Aerospace and Defence Identifier		Идентификатор авиакосмической и оборонной промышленности
AIDC	Automatic Identification and Data Capture		Автоматическая идентификация и сбор данных
ALE	Application Layer Event		Событие прикладного уровня
AWP	Automated Working Place	APM	Автоматизированное рабочее место
CB	Certification Body		Сертификационный орган
CBV	Core Business Vocabulary		Терминология профильного бизнеса
cc	class code		код класса
CD	Compact Disc		Компактный диск
CDMA	Code Division Multiple Access		Многостанционный доступ с кодовым разделением
CDR	Call Detail Record		Записи данных о вызовах
CEIR	Central Equipment Identity Register		Центральный регистр идентификации оборудования
CIPS	Comprehensive Information Protection System		Система всесторонней защиты информации
CoPC	Certification of Personnel Competencies		Сертификация компетенции персонала
DB	DataBase		База данных
DCI	Discovery, Configuration and Initialisation		Обнаружение, конфигурация и инициализация
DNS	Domain Name System		Система наименований доменов
DVD	Digital Versatile Disc		Универсальный цифровой диск
EIR	Equipment Identity Register		Регистр идентификации оборудования
EMC	Electromagnetic Compatibility ЭМС		Электромагнитная совместимость
EPC	Electronic Product Code		Код электронных продуктов
EPCIS	EPC Information Service		Информационная услуга EPC
GDTI	Global Document Type Identifier		Глобальный идентификатор типа документа
GIAI	Global Individual Asset Identifier		Глобальный идентификатор индивидуального имущества
GID	General Identifier		Общий идентификатор
GII	Genuine IMEI Implant programme		Программа внедрения подлинных IMEI
GINC	Global Identification Number for Consignment		Глобальный идентификационный номер партии товара
GLN	Global Location Number		Глобальный номер предприятия
GRAI	Global Returnable Asset Identifier		Глобальный идентификатор возвратного имущества
GSIN	Global Shipment Identification Number		Глобальный идентификационный номер поставки
GSM	Global System for Mobile communications		Глобальная система подвижной связи

GSRN	Global Service Relation Number		Глобальный номер услуги
GTIN	Global Trade Item Number		Глобальный номер товара
HF	High Frequency	ВЧ	Высокая частота
ic	identification code		Идентификационный код
IC	Integrated Circuit		Интегральная схема
ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
ID	Identification		Идентификация
IMEI	International Mobile Equipment Identity		Международный идентификатор аппаратуры подвижной связи
IP	Intellectual Property	ИС	Интеллектуальная собственность
IP	Internet Protocol		Протокол Интернета
IPM	Interface Public-Members		Интерфейс для членов из частного сектора
IPR	Intellectual Property Rights	ПИС	Права интеллектуальной собственности
ISBN	International Standard Book Number		Международный стандартный книжный номер
ISSN	International Standard Serial Number		Международный стандартный номер серийного издания
IT	Information Technology	ИТ	Информационные технологии
LLRP	Low Level Reader Protocol		Протокол считывающего устройства низкого уровня
LTE	Long-Term Evolution		Долгосрочное развитие
ME	Mobile Equipment		Оборудование подвижной связи
MEID	Mobile Equipment Identity		Идентификатор оборудования подвижной связи
MIIM	Mobile Item Identification and Management		Идентификация мобильных объектов и управление ими
MRA	Mutual Recognition Agreement		Соглашение о взаимном признании
MSC	Mobile Switching Centre		Центр коммутации подвижной связи
MSISDN	Mobile Subscriber Integrated Services Digital Network		Цифровая сеть с интеграцией служб абонентов подвижной связи
NIR	Non-Ionizing Radiation		Неионизирующее излучение
OID	Object Identifier		Идентификатор объекта
ONS	Object Naming Service		Услуга по присвоению наименований объектам
QoS	Quality of Service		Качество обслуживания
RF	Radio Frequency	РЧ	Радиочастота
RFID	Radio Frequency Identification		Радиочастотная идентификация
RM	Reader Management		Управление считывающим устройством
RoHS	Restriction of Hazardous Substances		Ограничение содержания опасных веществ
RP	Reader Protocol		Протокол считывающего устройства
RUIM	Removable User Identity Module		Съемный модуль идентификации пользователя
SFP	Security Features Provider		Поставщик средств защиты

SGLN	Global Location Number with or without Extension		Глобальный номер предприятия с расширением или без расширения
SGTIN	Serialized Global Trade Item Number		Сериализованный глобальный номер товара
SIM	Subscriber Identity Module		Модуль идентификации абонента
SLDc	Second Level Domain code		Код домена второго уровня
SMD	Surface-Mounted Device		Устройство, предназначенное для монтажа на поверхности
SMS	Short Message Service		Служба передачи коротких сообщений
SNMP	Simple Network Management Protocol		Простой протокол управления сетью
SS7	Signalling System No. 7		Система сигнализации № 7
SSCC	Serial Shipping Container Code		Серийный код транспортной упаковки
TAC	Type Allocation Code		Код распределения типа
TC	Technical Committee	ТК	Технический комитет
TDS	Tag Data Standard		Стандарт данных маркера
TDT	Tag Data Translation		Перевод данных маркера
TID	Tag ID		Маркер ID
TLDc	Top Level Domain code		Код домена верхнего уровня
TV	TeleVision	ТВ	Телевидение
UHF	Ultra High Frequency		УВЧ Ультравысокая частота
UII	Unique Item Identifier		Уникальный идентификатор элемента
UIM	Unique Identification Mark		Уникальный идентификационный знак
UMTS	Universal Mobile Telecommunications System		Универсальная система подвижной электросвязи
UPC	Universal Product Code		Универсальный товарный код
URL	Uniform Resource Locator		Универсальный указатель ресурса
USB	Universal Serial Bus		Универсальная последовательная шина
WG	Working Group	РГ	Рабочая группа

Приложение A
Системы идентификации контрафактных мобильных устройств

Как излагается ранее в настоящем Техническом отчете, контрафактные мобильные устройства вызывали особую озабоченность и был предпринят ряд инициатив для ограничения их распространения. Некоторые из описанных схем первоначально были предназначены для обеспечения импорта мобильных устройств в соответствии с законным порядком (т. е. чтобы они не были контрабандными), и впоследствии они оценивались на предмет применимости для подтверждения того, что устройства не являются контрафактными. Такие схемы также имеют много общих характеристик с инициативами, специально предназначенными для борьбы с контрафакцией, которые основаны на аутентификации уникальных идентификаторов (IMEI).

В последующих разделах представлены примеры мер, принимаемых национальными властями и на региональном уровне.

A.1 Примеры мер, принимаемых национальными администрациями и регуляторными органами

A.1.1 Азербайджан

Система регистрации мобильных устройств (MDRS) (http://www.rabita.az/en/c-media/news/details/134) была создана в информационно-вычислительном центре (ИВЦ) Министерства связи и информационных технологий в соответствии с "Правилами регистрации мобильных устройств", утвержденными решением № 212 Кабинета министров Азербайджанской Республики от 28 декабря 2011 года.

Цель регистрации мобильных устройств состоит в том, чтобы противодействовать импорту низкокачественных устройств неизвестного происхождения, которые не соответствуют требуемым техническим стандартам, например ограничивающим опасные электромагнитные излучения, и чтобы увеличивать признание и конкурентоспособность компаний-производителей. Система регистрации предотвращает использование потерянных/украденных мобильных устройств и тех устройств, которые были незаконно ввезены в страну.

Начиная с 1 марта 2013 года, операторы подвижной связи ежедневно включают номера IMEI мобильных устройств, используемых в Азербайджане, в систему централизованной базы данных. Министерство связи и информационных технологий сообщало о том, что после внедрения MDRS было зарегистрировано более 12 млн. устройств GSM. Было разрешено продолжить работу примерно 300 тыс. устройств, не соответствующих стандартам, с использованием их нынешних номеров мобильных телефонов, но любые новые не соответствующие стандартам устройства работать в стране не будут (http://www.mincom.gov.az/media-en/news-2/details/1840).

Номера IMEI всех мобильных устройств, которые использовались в сети до 1 мая 2013 года, рассматривались как зарегистрированные и поэтому свободно работали в сетях. После начала работы системы регистрации номер IMEI каждого мобильного устройства, ввезенного в страну для личного пользования (с SIM-картой одного из операторов подвижной связи страны), следует регистрировать в течение 30 дней с даты его подключения к сети. Это правило не применяется к мобильным устройствам, находящимся в роуминге, где используются SIM-карты, выданные иностранными операторами.

Абоненты могут определить законность своих устройств на основе их номеров IMEI с использованием специальной веб-страницы (imei.az) или с помощью сообщений SMS.

Система централизованной базы данных создана в информационно-вычислительном центре (ИВЦ) Министерства связи и информационных технологий, и наряду с этим операторы подвижной связи установили необходимое оборудование, синхронизированное с централизованной базой данных. Программное обеспечение для MDRS было разработано местными специалистами.

A.1.2 Бразилия

SIGA − Комплексная система управления устройствами

В постановлении об услугах подвижной связи Национального агентства электросвязи Бразилии (Anatel) определяется, что операторам следует только предоставлять доступ к своим сетям и что пользователям следует использовать только те устройства, которые были сертифицированы Anatel (Статья 8, раздел IV, и Статья 10, раздел V, Постановления об услугах подвижной связи, утвержденного резолюцией 477/2007[9]). На основе этого Anatel настаивало на том, что операторы подвижной связи должны совместно внедрить технологическое решение, направленное на сокращение использования несертифицированных мобильных устройств с поддельным или скопированным IMEI.

В разработанном плане действий по выполнению этого обязательства, представленном операторами, кратко излагаются, среди прочего, технологическое решение, которое должно быть внедрено; возможные критерии, основанные на реальных пользователях, для максимального уменьшения воздействия на население; критерии, которые должны внедряться для новых пользователей после того, как решение начнет действовать, с тем чтобы получить доступ в сеть могли только те устройства, которые соответствуют постановлению Anatel; критерии, которые должны внедряться для пользователей подвижной связи, чтобы не создавать неудобств пользователям или иностранным пользователям; кампании по повышению уровня информированности.

Этот план действий был утвержден Anatel в 2012 году с учетом технических и регуляторных аспектов. Решение получило название SIGA − Комплексная система управления устройствами, которая разрабатывается на основе следующих технических исходных положений:

- централизованное решение, выработанное совместно всеми операторами подвижной связи Бразилии;
- комплексное решение с операторами платформ подвижной связи;
- автоматизированное решение, которое дает возможность ввода информации с незначительным участием человека;
- основано на масштабируемых и расширяемых росте и сложности;
- является динамичным и гибким, с правилами, которые со временем могут корректироваться;
- включает несколько источников информации, такие как записи данных о вызовах (CDR) и данные операторов систем управления, включая, среди прочего, при необходимости использование международных баз данных;
- эффективно позволяет принимать меры для сдерживания использования незаконных устройств;
- позволяет максимально сокращать потенциальное воздействие на постоянных конечных пользователей;
- является надежным и безопасным.

В настоящее время техническую работу SIGA осуществляет ABR Telecom[10] − техническая ассоциация, созданная как совместное предприятие большинства операторов электросвязи Бразилии для разработки, внедрения и эксплуатации централизованных технических решений для рынка электросвязи Бразилии.

В рамках этого проекта отмечается крепкое взаимодействие со всеми другими сторонами, участвующими в обеспечении успеха SIGA, такими как Anatel, таможенные органы, Ассоциация операторов (SindiTelebrasil), операторы, производители оборудования, Союз производителей (ABINEE) и компания ABR Telecom. Кроме того, этот вопрос является комплексным, поскольку он охватывает все сферы деятельности операторов, отдельных участников рынка и конечных пользователей, и поэтому требуется тщательное обсуждение всех действий.

---

9 http://legislacao.anatel.gov.br/resolucoes/2007/9-resolucao-477

10 http://www.abrtelecom.com.br

SIGA активно занимается сетью операторов с марта 2014 года, осуществляя сбор требуемой информации для определения размера рынка устройств, которые не соответствуют действующим в Бразилии нормативным положениям, с тем чтобы все заинтересованные стороны могли определить меры, необходимые для изъятия таких контрафактных, некачественных и неразрешенных устройств из сети с минимальным воздействием на потребителей.

Одна из возможных обсуждаемых мер по выполнению этого исходного требования состоит в создании унаследованной базы данных, содержащей все случаи (уникальная связь терминала и его пользователей), при которых разрешено продолжать эксплуатацию сети, но блокируется доступ к сети для любого нового ненадлежащего терминала. В этом смысле воздействие на пользователя существенно сокращается, и унаследованная база данных прекратит свое существование по мере сменяемости устройств.

Кроме того, важно включать в проводимые обсуждения структуры, представляющие пользователей, и внедрить прочную схему связи, прежде чем будут приняты любые меры, которые непосредственно воздействуют на пользователей (такие как блокирование или приостановка действия устройства).

В связи с этим схема связи SIGA разрабатывается совместно операторами, Anatel и Союзом производителей. Схему связи следует внедрять во всех этих структурах скоординированным образом по всем потребительским каналам (таким как рекламные сообщения, счета операторов и центры обработки вызовов), которые демонстрируют пользователям преимущества приобретения законных и сертифицированных терминалов и риск, который они берут на себя, пользуясь контрафактными и некачественными терминалами в рамках бразильского сценария.

Дополнительную информацию по техническом аспектам этого проекта можно получить непосредственно в Национальном агентстве электросвязи Anatel администрации Бразилии.[11]

A.1.3 Колумбия

В 2011 году Министерство информационно-коммуникационных технологий опубликовало Указ 1630 по созданию механизмов, направленных на контролирование выпуска на рынок и продажи как новых, так и использованных оконечных устройств и на создание двух типов централизованных баз данных: одной с регистром номеров IMEI оконечных устройств, о которых сообщалось как об украденных или потерянных, которая не допускает их использование или активирование, и другой базы данных с регистром зарегистрированных номеров IMEI для оконечных устройств, законно импортированных или произведенных в стране и связанных с идентификационным номером владельца или абонента.

Закон 1453 от 24 июня 2011 года о безопасности граждан предусматривает положение о приговоре в виде лишения свободы сроком от 6 до 8 лет для тех лиц, кто занимался подделкой, перепрограммированием, перемаркировкой или изменением IMEI мобильного устройства, и для тех лиц, активированные устройства которых являются, по сообщениям, украденными. Кроме того, переделанное оборудование конфискуется (http://www.gsma.com/latinamerica/wp-content/uploads/2012/05/Final-CITEL-Resolution-on-Handset-Theft.pdf).

Эти инициативы были приняты для контролирования продаж и использования украденных мобильных устройств, но, вероятно, также окажут воздействие на использование контрафактных продуктов.

A.1.4 Египет

В 2008 году Национальный регуляторный орган электросвязи (NTRA) создал департамент по надзору за рынком в целях поддержки своей деятельности по одобрению типа. В 2010 году в Египте была введена система для борьбы с использованием контрафактного оконечного оборудования подвижной связи. В этой системе используется база данных IMEI GSMA для еженедельного обновления "белого" списка IMEI TAC и базы данных центрального регистра идентификации оборудования (EIR) – IMEI. Это решение направлено на ограничение использования радиотелефонных трубок с незаконными, поддельными, недействительными и скопированными IMEI, на борьбу с кражей радиотелефонных трубок, а также на снятие опасений в области здоровья и безопасности.

[11] prre@anatel.gov.br

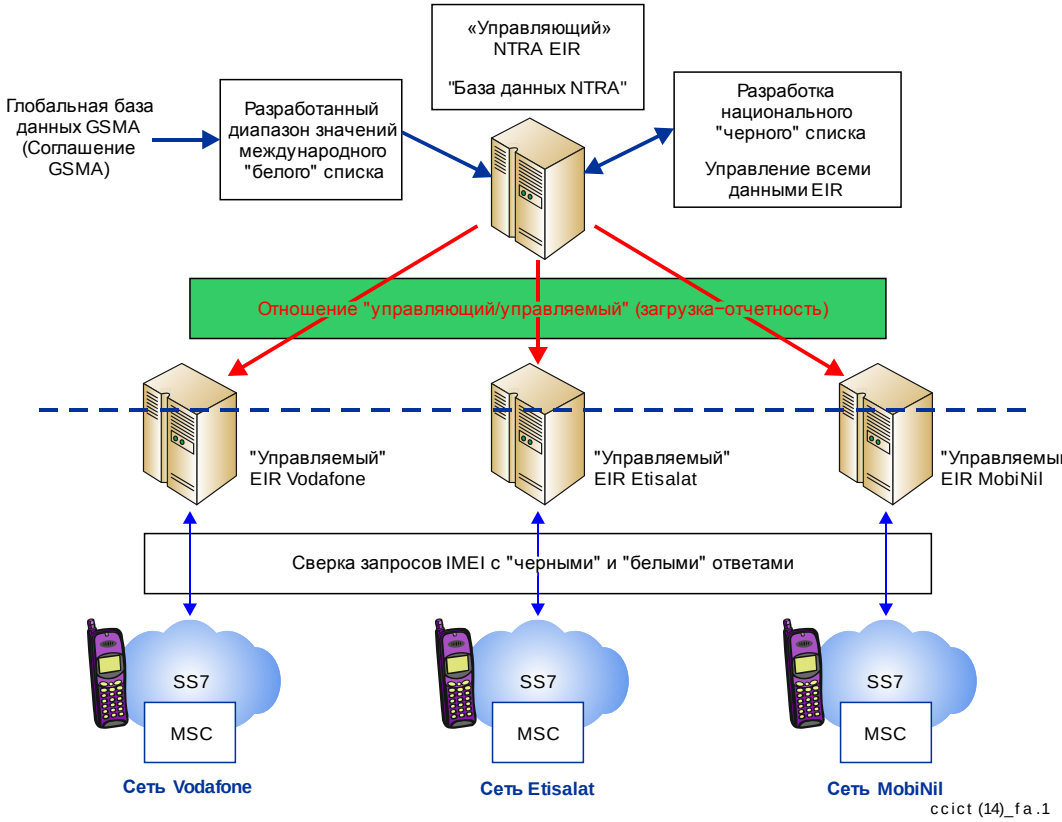


Рисунок A.1 – Решение в области центральной базы данных EIR IMEI в Египте

По данным NTRA, имеется 3,5 млн. мобильных телефонов с незаконным кодом IMEI 13579024681122, 250 тыс. радиотелефонных трубок с копированными IMEI, 500 тыс. радиотелефонных трубок с поддельными IMEI, 350 тыс. − с IMEI, полностью установленными на ноль, и 100 тыс. − без кода IMEI (http://www.itu.int/ITU-D/tech/events/2012/CI_ARB_AFR_Tunis_November12/CI_Forum_Tunis_2012_Report.pdf).

В феврале 2010 года NTRA объявило о том, что три оператора подвижной связи в стране блокируют на египетском рынке услуги для всех анонимных пользователей, а также сотовые телефоны без IMEI (http://www.cellular-news.com/story/42911.php).

A.1.5 Индонезия

В январе 2013 года условия импорта сотовых телефонов в Индонезию ужесточились благодаря внедрению технических процедур и требований к стандартам, ограничений на распространение и портовых ограничений, контроля перед отгрузкой и обязательства предварительно регистрировать номера IMEI перед импортом. Эти требования перечислены в Указе № 81/2012 министра промышленности и в Указе № 82/2012 министра торговли (http://trade.ec.europa.eu/doclib/docs/2013/september/tradoc_151703.pdf).

A.1.6 Кения

A.1.6.1 Введение

По сведениям Агентства по борьбе с контрафакцией (ACA) Кении, недобросовестная конкуренция между контрафактными и подлинными продуктами обходится деловому сообществу (местным производителям, инвесторам и новаторам) примерно в 50 млрд. кенийских шиллингов (приблизительно 596 млн. долл. США) в виде ежегодной потери доходов, угрожая таким образом закрытию и/или перемещению многих промышленных предприятий. Потери правительства и экономики от контрафакции оцениваются более чем в 19 млрд. кенийских шиллингов (приблизительно 227 млн. долл. США) ежегодно в виде уклонения от налогов (http://www.aca.go.ke/index.php?option=com_docman&task=doc_download&gid=20&Itemid=471).

К наиболее затрагиваемым контрафакцией товарам относятся медицинские препараты, электронное оборудование, CD и пиратское программное обеспечение, алкогольные напитки, мобильные телефоны и сельскохозяйственные средства производства.

Комиссия по связи Кении была создана в соответствии с главой 411A Закона Кении об информации и связи для лицензирования и регулирования информационно-коммуникационных услуг. В разделе 25 упомянутого Закона Комиссии поручается лицензирование операций и обеспечение систем и услуг электросвязи, соответственно, при соблюдении необходимых условий. Одно из лицензионных требований состоит в одобрении типа оборудования связи, чтобы подтвердить его совместимость с сетями связи общего пользования. Именно в связи с этим в положении 3 Постановления по информации и связи Кении (импорт, одобрение типа и обращение оборудования связи) 2010 года требуется, чтобы Комиссия одобряла типы всех мобильных телефонов перед их подключением к сетям общего пользования (http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf).

Суть процесса одобрения типа состоит в первую очередь в том, чтобы защитить население от нежелательных последствий, к которым приводят некачественные и/или контрафактные устройства мобильных телефонов, включая технические, экономические проблемы и проблемы для здоровья и безопасности. Дополнительная информация по проблемам, связанным с контрафактными радиотелефонными трубками в отрасли ИКТ, приводится ниже в разделе A.1.6.2. Мобильный телефон, не имеющий надлежащего международного идентификатора аппаратуры подвижной связи (IMEI), не может пройти одобрение типа.

По указанным выше причинам использование контрафактных устройств мобильных телефонов непременно должно быть прекращено. Но это происходит с должным учетом интересов всех заинтересованных сторон, так что поэтапная деятельность по их отключению ведется с 30 сентября 2012 года.

Для обеспечения учета интересов и обеспокоенности заинтересованных сторон Комиссия, начиная с октября 2011 года, провела серию открытых консультаций между участниками отрасли ИКТ, различными правительственными учреждениями и другими заинтересованными сторонами по вопросу контрафактных мобильных телефонов в целях рассмотрения тех проблем, которые они привносят в отрасль и экономику в целом. Благодаря этим консультациям были согласованы конкретные действия в связи с обсуждаемым вопросом.

Среди согласованных действий − проведение Комиссией кампании по повышению уровня информированности населения для обеспечения того, чтобы абоненты были осведомлены об отрицательном воздействии контрафактных устройств; создание системы, которая будет использоваться населением для определения того, являются ли их радиотелефонные трубки подлинными; создание системы блокирования контрафактных радиотелефонных трубок в сетях подвижной связи; а также предоставление вспомогательных услуг, касающихся потребителей.

Еще одним важным действием является активизация надзора и принятие строгих мер в связи с контрафактными мобильными устройствами со стороны всех соответствующих правительственных учреждений. Была создана система проверки радиотелефонных трубок с доступом к базе данных GSMA, чтобы дать абонентам возможность проверять свои телефоны с использованием представленного IMEI. Кроме того, внедрена система блокирования контрафактных радиотелефонных трубок в сетях подвижной связи.

В результате изложенной выше деятельности в Кении после 30 сентября 2012 года были выведены из обращения 1,89 млн. контрафактных мобильных телефонов.

A.1.6.2 Выведение из обращения контрафактных мобильных телефонов

1 Базовая информация

a) Внедрение системы регистра идентификации оборудования (EIR)

Сегодня в Кении использование подвижной связи является необходимостью, а не роскошью. Это видно из растущего числа абонентов в стране, которых сейчас насчитывается около 29,2 млн. Но с внедрением услуг подвижной связи возникла проблема кражи мобильных телефонов, а также возросла доля преступлений, совершенных с помощью мобильных телефонов, что создает большой риск для безопасности.

Вследствие этих угроз Комиссия в 2011 году приступила к серии консультаций с существующими лицензированными операторами подвижной связи, с тем чтобы найти долгосрочное решение этой проблемы. Тем временем Восточноафриканская организация связи (EACO) приняла резолюцию, в которой, среди прочего, содержится требование о том, чтобы регуляторные органы и операторы в регионе консультировались по поводу оптимального пути проверки краж мобильных телефонов в регионе.

В ходе этих консультаций было отмечено, что свойственный сетям подвижной связи элемент под названием регистр идентификации оборудования (EIR) обеспечивает механизм для решения вопроса кражи мобильных телефонов. EIR может проверять Международный идентификатор аппаратуры подвижной связи (IMEI) каждого телефона, который поступает в сеть подвижной связи, и сохраняет прежние записи. Такая информация затем будет по мере возможности предоставляться по запросу органов власти.

С этой целью со всеми операторами подвижной связи был заключен меморандум о взаимопонимании (MoB) для внедрения системы EIR, что также проложит путь для внедрения этой системы на региональном уровне. Также отмечалось, что существование контрафактных мобильных телефонов, которые в большинстве случаев имеют дублированные и/или поддельные IMEI, приведет к такой ситуации, когда приобретенная подобным незаконным образом радиотелефонная трубка отслеживается и деактивируется с использованием системы EIR. Некоторые другие радиотелефонные трубки с аналогичными IMEI скорее всего также будут деактивированы.

В таких условиях появляется причина решить вопрос, связанный с наличием контрафактных радиотелефонных трубок на рынке, до полного внедрения системы EIR, поскольку ее успех будет зависеть от искоренения контрафактных радиотелефонных трубок, что активно поддерживается на международном уровне.

b) Внедрение нормативно-правовой базы, касающейся мобильных телефонов

i) Нормативно-правовая база

В том что касается отрасли связи, надлежащая нормативно-правовая база, регулирующая вопросы, связанные с радиотелефонными трубками, предусмотрена в разделе 25 Закона Кении об информации и связи, глава 4II A. Выдаваемые в соответствии с этим Законом лицензии содержат условие с требованием, чтобы лицензиаты предоставляли услуги только тем, кто использует аппаратуру одобренного типа.

Кроме того, в Положении Кении об информации и связи от 2010 года (импорт, одобрение типа и распределение оборудования связи) явным образом требуется, чтобы все радиотелефонные трубки были одобренного типа. Важно отметить, что в соответствии с требованиями Комиссии по одобрению типа радиотелефонная трубка GSM без надлежащего IMEI или с поддельным IMEI не может пройти одобрение типа. Соответственно, все радиотелефонные трубки без надлежащего IMEI или с копированным IMEI по сути являются незаконными и поэтому их использование противоречит указанному выше Закону.

ii) Недавняя директива Комиссии и реакция операторов

В мае 2011 года Комиссия уведомила всех операторов сетей подвижной связи о том, что к 30 сентября 2011 года они должны вывести из обращения контрафактные радиотелефонные трубки в своих сетях. Эта директива соответствует духу и букве нормативных актов, регулирующих сектор связи.

2 Консультации с отраслью

По получении этой директивы участники отрасли подвижной связи обратились с просьбами пересмотреть директиву, отмечая большое количество абонентов, которые пользуются телефонами с одним и тем же или с неправильным IMEI. Кроме того, операторы опасались, что отключение предположительно более 2 млн. используемых контрафактных радиотелефонных трубок отрицательно скажется на их доходах.

В целях внедрения этой директивы с минимальными перебоями в обслуживании Комиссия создала комитет открытого состава, включающий в основном представителей от операторов подвижной связи, соответствующих правительственных министерств и ведомств, производителей оборудования, продавцов и гражданского общества.

Серия консультаций между участниками отрасли ИКТ и различными правительственными ведомствами также направлена на решение вопросов, связанных с контрафактными мобильными телефонами, в отрасли и экономике в целом. Ассоциация GSM (GSMA) отметила, что Кения − это одна из стран с достаточно обширным рынком телефонов, украденных в Европе или однозначно контрафактных. На основе своего опыта решения этого вопроса на международном уровне GSMA также внесла существенный вклад на уровне консультаций для поддержки проходящего в Кении процесса с помощью различных технических мероприятий. К настоящему времени в ходе консультаций было решено принимать конкретные меры для поддержки этой инициативы.

К числу важнейших из таких мер относятся проведение Комиссией кампании по повышению уровня информированности населения для обеспечения того, чтобы абоненты были информированы об отрицательном воздействии контрафактных устройств, а также принятое производителями мобильных телефонов обязательство создать систему, которая будет использоваться населением для определения подлинности своих радиотелефонных трубок. Кроме того, сетевые операторы создали системы, предназначенные для блокирования контрафактных радиотелефонных трубок в своих сетях и для предоставления вспомогательных услуг, относящихся к абонентам, а также для активизации надзора и принятия жестких мер со стороны правительственных ведомств в случае контрафактных радиотелефонных трубок.

Создание системы проверки радиотелефонных трубок с доступом в базу данных GSMA, которая позволяет абонентам проверять законность своих телефонов с помощью представленного IMEI, проходило вместе с проведением кампании по повышению уровня осведомленности потребителей (http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf).

A.1.7 Руанда

Агентство по регулированию коммунального сектора (RURA) Руанды объявило в 2013 году о плане запрета импорта в страну контрафактных мобильных устройств, при этом не блокируя те телефоны, которые уже используются (http://www.newtimes.co.rw/news/views/article_print.php?i=15290&a=64650&icon=Print). Кроме того, Руанда сталкивается с проблемой контрафактных телефонов, которые перенаправляют вызовы, сделанные по согласованным коротким кодам EACO 100 (служба по работе с клиентами), 101 (пополнение счета в Танзании) и 102 (проверка баланса в Танзании), на номер 112 (неотложная помощь, полиция). Это заставило RURA присвоить на временной основе другой короткий код для службы информирования потребителей (http://www.eaco.int/docs/19_congress_report.pdf).

A.1.8 Шри-Ланка

В марте 2013 года Комиссия по регулированию электросвязи Шри-Ланки (TRCSL) предложила выразить заинтересованность в плане "Проектирования, разработки и введения центрального регистра идентификации оборудования (CEIR) для сетей подвижной связи в Шри-Ланке" (http://www.trc.gov.lk/images/pdf/eoi_ceir_07032013.pdf).

В целях ограничения рынка контрафактных мобильных телефонов, противодействия кражам мобильных телефонов и защиты интересов потребителей TRCSL намерена ввести центральный регистр идентификации оборудования (CEIR), соединенный с EIR всех операторов подвижной связи. CEIR действует в качестве центральной системы для всех сетевых операторов, которые обмениваются информацией о включенных в "черный" список мобильных терминалах, для того чтобы устройства, внесенные в "черный" список в какой-либо одной сети, не работали в других сетях, даже если в устройстве карта модуля идентификации абонента (SIM) заменена.

В соответствии с требованиями TRCSL CEIR должен обеспечивать следующие функции:

i) CEIR должен иметь возможности вести базу данных IMEI всех устройств, зарегистрированных в сетях подвижной связи;

ii) CEIR должен быть способен идентифицировать следующие IMEI:

   a) IMEI, которые не распределены;

   b) IMEI, которые являются недействительными, скопированными или полностью установленными на ноль;

iii) база данных CEIR должна содержать следующую информацию об устройствах, зарегистрированных во всех сетях подвижной связи в Шри-Ланке:

a) IMEI;

b) статус IMEI ("белый", "серый", "черный");

c) дата создания записи;

d) дата последнего обновления записи;

e) номер модели устройства;

f) причина статуса IMEI (недействительный, украденный, скопированный, действительный);

iv) CEIR должен быть способен блокировать предоставление услуг абонентам, у которых имеются зарегистрированные устройства с недействительными или внесенными в "черный" список IMEI;

v) CEIR должен быть способен идентифицировать модель, версию и другую информацию об устройстве;

vi) CEIR должен давать возможность вносить новую запись в базу данных, содержащую IMEI, вне зависимости от того, когда будет активирован счет абонента;

vii) CEIR должен предоставлять операторам обновленную информацию по местным базам данных по "черному"/"белому"/"серому" спискам, с тем чтобы не допускать копирования между сетями и обновлять содержащуюся в базах данных информацию;

viii) CEIR должен периодически обновлять базу данных IMEI новейшей информацией о действительных присвоениях IMEI с использованием наиболее эффективных имеющихся методов;

ix) CEIR должен иметь возможности идентифицировать контрафактные IMEI путем сравнения IMEI, предоставленных GSMA.

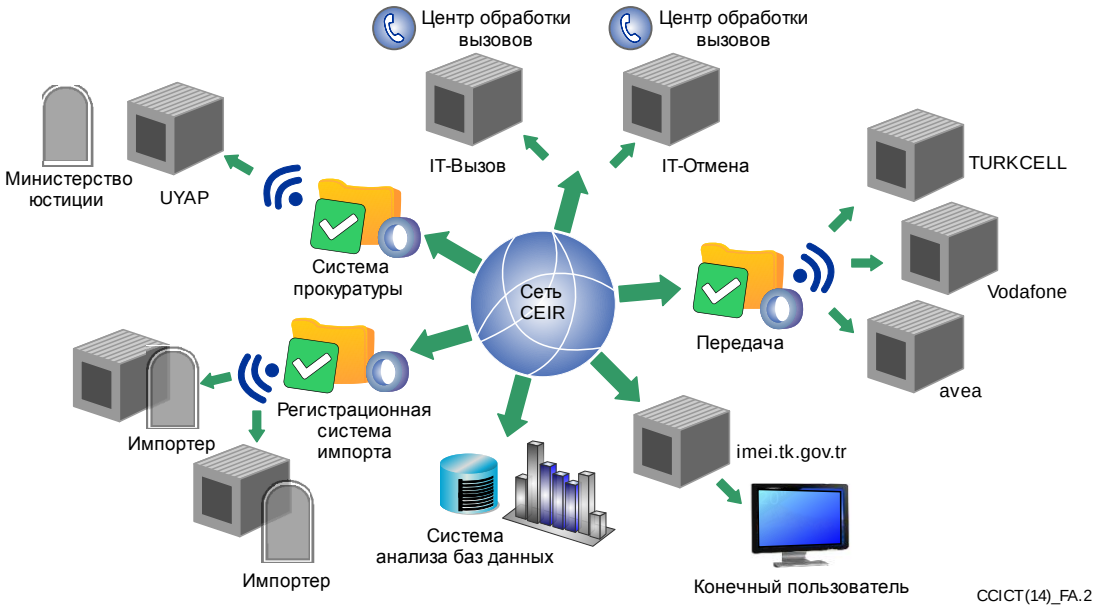
x) CEIR должен быть функционально совместимым со всеми соответствующими сетевыми элементами и интерфейсами операторов подвижной связи;

xi) база данных CEIR должна обеспечивать гибкий метод участия (с помощью ввода данных вручную, неструктурированных файлов, содержащих обновленные данные о сериях IMEI);

xii) CEIR должен осуществлять проверку формата IMEI на предмет действительности формата и серии.

A.1.9 Турция

В 2006 году Управление информационно-коммуникационных технологий (ICTA) Турции создало центральный регистр идентификации оборудования (CEIR) в целях предотвращения использования незарегистрированных мобильных телефонов, потери налогов, недобросовестной конкуренции в секторе, хищений, а также в целях автоматизации связанных с импортом процессов. Была создана инфраструктура для сокращения количества незаконно ввезенных устройств и отключения от сети беспроводной связи контрабандных, потерянных и украденных устройств или устройств с копированными номерами IMEI.



https://www.icta.mu/mediaoffice/publi.htm

Рисунок A.2 – Структура центрального регистра идентификации оборудования

В соответствии с Законом о радиосвязи номера IMEI относят к разным категориям следующим образом:

- "Белый" список: включает номера IMEI устройств, которые зарегистрированы и электронная информация об идентичности которых не изменялась.
- "Черный" список: включает номера IMEI, которые принадлежат к категории потерянных или украденных устройств, электронная информация об идентичности которых была изменена. Операторам электросвязи предоставлен мандат на отключение беспроводной связи для таких устройств.
- "Серый" список: включает номера IMEI, которые не содержатся ни в "белом", ни в "черном" списках и для которых беспроводная связь разрешена. От операторов электросвязи требуется анализировать детали вызовов с таких устройств и уведомлять ICTA. От операторов электросвязи также требуется уведомлять пользователей таких устройств с помощью текстовых сообщений о том, что их устройства не включены в "белый" список.
- Согласованный "белый" список: включает номера IMEI, которые копируют номер абонента подвижной связи в цифровой сети с интеграцией служб (MSISDN) устройств пользователей, которые внесли регистрационный сбор. Кроме того, он включает устройства, внесенные в абонентский договор с оператором электросвязи, которые находились в Турции в течение кратковременного периода с номером MSISDN.

Согласно ежегодному отчету ICTA за 2010 год, на конец 2010 года насчитывалось 131 836 847 номеров IMEI, зарегистрированных законным образом, и 14 308 239 номеров IMEI, включенных в "черный" список в связи с тем, что они являлись потерянными, контрабандными, украденными и скопированными (https://www.icta.mu/mediaoffice/publi.htm).

A.1.10 Уганда

Комиссия по связи Уганды (UCC) приступила к выполнению проекта (http://ucc.co.ug/data/mreports/18/0/ELIMINATION%20OF%20COUNTERFEIT%20MOBILE%20PHONES.html), направленного на постепенное удаление контрафактных мобильных телефонов с рынка Уганды. Исследование, одобренное UCC, свидетельствует о том, что около 30% мобильных телефонов на угандийском рынке являются поддельными. Кроме того, обследование показывает, что потери государства составляют около 15 млрд. шиллингов (примерно 5400 млн. долл. США по состоянию на ноябрь 2014 года) по линии налоговых поступлений, которые уходят дилерам, продающим поддельные или контрафактные мобильные телефоны (http://www.monitor.co.ug/Business/Commodities/Survey+finds+30++of+Ugandan+phones+fake/-/688610/1527408/-/elvou8z/-/index.html).

В декабре 2012 года UCC опубликовала консультативный документ "Сроки выведения из обращения контрафактных мобильных телефонов и распределение соответствующих задач" (http://www.ucc.co.ug/files/downloads/Counterfeit%20phones%20Consultative%20Document.pdf), в котором определяются сам проект и следующие четыре этапа его выполнения:

ЭТАП 1: Проверка мобильных телефонов

Во время этого этапа потребители смогут проверить статус своих телефонов с использованием одного или обоих приложений − интернета и SMS.

Потребителям рекомендуется незамедлительно проверить законность своих мобильных телефонов с использованием указанных выше двух методов.

ЭТАП 2: Отказ в обслуживании новых контрафактных телефонов

Во время этого этапа новым контрафактным мобильным телефонам, которые ранее не были зарегистрированы в какой-либо сети, должно быть отказано в обслуживании во всех сетях. Предложенная дата выполнения этого этапа была установлена на 31 января 2013 года.

ЭТАП 3: Отключение всех контрафактных мобильных телефонов

Во время этого этапа все контрафактные мобильные телефоны, в том числе уже зарегистрированные в какой-либо сети, должны быть отключены. Предложенная дата выполнения этого этапа была установлена на 1 июля 2013 года.

ЭТАП 4: Консолидация проекта

Во время этого этапа Комиссия должна изучить результаты проекта, касающиеся его выполнения, и вопросы, которые необходимо решать в связи с утилизацией электронных отходов и копированием IMEI. Предложения по решению различных вопросов на этом этапе все еще рассматриваются.

A.1.11 Украина

A.1.11.1 Введение

В 2008 году самая неотложная и насущная проблема, которую необходимо было решать, состояла в импорте контрабандных мобильных терминалов, на которые приходилось 93−95% рынка. Значительная часть этих радиотелефонных трубок неизвестного происхождения не соответствовали украинским стандартам ни по их техническим характеристикам, ни по их безопасности. Согласно Закону Украины "О радиочастотном ресурсе Украины" на Национальную комиссию, осуществляющую государственное регулирование в сфере связи и информатизации (НКРСИ), были возложены полномочия по внедрению дополнительных мер для защиты украинского рынка от низкокачественных, неразрешенных или незаконно ввезенных мобильных терминалов.

НКРСИ определила нормативную процедуру для импорта мобильных терминалов. В качестве технической реализации процедуры импорта в 2009 году была создана и введена в действие Украинским государственным центром радиочастот (УГЦР) автоматизированная информационная система учета мобильных терминалов на территории Украины (АИСУМТУ). Вследствие этого незаконный ввоз мобильных терминалов значительно сократился, составив в 2010 году не более 5−7% рынка, и в последующие годы продолжал сокращаться.

IMEI используются на Украине для создания базы данных устройств, которые были незаконно ввезены на территорию Украины. Ведутся следующие списки: "белый" список устройств, которые были импортированы законным образом, "серый" список устройств неподтвержденного статуса и "черный" список устройств, которым будет отказано в обслуживании. Доступ к этой базе данных предоставляется регуляторным и таможенным органам, сетевым операторам и населению в целом с правами доступа соответствующего уровня.

АИСУМТУ выполняет следующие функции:

- автоматизация обработки заявок импортеров на выполнение нормативных процедур регистрации и использование оконечного оборудования в сетях электросвязи;
- предотвращение нелегального "серого" ввоза мобильных терминалов на территорию Украины;
- борьба с кражей радиотелефонных трубок;

- автоматизация рабочих процессов УГЦР и повышение эффективности работы УГЦР с участниками рынка терминалов;
- определение "скопированных" кодов IMEI и блокирование терминалов с такими кодами.

Более подробная информация о АИСУМТУ приводится в разделе A.1.11.2.

Украинским законодательством запрещена продажа мобильных терминалов с кодами IMEI, не зарегистрированными в АИСУМТУ. Основная часть АИСУМТУ − это общая база данных, в которой содержатся "белый", "серый" и "черный" списки кодов IMEI мобильных терминалов. При первом подключении и регистрации терминала у любого оператора сети код IMEI этого терминала автоматически направляется оператором подвижной связи в общую базу данных. АИСУМТУ показывает коды IMEI, которые не содержатся в "белом" списке, определяет контрафактные мобильные телефоны и регистрирует соответствующие коды IMEI в "сером" списке. Все владельцы соответствующих терминалов получают сообщение SMS и должны в течение 90 дней с даты включения в "серый" список подтвердить законное происхождение терминала.

Коды IMEI украденных терминалов регистрируются в "черном" списке по запросу правоохранительного органа, что делает кражу терминалов бесполезной. Такая же процедура применяется к блокированию терминалов по просьбе владельцев потерянных телефонов. Терминалы, включенные в "черный" список, сетевыми операторами не обслуживаются.

Задача защиты потребителей достигается благодаря внедрению инструмента удобной проверки законного происхождения мобильного терминала до его приобретения. Любой потребитель может проверить статус кода IMEI терминала, направив SMS с этим кодом на общенациональный номер "307" или используя интернет-портал УГЦР. Время, необходимое для проверки, не превышает 10 секунд.

Внедрение АИСУМТУ обеспечивает на Украине легальный рынок терминалов и привело к резкому сокращению "серого" (нелегального) ввоза мобильных терминалов на Украину. Доля незаконно ввезенных мобильных терминалов сократилась с 93−95% в 2008 году до 5−7% в 2010 году и в последующие годы. За период 2010−2012 годов в государственный бюджет Украины поступили доходы в размере более 500 млн. долл. США в виде таможенных импортных пошлин на мобильные терминалы по сравнению с 30 млн. долл. США за предыдущие три года. Украинский рынок мобильных терминалов состоит в основном из мобильных терминалов, соответствующих требованиям по техническим характеристикам для использования на Украине.

A.1.11.2 Автоматизированная информационная система учета мобильных терминалов на территории Украины (АИСУМТУ)

A.1.11.2.1 Базовая информация

Стремительное развитие услуг подвижной (сотовой) связи, предоставляемых операторами, и значительное преобладание услуг электросвязи этого вида на Украине привели к быстрому росту украинского рынка мобильных терминалов и, как следствие, к росту импорта этих продуктов.

"Мобильный терминал" означает мобильный телефон или другое оборудование, используемое конечным пользователем в сети электросвязи, которое имеет международный идентификатор (код IMEI) и может идентифицироваться в сети с использованием этого кода.

В 2008 году на украинском рынке мобильных терминалов существовала критическая ситуация: 93−95% продуктов на этом рынке относились к "серому импорту", или просто говоря, были контрабандными товарами. Кроме того, значительная часть этих продуктов были копиями фирменных радиотелефонных трубок неизвестного происхождения, которые не соответствовали украинским стандартам ни по своим техническим характеристикам, ни по характеристикам безопасности. Различные меры рыночного регулирования не могли изменить эту ситуация, а терминалы на Украине не производились.

Тогда согласно Закону Украины "О радиочастотном ресурсе Украины" на независимый регуляторный орган − Национальную комиссию, осуществляющую государственное регулирование в сфере связи и информатизации (НКРСИ) − были возложены полномочия по внедрению дополнительных мер для защиты украинского рынка от низкокачественных, неразрешенных или незаконно ввезенных мобильных терминалов.

A.1.11.2.2 Задачи

Для контроля за импортом, реализацией и использованием терминалов НКРСИ установила следующие задачи:

1 Защита украинского рынка от низкокачественных мобильных терминалов, которые могут быть неразрешенными или опасными для здоровья человека.

2 Обеспечение надлежащего качества услуг подвижной связи.

3 Решение социальной проблемы, связанной с кражей радиотелефонных трубок, особенно у детей.

4 Борьба с незаконным ввозом и реализацией мобильных терминалов на украинском рынке.

С учетом вышеизложенных задач были разработаны процедуры импорта и реализации оборудования подвижной связи. Эти процедуры были включены в официальные акты – Порядок ввоза из-за границы радиоэлектронных средств и излучающих устройств и Порядок реализации в Украине радиоэлектронных средств и излучающих устройств.

A.1.11.2.3 Процедуры импорта

Импорт радиооборудования на Украину контролируется таможенными органами при соблюдении следующих условий:

- наличие документа о соответствии радиооборудования техническим нормам;
- соответствие Реестру радиоэлектронных средств и излучающих устройств, которые могут применяться на территории Украины в полосах радиочастот общего пользования;
- отсутствие в Реестре радиоэлектронных средств и излучающих устройств, которые не могут применяться на территории Украины в полосах радиочастот общего пользования.

Коды IMEI, представленные импортером в УГЦР, обрабатываются и включаются в "белый" список общей базы данных IMEI. Для регистрации международных идентификаторов оконечного оборудования, ввезенного на территорию Украины на законных основаниях, Государственная таможенная служба Украины на ежедневной основе предоставляет УГЦР выписки из таможенных деклараций (в электронной форме) на импорт радиоэлектронного оборудования.

В качестве технической реализации изложенной выше процедуры импорта 1 июля 2009 года была создана и введена в действие УГЦР автоматизированная информационная система учета мобильных терминалов на территории Украины (АИСУМТУ).

В соответствии с Законом Украины "О подтверждении соответствия" соответствие оконечного оборудования должно сертифицироваться органами, утвержденными регуляторным органом (НКРСИ).

A.1.11.2.4 Функции АИСУМТУ

Функции АИСУМТУ изложены в разделе A.1.11.1:

- автоматизация обработки заявок импортеров;
- предотвращение нелегального "серого" ввоза мобильных терминалов на территорию Украины;
- борьба с кражей радиотелефонных трубок;
- автоматизация рабочих процессов УГЦР и повышение эффективности работы УГЦР с участниками рынка терминалов;
- определение "скопированных" кодов IMEI и блокирование терминалов с такими кодами.

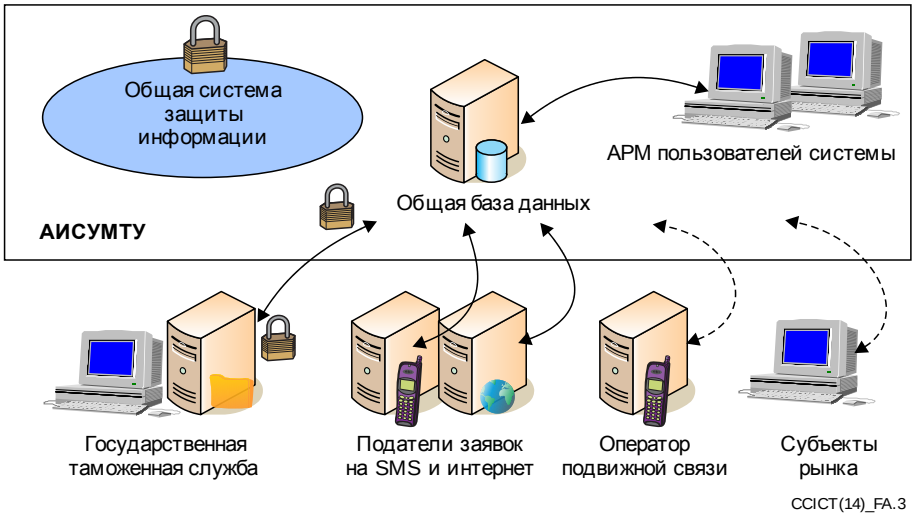


Рисунок А.3 – Функции АИСУМТУ

А.1.11.2.5 Предоставление полномочий

Согласно действующему законодательству полномочия пользоваться АИСУМТУ предоставлены следующим сторонам:

- Украинский государственный центр радиочастот;
- Национальная комиссия, осуществляющая государственное регулирование в сфере связи и информатизации;
- операторы подвижной связи;
- Государственная налоговая служба;
- Министерство иностранных дел;
- покупатели и пользователи мобильных терминалов; и
- импортеры.

А.1.11.2.6 Общая база данных IMEI

Основная часть АИСУМТУ − общая база данных IMEI, в которой ведется три списка, которые традиционно называют:

- "Белый" список: регистр кодов IMEI терминалов, ввезенных на законных основаниях или произведенных на Украине.
- "Серый" список: регистр общей базы данных с кодами IMEI терминалов, не включенных в "белый" или "черный" список на момент первой регистрации в сети электросвязи.
- "Черный" список: регистр кодов IMEI терминалов, запрещенных для обслуживания в сетях операторов (украденные или потерянные радиотелефонные трубки, терминалы с неподтвержденным законным происхождением по истечении 90 дней с даты включения в "серый" список).

Ведение подсистемы общей базы данных IMEI обеспечивает для уполномоченных пользователей УГЦР инструмент ввода данных в "белый" список. "Серый" и "черный" списки создаются автоматически. Уполномоченные пользователи УГЦР имеют ограниченное право изменять статус конкретных кодов IMEI в "сером" и "черном" списках.

Каждое действие уполномоченного пользователя УГЦР подтверждается индивидуальной электронной цифровой подписью пользователя.

Подсистема включает функцию импорта для передачи данных от импортеров терминалов и операторов подвижной связи в регистр IMEI.

Обрабатывая данные из "белого" списка и данные от операторов, импортеров и Таможенной службы, можно создать и вести регистры "серого" и "черного" списков.

На первом этапе ввода этой системы в действие были решены две задачи:

1 Защита украинского рынка от неразрешенных мобильных терминалов низкого качества, которые могут оказаться опасными для здоровья пользователей.

2 Предотвращение незаконного ввоза мобильных терминалов и их реализации на украинском рынке.

В дальнейшем была разработана система, обеспечивающая решение всех задач, в том числе демотивацию краж мобильных терминалов, особенно у детей.

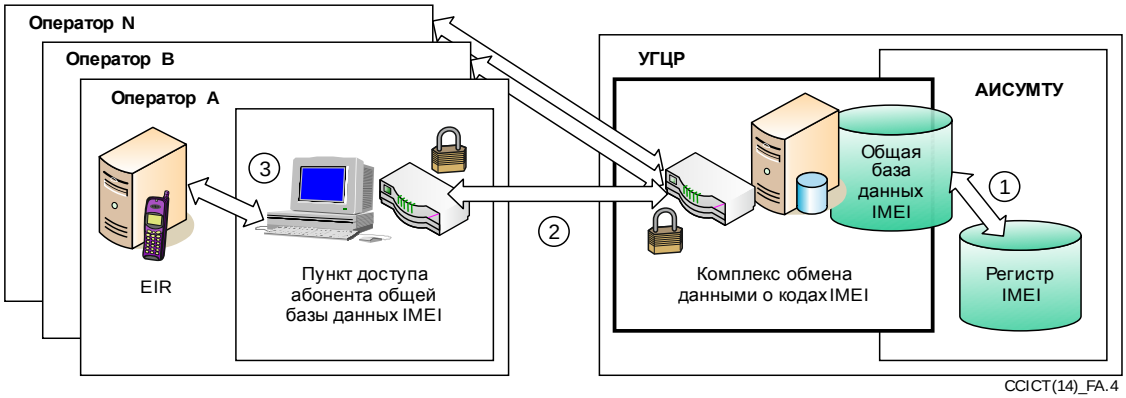


Рисунок А.4 – Общая база данных EIR и IMEI

На втором этапе была внедрена подсистема обмена кодами IMEI из "белого", "серого" и "черного" списков между АИСУМТУ и национальными операторами подвижной связи. На этом этапе обмен кодами IMEI производился "вручную".

Кроме того, были внедрены подсистемы обмена данными для информирования Министерства иностранных дел об украденных/потерянных терминалах и обмена данными с Таможенной службой для сообщения информации об импортированных терминалах.

В целях активного взаимодействия с АИСУМТУ операторы и УГЦР обеспечили:

- ведение регистра идентификации оборудования (EIR);
- пункт доступа абонента общей базы данных IMEI (абонентский пункт);
- канал для взаимодействия между абонентским пунктом и EIR;
- применение сертификатов электронных цифровых подписей для уполномоченных пользователей.

Включенная в АИСУМТУ система синхронизирует работу EIR операторов сотовой (подвижной) связи и общую базу данных IMEI. Это дает возможность автоматизированного обмена списками кодов IMEI между EIR сетей операторов подвижной связи и общей базой данных IMEI. При этом код IMEI каждого терминала после регистрации в сети оператора появляется в АИСУМТУ и проверяется по общей базе данных IMEI.

На настоящее время сервер синхронизации поддерживает как ручной, так и автоматический режимы для соединения EIR операторов.

А.1.11.2.7 Характеристики

К характеристикам системы относятся:

- использование отраслевых стандартов для хранения и передачи данных (обмена данными);
- обеспеченная безопасность данных и всей системы в целом;
- использование национального стандарта цифровой подписи для обеспечения целостности и невозможности отказа от обязательств на всех этапах обработки данных в системе;
- модульная структура системы;
- круглосуточный и ежедневный режим работы.

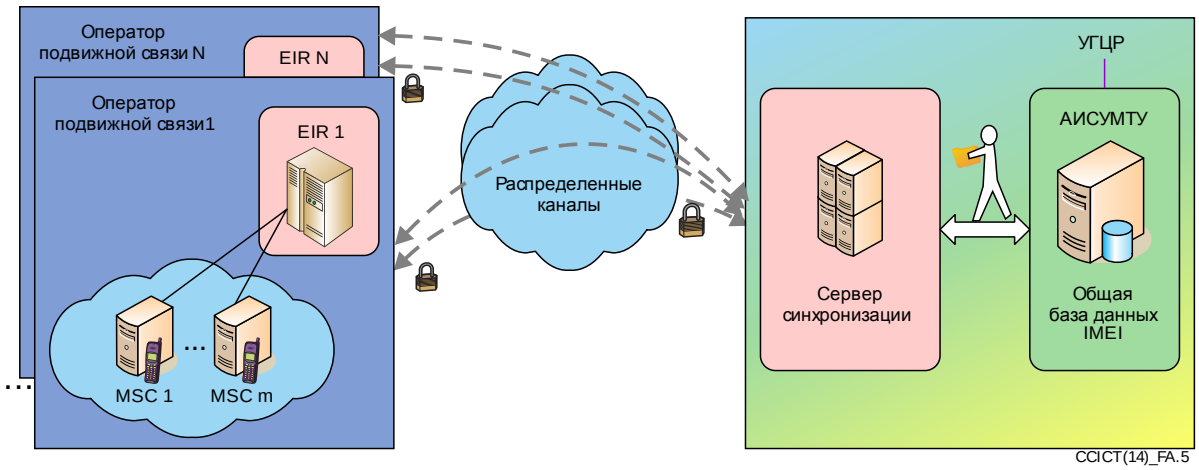


Рисунок А.5 – Сервер синхронизации

А.1.11.2.8 Безопасность данных

Система всесторонней защиты информации (CIPS) АИСУМТУ соответствует требованиям действующего законодательства, что подтверждается положительными заключениями, выданными на основе результатов обследования, проведенного компетентным правительственным органом.

CIPS обеспечивает:

- контроль за ограниченным доступом к конфиденциальной информации;
- определение угроз безопасности для информации ограниченного доступа, которая передается, обрабатывается и хранится в системе;
- защиту конфиденциальности, целостности и пригодности информации ограниченного доступа от несанкционированного доступа;
- предотвращение утечки информации при переходе в незащищенную среду;
- защиту технологический информации от несанкционированного доступа, разрушения, порчи или блокирования.

Безопасность и надежность гарантируются с помощью:

- использования надежных средств электронной цифровой подписи для обеспечения аутентичности и целостности информации, авторизации и аутентификации уполномоченных пользователей;
- внедрения электронной цифровой подписи в соответствии с национальными стандартами Украины;
- наличия системы резервного копирования и восстановления;
- обеспечения защищенного входа в систему (запись в системе любого действия пользователя или любого события).

А.1.11.2.9 Результаты внедрения

1 Защита потребителей

Каждый покупатель может проверить законность мобильного терминала до его приобретения на Украине. Это можно сделать с помощью использования официального веб-сайта УГЦР или направив SMS с кодом IMEI проверяемого терминала на номер "307", общий для всех операторов подвижной связи. Через несколько секунд в ответе будет указан статус запрашиваемого кода IMEI в общей базе данных IMEI.

Это обеспечивает защиту украинского рынка от терминалов, которые не соответствуют установленным на Украине требованиям к использованию.

Действующим украинским законодательством запрещается реализация мобильных терминалов с кодами IMEI, не зарегистрированными в общей базе данных IMEI.

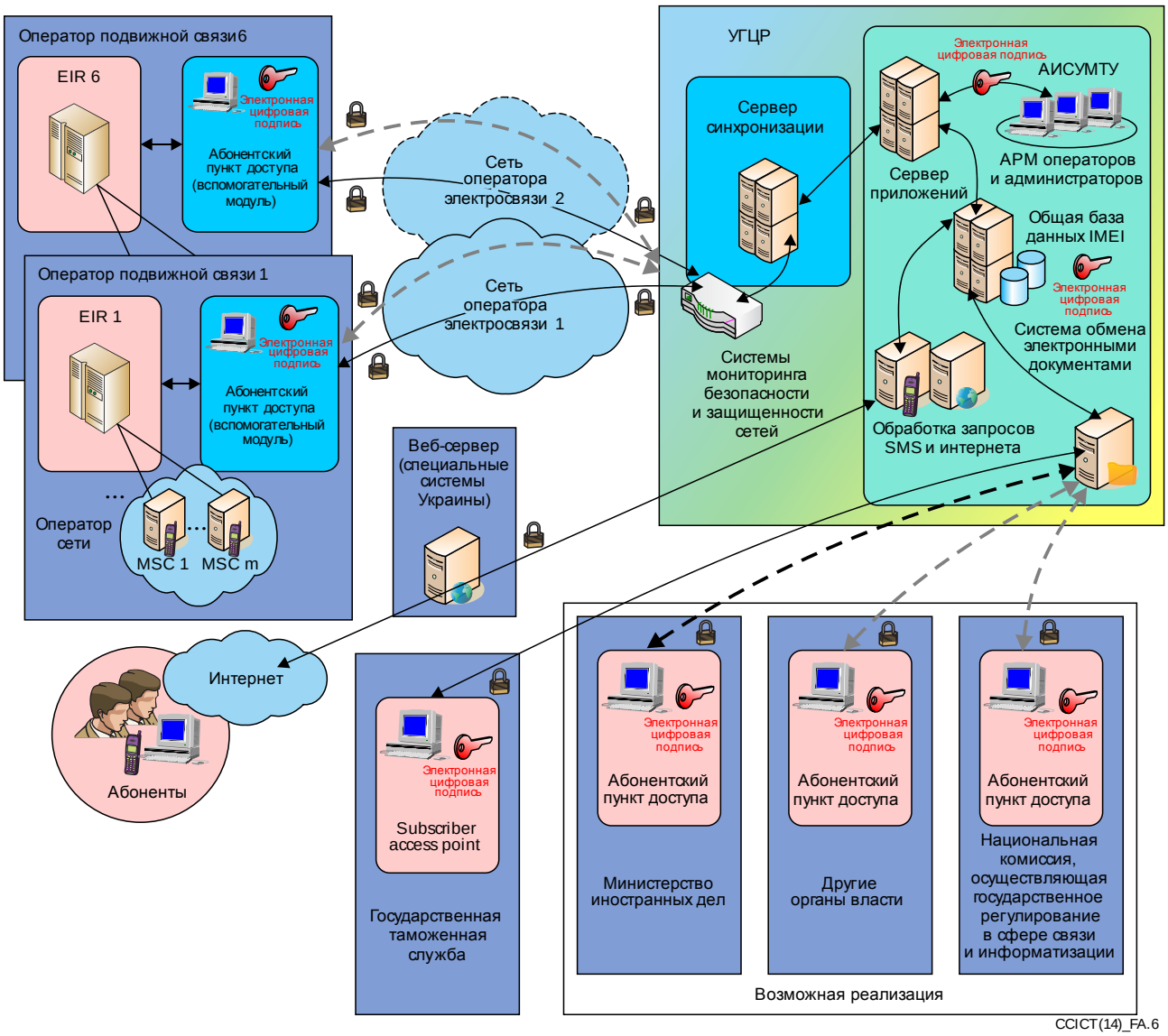


Рисунок А.6 – Действующая в АИСУМТУ система всесторонней защиты информации (CIPS)

2 Борьба с кражей терминалов

Коды IMEI украденных терминалов регистрируются в "черном" списке по запросу правоохранительного органа, что делает кражу терминалов бесполезной.

Такая же процедура применяется к блокированию терминалов по просьбе владельцев потерянных телефонов.

3 Пресечение незаконного импорта

При первом подключении к сети любого оператора любой терминал незамедлительно регистрируется в соответствующей сети. Коды IMEI терминалов, обслуживаемых сетью оператора (за исключением находящихся в международном роуминге), автоматически направляются своевременно (в ночное время) операторами подвижной связи в общую базу данных IMEI АИСУМТУ.

АИСУМТУ выявляет коды IMEI, которых нет в "белом" списке общей базы данных IMEI. Такие коды IMEI регистрируются в "сером" списке. Все владельцы соответствующих терминалов получают по SMS предупреждение о возможном блокировании терминалов в течение 90 дней.

По истечении 90-дневного периода код IMEI передается из "серого" списка в "черный" список. Терминалы из "черного" списка операторами не обслуживаются (отказ в регистрации в сети, за исключением неотложных вызовов на номер "112"). Подключение к сети любого другого оператора не приводит к изменению статуса "серого" или "черного" терминала.

По получении SMS-предупреждения о включении в "серый" список и об ограниченном 90-дневном периоде обслуживания владелец может обратиться в УГЦР, чтобы представить подтверждение законного импорта данного терминала. Сотрудники УГЦР рассматривают обращение владельца и, в случае подтверждения законного характера импорта, переводят код IMEI из "серого" в "белый" список. После этой процедуры операторы подвижной связи начинают обслуживать терминал без каких-либо ограничений по срокам.

Тем не менее, на настоящее время терминалы, включенные в "черный" список, не отключаются в связи с отсутствием необходимого правового документа.

В УГЦР действует центр обработки вызовов, который занимается вызовами, относящимися к запросам пользователей мобильных терминалов о статусе кодов IMEI и к импорту терминалов.

4 Законодательство, касающееся рынка терминалов на Украине

- "Серый" (незаконный) ввоз мобильных терминалов на Украину резко сократился. Доля законно ввезенных мобильных терминалов возросла в 2010 году до 93−95% (по сравнению с 7,5% в 2008 г.).
- За период 2010−2012 годов в государственный бюджет Украины поступили доходы в размере более 500 млн. долл. США в виде таможенных импортных пошлин на мобильные терминалы по сравнению с 30 млн. долл. США за предыдущие три года.
- Украинский рынок мобильных терминалов состоит в основном из мобильных терминалов, соответствующих требованиям по техническим характеристикам для использования на Украине.
- На 30 апреля 2013 года в общей базе данных IMEI АИСУМТУ было зарегистрировано 140 865 260 кодов IMEI мобильных терминалов.
- Система АИСУМТУ стала рентабельной всего за семь месяцев за счет средств, полученных УГЦР от платежей импортеров.

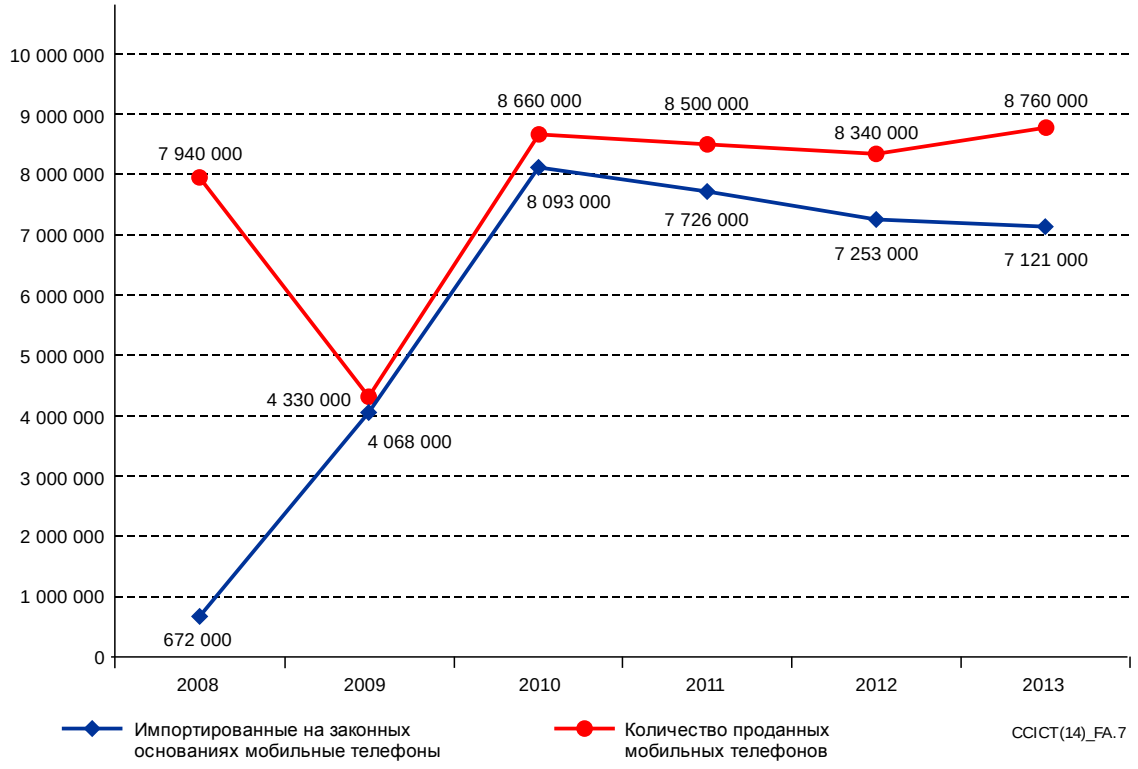


Рисунок A.7 – Последствия внедрения AISMTRU на Украине

A.1.12 Объединенные Арабские Эмираты (ОАЭ)

Законами об электросвязи ОАЭ запрещается использование, продажа, приобретение, распространение и продвижение на рынке поддельных мобильных устройств. Регуляторный орган

электросвязи (TRA) принимает все необходимые меры для полного прекращения продажи и использования таких устройств в ОАЭ. Тем, кто участвует в продаже поддельных мобильных телефонов, направляются уведомления и выписываются штрафы, а в некоторых случаях лицензии могут быть отозваны вследствие несоблюдения нормативных положений.

В 2011 году TRA начал новую кампанию (http://www.tra.gov.ae/download.php?filename=public-announcements/IMEI_announcement_en.pdf, http://www.tra.gov.ae/news_TRA_Launches_Fake_Mobile_Awareness_Campaign-354-1.php) по повышению уровня информированности и предотвращению использования поддельных мобильных телефонов в ОАЭ, а также объявил о том, что с 1 января 2012 года в сети подвижной электросвязи ОАЭ будет прекращена работа всех мобильных телефонов с фальшивыми номерами IMEI. TRA размещал в ежедневных газетах оповещения о введении запрета на контрафактные телефоны.

Хотя такие меры были направлены на то, чтобы вывести из употребления фальшивые мобильные телефоны, контракты на услуги не затрагивались и продолжали действовать обычным образом при использовании подлинных мобильных телефонов. Направляя SMS с номером IMEI мобильного устройства по номеру телефона "8877", пользователи могут получить ответ от поставщика услуг с информацией о статусе мобильного устройства. С пользователями поддельных устройств незамедлительно связываются их поставщики услуг, и телефоны без одобрения типа должны быть отключены от всех услуг электросвязи, включая вызовы, передачу текста и интернет.

TRA объявил о том, что фальшивые мобильные устройства представляют потенциальный вред для здоровья пользователей, и призвал всех пользователей принимать необходимые меры предосторожности при приобретении мобильных устройств и оборудования. По данным TRA, поддельные телефоны в особенной степени подвержены тому, что элементы питания подтекают и взрываются и при этом высвобождаются очень агрессивные и токсичные химические вещества. Кроме того, при низкокачественной сборке не проверяются уровни излучения, элементы питания быстрее разряжаются, а сигнал, как правило, принимается гораздо слабее.

Главная цель TRA состоит в том, чтобы ликвидировать в ОАЭ поддельные мобильные устройства и просветить население в целом и розничных продавцов о рисках, связанных с их использованием. TRA признал, что вопросы контрафакции и пиратства оказывают огромное воздействие на экономику и права интеллектуальной собственности, но поддельные мобильные телефоны, кроме того, являются устройствами низкого качества, которые производятся без необходимых тестов и проверок.

A.2 Примеры совместных мер, принятых на региональных уровнях

A.2.1 Межамериканская комиссия по электросвязи (СИТЕЛ)

СИТЕЛ была создана в 1994 году Генеральной ассамблеей Организации американских государств (ОАГ) в целях содействия развитию электросвязи/ИКТ в Северной и Южной Америке. Ее членами являются все 35 государств этого региона, а также более 100 ассоциированных членов из отрасли ИКТ.

Постоянный консультативный комитет I (Электросвязь) СИТЕЛ рекомендовал в 2009 году государствам-членам "рассмотреть вопрос о создании баз данных в рамках общей программы борьбы с контрафакцией и пиратством" (заключительный отчет 15-го собрания ПКК.I 2 СИТЕЛ, октябрь 2009 г.), а в декабре 2011 года ПКК.II (Радиосвязь, включая радиовещание) СИТЕЛ приступил к изучению мер, принимаемых администрациями электросвязи в отношении использования контрафактных мобильных телефонов.

ПКК.II решил обратиться к администрациям с просьбой представить информацию "о принятых или планируемых действиях и регламентарно-административных мерах в отношении поддельных, контрафактных и некачественных сотовых телефонов, а также их отрицательном воздействии на пользователей и операторов, в том числе в отношении помех, уровней неионизирующего излучения и использования опасных или запрещенных химических компонентов" (заключительный отчет 18-го собрания ПКК.II СИТЕЛ, 22 декабря 2011 г., решение 121).

Кроме того, СИТЕЛ рассмотрела проблему кражи мобильных телефонов, и оба постоянных консультативных комитета приняли ряд резолюций по этому вопросу.

ПКК.II в сентябре 2011 года принял резолюцию 73 "Создание регионального партнерства для борьбы с кражей мобильного оконечного оборудования". В этой резолюции ПКК.I поручается рассмотреть

вопрос о "содействии со стороны СИТЕЛ в разработке государствами-членами совместных мер по ограничению в любой стране региона активации такого украденного мобильного оконечного оборудования, а также в принятии конкретных рекомендаций для операторов, с тем чтобы они пользовались ресурсами, предоставляемыми технологиями, и не позволяли подключать к своим сетям оборудование, происхождение которого полностью не установлено, путем создания регионального партнерства по борьбе с кражей такого оборудования (заключительный отчет 17-го собрания ПКК.II, 6 сентября 2011 г., резолюция 73).

ПКК.I отреагировал практически незамедлительно, приняв резолюцию "Региональные меры по борьбе с кражей мобильных оконечных устройств" (заключительный отчет 19-го собрания ПКК.I СИТЕЛ, 20 сентября 2011 г., резолюция 189). В этой резолюции отмечается международный характер данной проблемы, поскольку мобильные устройства направляются в другие страны, когда какая-либо отдельная страна принимает меры против краж устройств, и поэтому необходимо принимать меры на региональном уровне. Помимо мер, касающихся потерянных/украденных радиотелефонных трубок, в резолюции 189 также предлагается государствам-членам "рассмотреть вопрос о включении в свою нормативно-правовую базу запрета на активацию и использование IMEI или электронных серийных номеров производителей устройств, о которых в региональных или международных базах данных сообщалось как об украденных, потерянных или *имеющих незаконное происхождение"* (выделено редактором).

Приложение к резолюции 189 включает ряд дополнительных мер, таких как "изучение технической возможности внедрения контроля за местной торговлей мобильными оконечными устройствами и их подключением к сетям" и "содействие созданию регуляторных налоговых и/или таможенных механизмов, обеспечивающих, чтобы импортируемые мобильные оконечные устройства и/или их части имели законное происхождение и были сертифицированы в соответствии с нормативно-правовой базой каждого государства-члена, а также обеспечивающих таможенный контроль, препятствующий вывозу или реэкспорту украденных мобильных оконечных устройств и/или их частей".

ПКК.I принял в 2012 году рекомендацию "Региональные меры, направленные на обмен информацией по мобильным оконечным устройствам, о которых сообщалось как об украденных, потерянных или восстановленных" (заключительный отчет 20-го собрания ПКК.I СИТЕЛ, 10 июня 2012 г., рекомендация 16), которая включала также терминалы "незаконного происхождения". Государствам-членам предлагается "на национальном, региональном и международном уровнях осуществить действия и принять меры, направленные на то, чтобы поставщики услуг подвижной электросвязи обменивались информацией об украденных, потерянных или незаконных мобильных оконечных устройствах с использованием различных существующих и функционирующих платформ, предназначенных для различных технологий доступа, в целях борьбы с неорганизованными рынками, содействия сотрудничеству между странами и защиты принципов безопасности граждан и прав конечных пользователей". Государствам-членам также рекомендуется "рассмотреть вопрос о создании платформы баз данных для обмена информацией по мобильным оконечным устройствам, которые украдены, потеряны или имеют незаконное происхождение, с использованием номеров MEID (идентификатора оборудования подвижной связи), применяемых при многостанционном доступе с кодовым разделением (CDMA), эволюционировавшей оптимизированной передаче данных (EV-DO) и двойном режиме CDMA/4G, а также, во многих сетях, RUIM (съемном модуле идентификации пользователя)".

ПКК.I также согласовал "Техническую книгу" по "Украденным и/или потерянным мобильным терминалам" (заключительный отчет 23-го собрания ПКК.I СИТЕЛ, 10 октября 2013 г., резолюция 217).

В мае 2014 года СИТЕЛ утвердила резолюцию 222 (XXIV-14) "Укрепление региональных мер по борьбе с распространением контрафактных, некачественных и неодобренных мобильных устройств".

В результате этого была создана группа, работающая по переписке, для обсуждения региональных мер по борьбе с распространением контрафактных, некачественных и неодобренных мобильных устройств в целях обмена с государствами-членами информацией, опытом и передовой технической и регуляторной практикой, которые касаются этого вопроса, в интересах разработки рекомендаций и руководящих указаний, которые можно было бы внедрять в регионе Северной и Южной Америки.

В августе 2014 года план работы этой группы, работающей по переписке, был утвержден и включен в сферу деятельности группы докладчиков по вопросам контроля за мошенничеством, по нормативной практике в случае несоблюдения требований в области электросвязи и региональным мерам по борьбе с кражей мобильных оконечных устройств со следующим мандатом:

1 Разработка определения того, что означают контрафактные, некачественные и неодобренные мобильные устройства.

2 Оценка масштабов и характера проблемы контрафактных, некачественных и неодобренных мобильных устройств.

3 Содействие обмену между членами СИТЕЛ информацией и опытом, которые касаются мер, принятых для борьбы с продажей и использованием контрафактных, некачественных и неодобренных мобильных устройств.

4 Документальное оформление передового опыта со всего мира в области борьбы с продажей и использованием контрафактных, некачественных и неодобренных мобильных устройств.

5 Предложение о создании технических книг, рекомендаций и/или резолюций СИТЕЛ, посвященных техническим и регуляторным мерам по борьбе с продажей и использованием контрафактных, некачественных и неодобренных мобильных устройств в регионе Северной и Южной Америки.

6 Завершение работы и представление отчета о достигнутых результатах группе докладчиков по вопросам нормативной практики в случае несоблюдения требований и контроля за мошенничеством в области электросвязи.

A.2.2 Восточноафриканское сообщество (BAC)

Ежегодные потери доходов стран Восточной Африки от поддельной продукции составляют более 500 млн. долл. США (http://www.trademarkea.com/ea-loses-huge-sums-of-money-in-counterfeit-products/). На упаковках дешевых некачественных продуктов, поставляемых через иностранных и местных продавцов и производителей, незаконным образом копируются названия и дизайн хорошо известных торговых марок.

Согласно протоколу Общего рынка, принятому BAC в 2010 году, положить конец контрафактным продуктам и торговле ими можно только с помощью сотрудничества.

Восточноафриканская организация связи (EACO) − это региональный орган, объединяющий регуляторные, почтовые, радиовещательные организации и организации электросвязи пяти государств-членов BAC (Кении, Танзании, Руанды, Бурунди и Уганды). EACO рассматривала вопрос контрафактных мобильных телефонов, наводнивших регион, и согласовала в 2012 году соответствующую совместную инициативу.

Целевая группа EACO по вопросам нумерации (CCK-Кения, TCRA-Танзания, RURA-Руанда, ARCT-Бурунди, UCC-Уганда) в мае 2012 года рекомендовала разработать национальные базы данных и процедуры, принятые для проверки радиотелефонных трубок, в целях защиты потребителей, предприятий и сетей от воздействия контрафакции (отчет Целевой группы EACO по вопросам нумерации за 2011−2012 гг.).

В 2012 году 19-му Конгрессу EACO была представлена информация о статусе внедрения в регионе регистров идентификации оборудованияs (EIR), и были изложены некоторые встреченные проблемы (http://www.eaco.int/docs/19_congress_report.pdf). К их числу относятся:

- дублирование и отсутствие международного идентификатора аппаратуры подвижной связи (IMEI);
- недостаточная информированность потребителей об опасностях, связанных с контрафактным оборудованием, и недостаточные знания о том, как проверять подлинность оборудования;
- недостаточная информированность продавцов/перепродавцов по вопросам, связанным с продажей дешевого некачественного оборудования; и
- высокая стоимость внедрения.

Для преодоления этих проблем были предложены следующие решения:

- проведение кампаний по повышению уровня информированности потребителей и местных продавцов;
- лицензирование всех продавцов/перепродавцов;
- совершенствование процедур одобрения типа;
- создание баз данных оборудования; и
- требование о регистрации SIM-карт.

A.2.3 Ассоциация регуляторных органов в области связи и электросвязи Сообщества португалоязычных стран (ARCTEL-CPLP)

Членами Ассоциации регуляторных органов в области связи и электросвязи Сообщества португалоязычных стран (ARCTEL-CPLP) являются Ангола, Бразилия, Кабо-Верде, Гвинея-Бисау, Мозамбик, Португалия, Сан-Томе и Принсипи и Восточный Тимор (http://www.arctel-cplp.org). На Глобальном симпозиуме МСЭ для регуляторных органов 2012 года ARCTEL-CPLP выступила с презентацией региональных подходов к борьбе с кражей мобильных телефонов, "серым" рынком и контрафактными устройствами (https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/Batista3_ARCTEL_Session3_mobilerobbery.pdf).

ARCTEL-CPLP предложила расширить традиционное решение (а именно национальные системы баз данных по "черным" спискам) до регионального уровня путем:

- обмена базами данных GSM и CDMA по "черным" спискам с помощью двусторонних или многосторонних соглашений;
- создания регуляторных налоговых и/или таможенных механизмов, которые обеспечивают более строгий контроль за импортом радиотелефонных трубок и предотвращают реэкспорт;
- соблюдения в отрасли рекомендаций по безопасности в целях предотвращения перепрограммирования или дублирования IMEI или серийного идентификационного номера электронного оборудования производителя;
- проведения кампаний по повышению уровня информированности населения о важности сообщать о краже или потере мобильных оконечных устройств.

_____