

2-я Исследовательская комиссия Вопрос 4

Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость, а также в борьбе с использованием контрафактного оборудования информационно-коммуникационных технологий и хищением мобильных устройств



Отчет о результатах работы по Вопросу 4/2 МСЭ-D

**Помощь развивающимся
странам в выполнении
программ по проверке на
соответствие и функциональную
совместимость, а также в
борьбе с использованием
контрафактного оборудования
информационно-
коммуникационных
технологий и хищением
мобильных устройств**

Исследовательский период 2018–2021 гг.



Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость, а также в борьбе с использованием контрафактного оборудования информационно-коммуникационных технологий и хищением мобильных устройств – Отчет о результатах работы по Вопросу 4/2 МСЭ-D за исследовательский период 2018–2021 годов

ISBN 978-92-61-34104-6 (электронная версия)

ISBN 978-92-61-34144-2 (версия EPUB)

ISBN 978-92-61-34154-1 (версия Mobi)

© Международный союз электросвязи, 2021 год

International Telecommunication Union, Place des Nations, CH-1211 Geneva, Switzerland

Некоторые права сохранены. Настоящая работа лицензирована для широкого применения на основе использования лицензии международной организации Creative Commons Attribution-Non-Commercial-ShareAlike 3.0 IGO licence (CC BY-NC-SA 3.0 IGO).

По условиям этой лицензии допускается копирование, перераспределение и адаптация настоящей работы в некоммерческих целях, при условии наличия надлежащих ссылок на настоящую работу. При любом использовании настоящей работы не следует предполагать, что МСЭ поддерживает какую-либо конкретную организацию, продукты или услуги. Не разрешается несанкционированное использование наименований и логотипов МСЭ. При адаптации работы необходимо в качестве лицензии на работу применять ту же или эквивалентную лицензию Creative Commons. При создании перевода настоящей работы следует добавить следующую правовую оговорку наряду с предлагаемой ссылкой: "Настоящий перевод не был выполнен Международным союзом электросвязи (МСЭ). МСЭ не несет ответственности за содержание или точность настоящего перевода. Оригинальный английский текст должен являться имеющим обязательную силу и аутентичным текстом". С дополнительной информацией можно ознакомиться по адресу: <https://creativecommons.org/licenses/by-nc-sa/3.0/igo/>.

Предлагаемая ссылка. "Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость, а также в борьбе с использованием контрафактного оборудования информационно-коммуникационных технологий и хищением мобильных устройств" – Отчет о результатах работы по Вопросу 4/2 МСЭ-D за исследовательский период 2018–2021 годов. Женева: Международный союз электросвязи, 2021 год. Лицензия CC BY-NC-SA 3.0 IGO.

Материалы третьих сторон. Желаящие повторно использовать содержащиеся в данной работе материалы, авторство которых принадлежит третьим сторонам, к примеру, таблицы, рисунки или изображения, несут ответственность за определение необходимости получения разрешения на такое повторное использование и получение разрешения от правообладателя. Риск, связанный с возможным предъявлением претензий в результате нарушения прав на любой компонент данной работы, принадлежащий третьим сторонам, несет исключительно пользователь.

Оговорки общего характера. Употребляемые обозначения, а также изложение материала в настоящей публикации не означают выражения какого бы то ни было мнения со стороны МСЭ или его Секретариата в отношении правового статуса какой-либо страны, территории, города или района, или их властей, а также в отношении делимитации их границ.

Упоминание конкретных компаний или продуктов определенных производителей не означает, что они одобряются или рекомендуются МСЭ в предпочтение аналогичных другим компаниям или продуктам, которые не упоминаются. За исключением ошибок и пропусков названия проприетарных продуктов выделяются начальными заглавными буквами.

МСЭ принял все разумные меры для проверки информации, содержащейся в настоящей публикации. Тем не менее, публикуемый материал распространяется без каких-либо гарантий, четко выраженных или подразумеваемых. Ответственность за истолкование и использование материала несет читатель. Ни при каких обстоятельствах МСЭ не несет ответственности за ущерб, возникший в результате использования этого материала.

Фото на обложке: Shutterstock

Выражение признательности

Исследовательские комиссии Сектора развития электросвязи МСЭ (МСЭ-D) обеспечивают нейтральную платформу, где собираются эксперты из правительственных органов, компаний отрасли, организаций электросвязи и академических организаций со всего мира с целью разработки практических инструментов и ресурсов для решения проблем развития. В связи с этим обе исследовательские комиссии МСЭ-D отвечают за разработку отчетов, руководящих указаний и рекомендаций на основе вкладов, полученных от членов. Решения об определении Вопросы для исследования принимаются раз в четыре года на Всемирной конференции по развитию электросвязи (ВКРЭ). Члены МСЭ, собравшиеся на ВКРЭ-17 в Буэнос-Айресе в октябре 2017 года, согласовали для 2-й Исследовательской комиссии на период 2018–2021 годов семь Вопросы в рамках общей темы "Использование услуг и приложений информационно-коммуникационных технологий в целях содействия устойчивому развитию".

Общее руководство подготовкой настоящего отчета по Вопросу 4/2 **"Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость, а также в борьбе с использованием контрафактного оборудования информационно-коммуникационных технологий и хищением мобильных устройств"** и координацию работы осуществлял руководящий состав 2-й Исследовательской комиссии МСЭ-D во главе с председателем г-ном Ахмадом Реза Шарафатом (Исламская Республика Иран), которому оказывали поддержку следующие заместители председателя: г-н Нассер Аль-Марзуки (Объединенные Арабские Эмираты) (сложил полномочия в 2018 г.), г-н Абдельазиз Альзаруни (Объединенные Арабские Эмираты), г-н Филипе Мигел Антунеш Батишта (Португалия) (сложил полномочия в 2019 г.), г-жа Нора Абдалла Хассан Башер (Судан), г-жа Мария Большакова (Российская Федерация), г-жа Селина Дельгадо Кастельон (Никарагуа), г-н Яков Гасс (Российская Федерация) (сложил полномочия в 2020 г.), г-н Ананда Радж Ханал (Республика Непал), г-н Роланд Йоу Кудозиа (Гана), г-н Толибджон Олтинович Мирзакулов (Узбекистан), г-жа Алина Модан (Румыния), г-н Генри Чуквудумеме Нкемаду (Нигерия), г-жа Ке Ван (Китай), г-н Доминик Вюрж (Франция).

Подготовкой Отчета руководил Докладчик по Вопросу 4/2 г-н Шейх Тиджани Удаа (Мавритания), с которым сотрудничали следующие заместители Докладчика: г-н Ахмаду Ди Ади Сисс (Мали), г-жа Амель Хиар (Алжир), г-н Джозеф Оная (Кения), г-н Брийан Харивони Ракоторатсиманжефи (Мадагаскар) и г-н Серинь Абду Лахатт Силла (Сенегал).

Особая благодарность выражается координаторам по главам за их преданность делу, поддержку и опыт.

Настоящий отчет был подготовлен при поддержке координаторов БРЭ, редакторов, а также группы по подготовке публикаций и секретариата исследовательских комиссий МСЭ-D.

Содержание

Выражение признательности	iii
Перечень таблиц и рисунков	vi
Резюме	vii

Глава 1 – Продукты информационно-коммуникационных технологий, способствующие достижению Целей в области устойчивого развития

1.1	Значимость продуктов ИКТ для общества	1
1.2	Вспомогательная роль устройств ИКТ в построении социальной экономики	1
1.3	Подключение и защита пользователей и сетей ИКТ путем обеспечения соответствия признанным стандартам	2
1.4	Влияние пандемии COVID-19 на процедуры одобрения типа	3

Глава 2 – Соответствие и функциональная совместимость

2.1	Введение	4
2.2	Обзор важнейших/приоритетных вопросов в странах и регионах	4
2.3	Технические требования и стандарты	5
2.4	Договоренности о взаимном признании/соглашения об оценке соответствия	6
2.4.1	Что такое договоренность/соглашение о взаимном признании?	6
2.4.2	Роль MRA в режиме C&I	7
2.5	Виртуальная инфраструктура	7
2.5.1	Виртуальное тестирование	7
2.5.2	Дистанционное тестирование на функциональную совместимость	8
2.5.3	Дистанционное тестирование в целях одобрения типа	9
2.6	Надзор за рынком	9
2.6.1	Основные заинтересованные стороны	10
2.6.2	Консультации по вопросу об обмене данными и опытом в сфере надзора за рынком	10
2.7	Оценка соответствия новых технологий	10
2.7.1	Трудности, связанные с новыми технологиями	11
2.7.2	Предварительное тестирование на соответствие	11
2.7.3	Предполагаемое воздействие	11

Глава 3 – Борьба с распространением контрафактных, не соответствующих стандартам и поддельных устройств

3.1	Проблемы и вопросы	12
3.2	Определения	13
3.3	Руководящие указания	14
3.4	Национальный опыт (исследование конкретных ситуаций)	15
3.4.1	Мадагаскар	15
3.4.2	Гвинея	16
3.4.3	Сенегал	16
3.4.4	Руанда	17
3.4.5	Зимбабве	17
3.4.6	Гана	17
3.4.7	Пакистан	18
3.4.8	Ассоциация GSM	19
3.4.9	Бразилия	19
3.4.10	Оман	20
3.4.11	Международные стандарты и рекомендации	20

Глава 4 – Хищение мобильных устройств	21
4.1 Введение	21
4.2 Проблемы и задачи	21
4.2.1 Преступные и мошеннические действия, связанные с устройствами.....	22
4.2.2 Задачи и ответственность заинтересованных сторон	22
4.2.3 Важнейшие инструменты борьбы с хищением устройств	23
4.3 Руководящие указания	23
4.4 Национальный опыт (исследование конкретных ситуаций)	24
4.4.1 Центральноафриканская Республика	24
4.4.2 Мексика	25
4.4.3 Научно-технологический университет Ирана.....	26
Глава 5 – Интернет вещей и C&I	27
5.1 Введение	27
5.2 Влияние IoT на C&I и разработку ИКТ	27
5.2.1 Задачи в области IoT	27
5.2.2 Сложности в сфере IoT	28
5.2.3 Пример: Тестирование IoT, применяемое в Rohde & Schwarz	30
5.2.4 Организации по разработке стандартов	30
5.3 Регулирование и политика в области IoT и ИКТ	31
5.3.1 Обзор совместного регулирования	31
5.3.2 Регулирование IoT	32
5.4 Заключение.....	33
Глава 6 – Передача информации, ноу-хау и знаний.....	34
6.1 Потребности в плане обучения и образовательные возможности в сфере C&I	34
6.2 Удовлетворение потребностей, связанных с получением/сохранением знаний	34
6.3 Выводы	36
Annexes	37
Annex 1: Conformance and interoperability frameworks: country data	37
Annex 2: Counterfeiting – a survey of national frameworks and practices.....	38
Annex 3: Initiatives in the fight against equipment counterfeiting and mobile terminal theft in Burundi.....	40
A3.1 Introduction.....	40
A3.2 Impact of the proliferation and use of counterfeit mobile terminals	40
A3.3 National initiatives in the fight against mobile terminal theft and equipment counterfeiting	40
A3.4 Conclusion	41
Annex 4: Illustrations for chapters of the Output Report on Question 4/2.....	42
Annex 5: Ideas for the future of the Question	45
Annex 6: List of contributions and liaison statements received on Question 4/2.....	46

Перечень таблиц и рисунков

Таблица

Table 1A: Summary of ITU World Telecommunication/ICT Regulatory Survey (edition 2019): Survey on regulatory practices related to the distribution and use of counterfeit ICTs	38
---	----

Рисунки

Рисунок 1: Деятельность по оценке соответствия	5
Рисунок 2: Дистанционное тестирование на функциональную совместимость	8
Рисунок 3: Дистанционное тестирование в целях одобрения типа	9
Рисунок 4: Снижение продаж из-за фальшивых смартфонов в ЕС и во всем мире.....	12
Рисунок 5: Ответственность за борьбу с контрафакцией	14
Рисунок 6: Процесс одобрения типа	18
Рисунок 7: Система идентификации, регистрации и блокировки устройств (DIRBS)	19
Рисунок 8: Схема работы SEMI	20
Рисунок 9: Число активных подключенных устройств в мире	27
Рисунок 10: Беспроводные технологии, используемые для IoT	28
Рисунок 11: Число общеизвестных платформ IoT	29
Рисунок 12: Схематический обзор альянсов и организаций по разработке стандартов в области IoT (в вертикальной и горизонтальной плоскостях).....	29
Рисунок 13: Необходимость адаптированных схем сертификации	30
Рисунок 14: Измерения ОТА	30
Рисунок 15: Поколения регулирования в области ИКТ– концептуальная схема	32
Рисунок 16: Совместное регулирование	32
Рисунок 17: Учебные модули СИП (ОМ – обязательные модули, ЭМ – элективные модули).....	35
Figure 1A: Legal C&I Frameworks from 114 countries that provided information	37
Figure 2A: Regional distribution of responses from survey – Question 1	39
Figure 3A: Regional distribution of responses from survey – Question 2	39
Figure 4A: Regional distribution of responses from survey – Question 3	39
Figure 5A: Illustration for Chapter 2 – What is conformance and interoperability (C&I)	42
Figure 6A: Illustration for Chapter 2 – C&I frameworks.....	43
Figure 7A: Illustration for Chapter 3 – Combating the proliferation of counterfeit, substandard and tampered devices.....	43
Figure 8A: Illustration for Chapter 5 – The Internet of Things and C&I.....	44

Резюме

Использование устройств ИКТ и доверие к ним в мире

Устройства информационно-коммуникационных технологий (ИКТ) являются главными воротами в цифровой мир. Координация в области стандартов и обеспечение соответствия им на глобальном уровне играют ключевую роль в обеспечении функциональной совместимости сетей и возможности взаимодействия пользователей и машин.

Прогресс в осуществлении программ по проверке на соответствие и функциональную совместимость (C&I) и передовых методов борьбы с распространением контрафактного оборудования ИКТ и хищением мобильных устройств наблюдается во всех странах, однако некоторые из стран продвигаются вперед быстрее, чем остальные.

Сектор развития электросвязи (МСЭ-D) оказывает Государствам-Членам помощь в оценке технических и экономических проблем, касающихся соответствия и функциональной совместимости устройств ИКТ, уделяя особое внимание вопросам содействия, создания потенциала и обмена передовой практикой Государств – Членов МСЭ. МСЭ-D тесно сотрудничает по этим аспектам с Сектором радиосвязи (МСЭ-R) и Сектором стандартизации электросвязи (МСЭ-T) в целях создания синергии в этих усилиях и достижения более широкого воздействия.

Кроме того, во все более соединенном при помощи устройств ИКТ обществе использование систем C&I продолжает оставаться предметом широких споров между разработчиками, производителями, импортерами, операторами и пользователями. В этом контексте ключевая роль в поиске равновесия между необходимыми уровнями безопасности и контроля принадлежит регуляторным органам.

И наконец, еще один важный вопрос для будущего C&I – это появление новых технологий во всех отраслях, работающих при поддержке интернета вещей (IoT), и стандарты, которые необходимо учитывать при внедрении или пересмотре систем C&I в развивающихся странах.

В этом контексте в настоящем отчете рассматривается передовая практика в интересах выработки оптимальных решений.

Подготовительная работа в области C&I

В ходе предыдущих исследовательских периодов МСЭ уделял основное внимание значимому вопросу оказания помощи развивающимся странам в вопросах обеспечения соответствия и функциональной совместимости. Был получен ряд важных результатов, которые остаются актуальными для работы МСЭ-D по Вопросу 4/2. С предыдущим отчетом по Вопросу 4/2 можно ознакомиться в интернете по адресу: <https://www.itu.int/pub/D-STG-SG02.04.1-2017>, а информация о дополнительных видах деятельности МСЭ-D по оказанию помощи развивающимся странам, таких как, например, база данных национальных и региональных систем C&I, региональные оценки и мероприятия по созданию потенциала, размещена в интернете по адресу: https://itu.int/go/CI_Development.

Глава 1 – Продукты информационно-коммуникационных технологий, способствующие достижению Целей в области устойчивого развития

1.1 Значимость продуктов ИКТ для общества

Цифровая трансформация способствует стремительным изменениям в каждой отрасли и во всех аспектах нашей жизни. В результате развития трех фундаментальных составляющих информационно-коммуникационных технологий (ИКТ) — подвижной связи, широкополосного доступа и облачных технологий — трансформируются цепочки создания стоимости, происходит цифровизация бизнес-моделей, сокращаются расстояния. Так формируется новая экономика услуг, в которой, например, люди могут все чаще пользоваться товарами и услугами совместно, а не покупать их в собственность: все это наглядно демонстрирует, как цифровая эпоха порождает новые инновационные бизнес-модели и преобразует нашу жизнь¹.

Главными преимуществами ИКТ являются расширение доступа, возможности установления соединений и повышение эффективности для отдельных лиц, сообществ и экономик²:

- *доступ к информации и услугам*: благодаря устройствам и инфраструктуре ИКТ, а также использованию таких технологий как мобильные телефоны, сотовые сети электросвязи (например, 3G и LTE), интернет и широкополосная связь ИКТ могут способствовать улучшению универсального доступа к информации и услугам для людей во всем мире, как в сельских, так и в городских районах;
- *возможность установления соединений* между людьми и организациями: установление соединений между отдельными лицами, организациями и сетями в мгновенном или близком к мгновенному режиме может способствовать повышению производительности и внедрению инноваций во многих отраслях и сообществах, а также обеспечить связь в режиме реального времени, необходимую для быстрого развертывания критически важных услуг;
- *повышение эффективности за счет роста производительности* и рационального использования ресурсов;
- внедрение "*зеленых*" стандартов путем обеспечения соответствия в целях уменьшения последствий изменения климата;
- способность ИКТ содействовать раскрытию и использованию преимуществ от *повышения производительности* за счет улучшения доступа к информации и коммуникации между отдельными лицами (и тем самым сокращения расходов на поездки, сбор данных вручную), а также обеспечения инфраструктуры для сбора и анализа больших массивов данных ("больших данных").

1.2 Вспомогательная роль устройств ИКТ в построении социальной экономики

Для осуществления последовательной политики и укрепления инициатив в области развития с использованием ИКТ необходима стратегическая рамочная основа. ИКТ должны быть интегрированы во все аспекты государственной политики и экономической деятельности. Для этого необходимо следующее:

- разработать государственную политику и нормативные положения, обеспечивающие возможность полноценного использования ИКТ;
- обеспечить быстрое распространение и модернизацию инфраструктуры ИКТ;
- поощрять государственно-частные партнерства в целях содействия развитию новых стартапов в области ИКТ, которые будут предоставлять значимые на местном уровне услуги;

¹ Предисловие Ханса Вестберга, президента и генерального директора компании Ericsson, к [Заключительному отчету по ИКТ и ЦУР: как информационно-коммуникационные технологии могут ускорить достижение Целей в области устойчивого развития](#). Подготовлено Институтом исследования проблем Земли, Колумбийским университетом и компанией Ericsson.

² Компания Huawei. [Контрольные показатели ИКТ для Целей в области устойчивого развития за 2017 год](#). Huawei, 2017 год.

- урегулировать вопросы функциональной совместимости ИКТ;
- создавать потенциал для управления системами ИКТ;
- принимать меры к тому, чтобы политика и регулирование успевали за стремительно развивающимися инновациями и развертыванием ИКТ.

1.3 Подключение и защита пользователей и сетей ИКТ путем обеспечения соответствия признанным стандартам

Инвестиции в инфраструктуру и инновации являются важнейшей движущей силой экономического роста и развития. Технический прогресс также играет ключевую роль в определении долгосрочных решений как для экономических, так и для экологических задач, таких как создание новых рабочих мест и повышение энергоэффективности. Поощрение развития экологически безопасных отраслей промышленности и инвестирование в научные исследования и инновации — это все важные пути содействия устойчивому развитию³.

ЦУР 9: Создание стойкой инфраструктуры, содействие всеохватной и устойчивой индустриализации и инновациям

Задачи:

9.1 Развивать качественную, надежную, устойчивую и стойкую инфраструктуру, включая региональную и трансграничную инфраструктуру, в целях поддержки экономического развития и благополучия людей, уделяя особое внимание обеспечению недорогого и равноправного доступа для всех;

9.a Содействовать развитию экологически устойчивой и стойкой инфраструктуры в развивающихся странах за счет увеличения финансовой, технологической и технической поддержки африканских стран, наименее развитых стран, развивающихся стран, не имеющих выхода к морю, и малых островных развивающихся государств;

9.b Поддерживать разработки, исследования и инновации в сфере отечественных технологий в развивающихся странах, в том числе путем создания политического климата, благоприятствующего, в частности, диверсификации промышленности и увеличению добавленной стоимости в сырьевых отраслях;

9.c Существенно расширить доступ к информационно-коммуникационным технологиям и стремиться к обеспечению всеобщего и недорогого доступа к интернету в наименее развитых странах к 2020 году.

Для защиты пользователей и сетей ИКТ весьма важно сосредоточиться на следующих аспектах:

- качество;
- безопасность;
- функциональная совместимость;
- свободная от помех спектральная среда;
- национальные правила;
- экологическая безопасность;
- надежность;
- устойчивость;
- доступность в ценовом отношении (за счет экономии от масштаба, возможной благодаря работе по обеспечению соответствия и функциональной совместимости, или C&I).

³ Программа развития Организации Объединенных Наций (ПРООН). Цели в области устойчивого развития. [ЦУР 9: Промышленные инновации и инфраструктура](#).

Для этих целей должны быть приняты во внимание вопросы, связанные с оборудованием и системами ИКТ, в том числе:

- технические требования и стандарты;
- оценка соответствия;
- контроль оборудования;
- слепопродажное наблюдение;
- содействие заключению соглашений о взаимном признании.

Следовательно, необходимо внедрять **инновационные методы** оценки C&I, в том числе:

- создание новых или совместное использование имеющихся лабораторий по тестированию;
- услуги виртуальных лабораторий;
- соглашения о взаимном признании (MRA), отражающие местные и региональные требования и ограничения;
- слепопродажное наблюдение;
- решения для интеллектуального тестирования;
- согласование стандартов.

К **задачам** относятся:

- повышение осведомленности;
- создание сетевой платформы для взаимодействия членов МСЭ-D по вопросам C&I;
- поощрение сотрудничества, исследовательской работы и обмена опытом по направлениям, охватываемым Вопросом;
- обеспечение представительства членов МСЭ-D на других форумах, занимающихся вопросами C&I (например, на собраниях группы ИСО/CASCO STAR);
- подготовка вопросника для сбора данных по стране и отслеживания прогресса в области C&I;
- разработка руководящих указаний;
- публикация рекомендаций.

1.4 Влияние пандемии COVID-19 на процедуры одобрения типа

Пандемия COVID-19 оказала – и продолжает оказывать – значительное воздействие на международную торговлю и оценку соответствия продуктов, включая устройства ИКТ. Из-за закрытия границ и трудностей с доступом к оборудованию (например, к физическим лабораториям по тестированию, а также к услугам специалистов в данной области) серьезно пострадала деятельность по одобрению типа. В этих условиях возникла необходимость поиска инновационных способов сертификации соответствия и качества продуктов. Регуляторные органы, производители и операторы разрабатывают нестандартные решения, для того чтобы поддерживать работу бизнеса и не допускать нарушений торговой цепочки. Настало время задействовать весь потенциал цифровых технологий для выработки возможных способов оценки соответствия.

Глава 2 – Соответствие и функциональная совместимость

2.1 Введение

Оценка соответствия гарантирует, что оборудование ИКТ отвечает требованиям технических спецификаций и стандартов. Проверка на соответствие позволяет поставщикам и пользователям оценить, как будет работать оборудование при его интегрировании в сеть с другими устройствами для предоставления сетевой услуги. Тестирование на функциональную совместимость позволяет оценить, правильно ли два или более продуктов выполняют технические спецификации, которые необходимы для успешной интеграции, обеспечивающей конкретные протоколы связи.

Тестирование на соответствие и функциональную совместимость играет важную роль в выявлении таких характеристик оборудования для сети ИКТ, которые могут не отвечать признанным отраслевым стандартам и, соответственно, пагубно отразиться на качестве предоставляемых сетевых услуг. Доступность передовых высококачественных продуктов для коммерческого использования способствует широкому развертыванию сетевых технологий и связанных с ними сетевых услуг.

2.2 Обзор важнейших/приоритетных вопросов в странах и регионах

Вопросы C&I сопряжены с целым рядом опасений и проблем, в частности следующих⁴:

- функционирование служб сигнализации интеллектуальных сетей прежних версий (проблемы совместимости) при замене оборудования, сигнализация в сетях подвижной связи (например, доступ, базовая сеть, SMS);
- несоответствие и недостаточная функциональная совместимость оборудования от разных поставщиков;
- нестандартизированные интерфейсы или протоколы, используемые в оборудовании разных производителей;
- оборудование одного и того же производителя с разными версиями программного обеспечения, что приводит к несовместимости клиентов протокола инициации сеанса (SIP);
- соответствие установленным требованиям оборудования абонентских приставок (STB), выпускаемых разными производителями межплатформенных программных средств на основе протокола Интернет (IPTV);
- полоса пропускания, то есть пропускная способность для передачи голоса, данных и видеоизображения при повышенной пользовательской нагрузке на существующую сеть;
- достижение функциональной совместимости в сложных сетях путем интеграции сетей и устройств;
- услуги, предлагаемые некоторыми поставщиками, которые не обеспечены инфраструктурой и специалистами службы поддержки, позволяющими взаимодействовать с другими операторами;
- разработка системы методов для принятия стандартов;
- управление данными о вызовах для выставления счетов;
- реализация новых функций и услуг на всех платформах;
- наличие разных моделей начисления платы;
- новые технологии, несовместимые с традиционным оборудованием;
- нехватка центров тестирования и тестового оборудования;
- нехватка квалифицированного персонала для решения задач C&I;

⁴ МСЭ-D, Заключительный отчет по Вопросу 4/2 2-й Исследовательской комиссии МСЭ-D за исследовательский период 2014–2017 годов "[Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость](#)". МСЭ, 2017 год.

- проблемы поддержки ЦСИС;
- проблемы пользовательских терминалов различных систем;
- вопросы функциональной совместимости услуг с оконечным абонентским оборудованием;
- использование поставщиками проприетарных нестандартных интерфейсов;
- затраты;
- нехватка кадров и возможностей для обучения;
- слабые институциональные системы;
- недостаточное понимание вопросов стандартизации;
- проблемы функциональной совместимости.

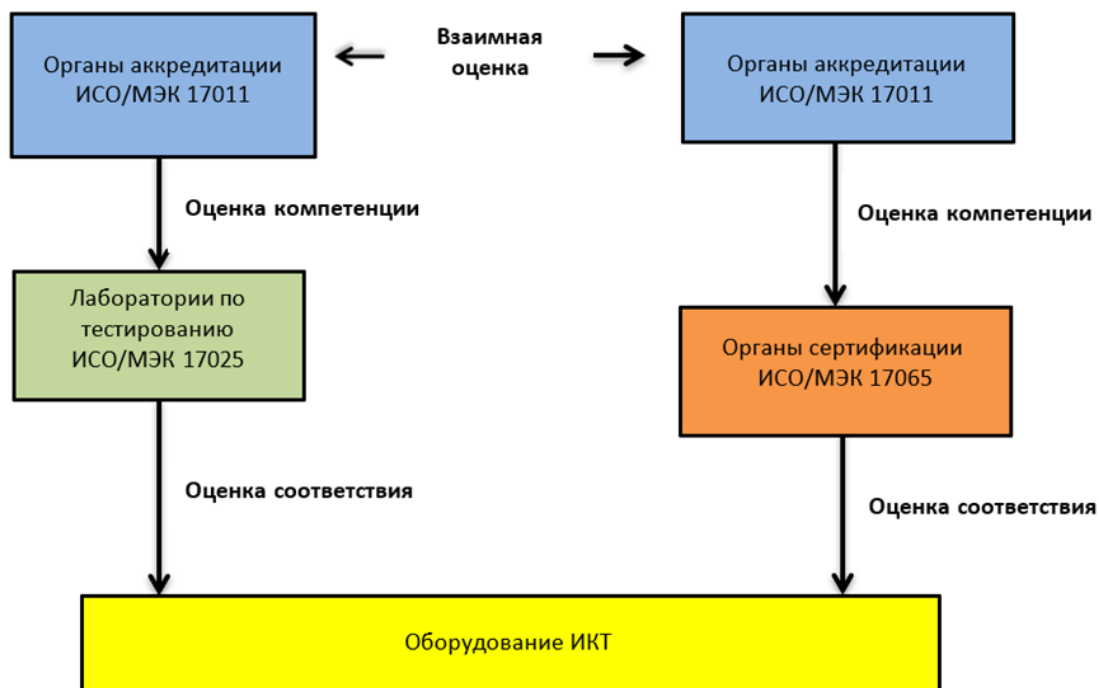
Деятельность по оценке соответствия

К видам деятельности по оценке соответствия относятся:

- назначение/признание органов по аккредитации;
- назначение/признание органов по сертификации;
- назначение/признание лабораторий по тестированию;
- регистрация/сертификация.

Виды деятельности по оценке соответствия приведены на **Рисунке 1**.

Рисунок 1: Деятельность по оценке соответствия



2.3 Технические требования и стандарты

Поставщики услуг и операторы определяют стандарты и требования для оборудования и систем, которые они используют для предоставления услуг потребителям. Национальные регуляторные органы устанавливают нормативные требования, стандарты и спецификации для оборудования и систем, развертываемых на территориях их стран. Пользователи, поставщики услуг и национальные регуляторные органы нуждаются в подтверждении и доказательствах того, что оборудование и системы

отвечают требованиям соответствующих стандартов и спецификаций и способны взаимодействовать установленным образом⁵.

В целях скорейшей разработки международных стандартов, руководств и рекомендаций Комитет по техническим барьерам в торговле (ТБТ) Всемирной торговой организации (ВТО) определил следующие шесть принципов⁶:

- прозрачность;
- открытость;
- беспристрастность и консенсус;
- актуальность и эффективность;
- согласованность;
- аспекты развития.

Значение стандартов

Соответствие техническим стандартам:

- имеет ключевое значение для функциональной совместимости оборудования и сетей;
- снижает риск оказаться "привязанным" к определенной технологии или поставщику;
- обеспечивает соблюдение законных интересов, в том числе в сфере безопасности и непричинения помех;
- способствует региональной интеграции;
- способствует укрупнению рынков, повышению конкуренции и развитию торговли.

Новые процедуры

Новые процедуры предполагают следующее сочетание:

- декларация производителя о соответствии, тестирование на соответствие коммерческими предприятиями по тестированию и надзор за рынком;
- глобальные стандарты и MRA в отношении стандартов и одобрений между странами или группами стран.

2.4 Договоренности о взаимном признании/соглашения об оценке соответствия

2.4.1 Что такое договоренность/соглашение о взаимном признании?

Договоренность о взаимном признании/соглашение об оценке соответствия (далее именуемые MRA) – это добровольная договоренность/соглашение (о процедурах и процессах) между сторонами (частными или государственными организациями) о признании результатов оценки соответствия.

Соглашение о взаимном признании представляет собой официальное письменное обязательство сторон по признанию результатов оценки соответствия в отношении оборудования электросвязи. Его предметом являются регуляторные требования, поэтому ниже оно именуется "регуляторным MRA". Такие соглашения часто заключаются на двусторонней, региональной или многосторонней основе между двумя или более правительствами.

Договоренность о взаимном признании – это добровольная договоренность между сторонами о признании результатов оценки соответствия в отношении оборудования электросвязи. Ее предметом являются нерегуляторные требования, поэтому она именуется ниже "нерегуляторным MRA". Примером договоренности о взаимном признании является обязательство органов аккредитации на взаимной

⁵ МСЭ. [Создание режимов соответствия и функциональной совместимости: полные руководящие указания](#), февраль 2015 года.

⁶ ВТО. Комитет по техническим барьерам в торговле. Документ [G/TBT/9](#), ноябрь 2000 года.

основе признавать результаты оценки соответствия, полученные аккредитованными органами по оценке соответствия.

Стороны МРА несут обязательства по выполнению процессов и процедур, направленных на осуществление МРА к их обоюдной выгоде. Это относится как к регуляторным, так и к нерегуляторным МРА.

МРА не наносит ущерба деятельности регуляторных органов в юрисдикции сторон соглашения/ договоренности. В МРА следует указать различные органы, участвующие в его осуществлении:

- *сторона*: организация, которая дала согласие на участие в МРА;
- *назначающий орган*: государственный орган или признанный компетентный орган, определенный стороной для назначения органа по оценке соответствия для целей проведения оценки соответствия согласно МРА;
- *орган по аккредитации*: орган, ответственный за оценку и признание конкретной компетенции лабораторий по тестированию и/или органов по сертификации в соответствии с международными стандартами;
- *орган по оценке соответствия*: орган, назначаемый для целей проведения оценки соответствия требованиям в области электросвязи другой стороны согласно МРА (это может быть третья сторона, тестовая лаборатория поставщика или орган по сертификации);
- *объединенный комитет*: комитет, учреждаемый сторонами для руководства составлением и осуществлением МРА, внесения коррективов, а также решения по мере необходимости любых других вопросов, касающихся бесперебойного функционирования МРА, в том числе будущих изменений и коррективов;
- *регуляторный орган*: ведомство, обладающее правовыми полномочиями и ответственное за вопросы электросвязи.

2.4.2 Роль МРА в режиме C&I

МРА служат для целей:

- признания компетенции третьих сторон в области выполнения национальных регуляторных процессов/процессов одобрения типа;
- предотвращения дублирования затрат на тестирование и поощрения прозрачности;
- облегчения доступа на зарубежные рынки;
- экономии времени вывода на рынок и производственных затрат;
- преодоления хищнической практики и препятствий для выхода на рынок;
- оптимизации процедур и методов и содействия тем самым снижению затрат производителей, осуществляющих продажу на многих рынках.

Конечная цель: "Единственное тестирование, действительное по всему миру".

2.5 Виртуальная инфраструктура

2.5.1 Виртуальное тестирование⁷

В отрасли ИКТ расширяется спектр услуг, предоставляемых виртуально, через интернет. Эта новая реальность охватывает также формирующиеся механизмы оценки установления соединений оборудования ИКТ по IP-сетям и согласуется с потребностями новых конвергированных сетей.

Виртуальные лаборатории способны предоставлять своевременные, доступные в ценовом отношении и стабильные услуги по тестированию развивающимся странам, которым недостает собственных возможностей для проведения тестирования.

⁷ МСЭ-D. Заключительный отчет по Вопросу 4/2. (Исследовательский период 2014–2017 гг.). Там же.

Ниже описываются два практических решения для виртуального тестирования – дистанционное тестирование на функциональную совместимость и дистанционное тестирование на одобрение типа.

2.5.2 Дистанционное тестирование на функциональную совместимость

Цель: Оценка сетей операторов в разных странах/регионах на функциональную совместимость.

Мировой опыт указывает на необходимость стандартизированных процедур тестирования и сертификации продуктов на базе ИКТ для предупреждения многочисленных проблем, которые они в противном случае создают пользователям и операторам.

Рисунок 2: Дистанционное тестирование на функциональную совместимость



Недостаточная функциональная совместимость может привести к множеству проблем, включая:

- снижение скорости передачи данных;
- ненадежная связь;
- сокращение срока эксплуатации устройств и оборудования;
- высокое энергопотребление;
- создание службами помех друг другу (особенно в беспроводных системах);
- не соответствующее стандартам оборудование, сдерживающее технический прогресс и несовместимое с новыми технологиями и протоколами;
- функциональная несовместимость оборудования, вызывающая проблемы связи (которые часто очень трудно диагностировать);
- непостоянные рабочие характеристики сети из-за отсутствия процедур контроля изменений в оборудовании и программном обеспечении;
- трудности взаимодействия между оборудованием разных производителей и между сетями разных стран.

Удаленное тестирование может осуществляться в следующих конкретных целях: разработка продуктов, сертификация регуляторными органами, предварительное тестирование на соответствие и функциональную совместимость продуктов ИКТ, оценка соответствия мобильных устройств и IP-протоколов, а также эксплуатационное обслуживание.

Целевая аудитория: операторы электросвязи, производители и пользователи оборудования (имеющие ряд потребностей – клиенты, операторы, объединения, регуляторные органы и т. д.).

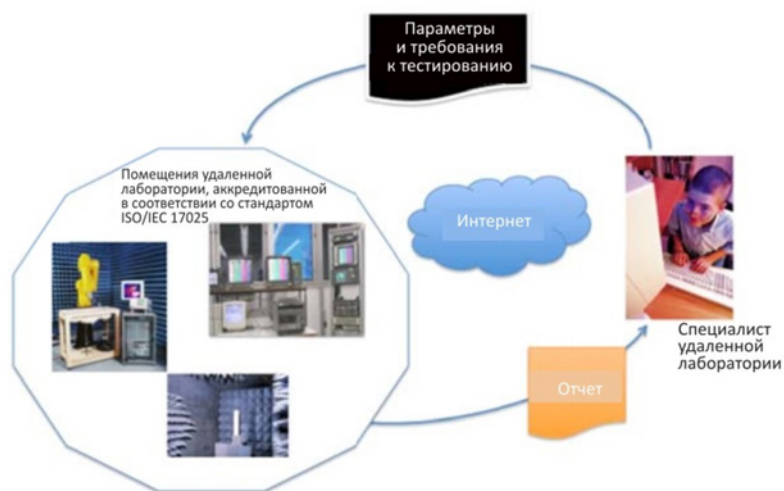
Желательно установить тесные и прочные партнерские связи с крупнейшими производителями контрольно-измерительных систем, что гарантирует быстрое обновление инфраструктуры в случае такой необходимости.

2.5.3 Дистанционное тестирование в целях одобрения типа

Цель: Обеспечение дистанционного доступа к физической инфраструктуре для проведения тестирования для одобрения типа.

Дистанционное тестирование в целях одобрения типа позволяет проводить лабораторное тестирование в процессе разработки, предварительное тестирование на соответствие, а также тестирование на соответствие и функциональную совместимость образцов продуктов ИКТ с использованием дистанционных или виртуальных средств и инфраструктуры других лабораторий. Образцы предоставляются другими организациями (участие сообществ).

Рисунок 3: Дистанционное тестирование в целях одобрения типа



Комплекс предлагаемых лабораторией услуг может предоставляться в несколько этапов:

- Этап 1: дистанционное обучение.
- Этап 2: тестирование образцов с видеозаписью каждого шага и передачей данных для составления отчета.
- Этап 3: местная лаборатория все более активно участвует в тестировании некоторых типов продуктов, в частности основных сетевых продуктов (с тем чтобы максимально использовать возможности по удовлетворению потребностей основной инфраструктуры).
- Этап 4: обеспечение инфраструктуры для дистанционного тестирования (инвестиции в надлежащую инфраструктуру для измерений).
- Этап 5: консультирование и обучение для подготовки перехода к приобретению местной инфраструктуры для тестирования (если это целесообразно).

Требования: применимые стандарты, тестирование, отбор и т. д.

2.6 Надзор за рынком

Цель надзора за рынком развешиваемого оборудования электросвязи – обеспечить условия для того, чтобы продукты, реализуемые на рынке, не создавали электромагнитных помех, не наносили ущерба сетям электросвязи общего пользования, не угрожали здоровью и безопасности и не вредили общественным интересам любым другим образом. На практике надзор за рынком включает в себя любые меры (в том числе запрет, изъятие, снятие с продажи), необходимые для прекращения распространения продуктов,

которые не отвечают требованиям, изложенным в соответствующих законодательных и регуляторных положениях, обеспечения соответствия продуктов установленным требованиям и применения санкций. Надзор за рынком жизненно важен для бесперебойного функционирования рынка электросвязи. Он необходим для защиты потребителей и работников от рисков, связанных с продуктами, которые не соответствуют нормам. Кроме того, надзор за рынком помогает защитить ответственных предпринимателей от нечестной конкуренции со стороны недобросовестных участников рынка, которые игнорируют или пытаются обходить установленные правила. Многие регуляторные органы во всем мире применяют конкретные законодательные требования в области организации надзора за рынком. В регуляторных положениях, как правило, четко излагаются обязанности осуществляющих надзор за рынком органов, в том числе предусматривающие наличие у этих органов необходимых полномочий, ресурсов и знаний для надлежащего выполнения своих функций. Должны быть введены процедуры для рассмотрения жалоб, отслеживания конкретных инцидентов, проверки правильности мер по исправлению ситуации и сбора научно-технической информации по вопросам безопасности.

2.6.1 Основные заинтересованные стороны

Основными заинтересованными сторонами являются:

- правительства/регуляторные органы;
- органы по аккредитации (AB);
- органы по оценке соответствия (СAB);
- производители, импортеры, поставщики оборудования и услуг.

2.6.2 Консультации по вопросу об обмене данными и опытом в сфере надзора за рынком

К этим видам деятельности относятся:

- обмен информацией и консультации с другими странами, внедрившими программы надзора за рынком и обеспечения соблюдения, в частности в границах регионов, имеющих общий язык и, возможно, общую систему управления использованием спектра и частотные присвоения службам;
- направление партнерам уведомлений или заблаговременных предупреждений, касающихся проблем соответствия установленным требованиям технологий и продуктов, которые могут быть вскоре развернуты в конкретной стране или регионе, с тем чтобы оповестить партнеров о возможных проблемах соответствия при более широком развертывании продуктов или технологий и обеспечить возможность более четко направлять работу инспекторов и аудиторов.

2.7 Оценка соответствия новых технологий

Поскольку услуги и приложения ИКТ присутствуют во всех аспектах жизни людей, а распространение новых технологий (IoT, 5G и пр.) становится реальностью, обеспечение соответствия и функциональной совместимости превратится в серьезную проблему для развивающихся стран, в случае если они не успеют подготовиться к этим изменениям.

Ожидание будущего, где все будет соединено, подпитывает спрос на C&I. Развивающиеся страны ищут инновационные пути решения возникающих проблем, в том числе за счет:

- установления общих технических требований;
- определения основных технических ориентиров на международном уровне (стандартов);
- разработки политики для обеспечения надежных систем C&I в целях поощрения сотрудничества в среде ИКТ с участием многих заинтересованных сторон (например, путем учреждения соответствующих механизмов, включая принятие деклараций поставщиков и соглашений о взаимном признании).

2.7.1 Трудности, связанные с новыми технологиями

К таким трудностям относятся:

- влияние проблем функциональной совместимости на работу по расширению масштаба:
 - понимание на уровне регуляторных органов;
 - восприятие нормативных положений как помехи для выхода на рынок;
- понимание среди разработчиков и восприятие C&I:
 - затраты в денежном выражении;
 - затраты, связанные с аспектами безопасности и кадров.
- ограниченное финансирование и ресурсы для проектов/продуктов:
 - затраты на сертификацию;
 - рынки еще находятся на этапе становления.

2.7.2 Предварительное тестирование на соответствие

Для предварительного тестирования на соответствие требуются:

- понимание C&I:
 - сообразно конкретному формату продукта;
 - на всех этапах продвижения продукта на рынок;
- понимание влияния C&I:
 - оценка затрат (в денежном, временном, техническом выражении) на запуск стартапа;
 - восприятие нормативных положений как преимущества, а не как помехи.

2.7.3 Предполагаемое воздействие⁸

Меры C&I способны расширить возможности для успеха путем:

- содействия разработке "умного" ассортимента продуктов;
- внедрения C&I с самого начала;
- четкого понимания, какие кадры и ресурсы и на каком этапе потребуются.

Они также способны помочь регуляторным органам придать импульс развитию появляющихся продуктов и бизнеса путем:

- содействия заключению межотраслевых MRA;
- поощрения осознанного взаимодействия с предпринимателями.

⁸ МСЭ. [Тематическая сессия по Вопросу 4/2](#). 16 октября 2019 года.

Глава 3 – Борьба с распространением контрафактных, не соответствующих стандартам и поддельных устройств

Сегодня рынок контрафактных мобильных устройств ИКТ и торговля ими – это глобальная социально-экономическая проблема, которая негативно сказывается на инновационной и инвестиционной деятельности, экономическом росте, сфере здоровья и занятости. Также существует опасность перенаправления ресурсов в распоряжение организованной преступности.

Всемирная конференция по развитию электросвязи в 2017 году (ВКРЭ-17) в своей Резолюции 79 (Пересм. Буэнос-Айрес, 2017 г.) определила борьбу с распространением контрафактного оборудования и устройств в качестве приоритетного направления работы по Вопросу 4/2. В настоящей главе описываются проблемы, создаваемые контрафактными устройствами электросвязи/ИКТ, и предлагаются руководящие указания по их выявлению и борьбе с их использованием.

3.1 Проблемы и вопросы

Производство контрафактного оборудования электросвязи/ИКТ, особенно мобильных телефонов, представляет собой глобальную проблему для пользователей, производителей и правительств, а также для инновационной и инвестиционной деятельности и экономического роста. Ведомство по интеллектуальной собственности Европейского союза (EUIPO) оценило потери прибыли от продаж смартфонов из-за контрафактной продукции в 2015 году в 45,3 млрд. евро⁹.

Рисунок 4: Снижение продаж из-за фальшивых смартфонов в ЕС и во всем мире



Что касается пользователей, то стимулами к распространению контрафактных терминалов служат следующие факторы:

- контрафактные и поддельные устройства часто доступнее в ценовом отношении, нежели подлинные, и обеспечивают доступ к сети;
- такие устройства предоставляют пользователям удобные функциональные возможности, такие как использование нескольких SIM-карт, ТВ, FM-радио, а также различные полезные услуги мобильного интернета (чат, видеозвонки, просмотр веб-страниц, денежные переводы и т. д.) при небольших затратах.

⁹ EUIPO. [Исследование проблемы контрафактных смартфонов](#), октябрь 2018 года.

Отрицательное влияние контрафактных терминалов на здоровье людей, на качество сетей, услуг и финансовую сферу складывается из нескольких факторов, включая, в частности, следующие:

- мобильные контрафактные устройства ненадежны и представляют угрозу для здоровья человека и для окружающей среды из-за опасных компонентов (например, свинца или кадмия), которые имеют высокий удельный коэффициент поглощения (SAR), или использования в них взрывоопасных аккумуляторных батарей;
- снижение качества обслуживания (QoS), включая проблемы с голосовым управлением, разъединением вызовов, мобильностью (передача обслуживания) и снижение скорости;
- финансовые убытки производителей подлинных терминалов (снижение продаж, негативное влияние на ценовую составляющую);
- убытки в налогово-бюджетной сфере (таможенные сборы и налоги);
- нарушение авторских прав и товарных знаков, недобросовестная конкуренция;
- потеря гарантии и технической поддержки;
- нарушение работы сетей электросвязи, в частности вызванное невозможностью регулировки мощности.

Что касается вопроса работы сетей, как становится понятно из отчета Qualcomm¹⁰, контрафактное оборудование оказывает следующее пагубное воздействие на сети:

- снижение пропускной способности сети: объем передачи данных при использовании технологии долгосрочного развития (LTE) уменьшается на 23%, объем передачи данных при использовании высокоскоростного пакетного доступа (HSPA) уменьшается на 6%, пропускная способность передачи речи в рамках универсальной системы подвижной электросвязи (UMTS) уменьшается на 27%;
- сокращение возможностей поддержки новейших функций LTE, таких как LTE-CA (объединение несущих), MIMO (многоканальный вход и многоканальный выход) 4x4 и 256 QAM (квадратурная амплитудная модуляция), что отрицательно сказывается на качестве обслуживания пользователей;
- повышение требований к количеству узлов сети, что чревато капитальными и эксплуатационными расходами и оказывает негативное воздействие на экономические модели операторов подвижной связи.

К числу проблем, связанных с использованием контрафактных устройств с недействительными кодами IMEI, относятся:

- сложность выявления и блокировки контрафактных мобильных устройств, поскольку у многих из них есть коды IMEI, которые кажутся законными. Производители контрафактной продукции обычно используют в своих продуктах диапазоны номеров IMEI, которые соответствуют диапазонам производителей законных устройств, что затрудняет процесс разграничения законных и контрафактных продуктов;
- угрозы общественной безопасности: такие устройства потенциально могут способствовать преступной и террористической деятельности;
- вследствие нарушений связи из-за блокировки уже реализованных контрафактных устройств наказанию нередко подвергаются пользователи, а не торговцы поддельными продуктами.

3.2 Определения

- **Оконечное устройство** – оборудование, подключенное к сети электросвязи, для обеспечения доступа к одной или нескольким конкретным службам (Рекомендация МСЭ-R V.662-3)¹¹.
- **IMEI**: (Международный идентификационный код подвижного оборудования) – уникальный код, назначаемый производителем каждому мобильному терминалу IMT-2000 и используемый для определения терминала IMT-2000 сети для целей одобрения оконечного оборудования или аналогичных целей.

¹⁰ Qualcomm. [Противодействие контрафакту и хищению мобильных устройств](#), октябрь 2018 года.

¹¹ Сектор радиосвязи МСЭ (МСЭ-R). Рекомендация [МСЭ-R V.662-3 \(05/2000\)](#). Термины и определения.

- **EIR** (Регистр идентификаторов оборудования) – регистр, которому для целей записи ситуации может быть назначен идентификационный код оборудования пользователя. Вопрос характера, цели и применения этой информации требует дальнейшего изучения.
- **Белый список** – реестр устройств, разрешенных для использования в стране (включая устройства, легально импортированные или изготовленные в этой стране).
- **Черный список** – это реестр устройств, обслуживание которых в сети электросвязи должно быть запрещено.

3.3 Руководящие указания

Важно, чтобы все заинтересованные стороны (правительства, производители, операторы сетей и потребители) вели совместную работу по борьбе с распространением контрафактного оборудования электросвязи/ИКТ.

Рисунок 5: Ответственность за борьбу с контрафакцией



Сотрудничество играет важнейшую роль в создании нормативно-правовой и технической базы для борьбы с распространением контрафактных продуктов. С этой целью:

- Правительствам и регуляторным органам следует разрабатывать нормативно-правовые рамки, предусматривающие стандартные процедуры, а также внедрять технологические платформы для обеспечения соблюдения норм; организовывать кампании по повышению осведомленности, в частности об опасностях, которые контрафактные устройства представляют для пользователей, включая угрозу здоровью и плохое качество обслуживания; и содействовать осуществлению надзора за рынком в целях предотвращения торговли незаконными устройствами.
- Правительствам следует рассмотреть возможность снижения налогов и пошлин на законные импортные устройства ИКТ. Эта мера также может сократить стоимость владения.
- На национальном уровне регуляторным органам следует сотрудничать с производителями и операторами сетей в целях определения масштабов использования контрафактных устройств на местном рынке.
- Таможенным службам и службам безопасности следует предоставлять необходимые ресурсы для борьбы с незаконным оборотом и проверки законности идентификаторов устройств в пунктах импорта.
- Производители и импортеры должны регистрировать все импортируемое или изготовляемое в стране оборудование и соблюдать процедуры одобрения типа, установленные регуляторным органом.
- Производителям следует повышать безопасность кодов IMEI путем соблюдения принципов технического проектирования для моделей безопасности IMEI и участия в процессе Ассоциации GSM (GSMA) по представлению отчетов об уязвимостях в области безопасности IMEI и их устранению.
- Операторы могут вносить вклад в борьбу с распространением контрафакции путем предоставления сетевых данных устройств регуляторному органу и заинтересованным сторонам из государственного сектора; создания базы данных EIR для поддержки эффективного функционирования черных и белых списков IMEI в целях запрета доступа для контрафактных устройств; а также информирования абонентов о статусе их устройства с помощью SMS, если это необходимо.

- Потребители также могут вносить вклад, проверяя законность устройств, которые они планируют приобрести, с помощью услуг, которые предоставляют другие заинтересованные стороны; регистрируя устройства, импортированные в индивидуальном порядке; и информируя органы власти о контрафактных устройствах.
- Следует устанавливать режимы оценки соответствия, а также создавать централизованные национальные базы данных, содержащие полную информацию об устройствах (идентификаторы, технические спецификации, жизненный цикл устройства и т. д.) для содействия эффективному надзору за рынком.

Исходя из опыта таких стран, как Руанда (см. п. 3.4.4), на региональном уровне рекомендуется следующее:

- необходимо заключать межгосударственные соглашения о взаимном признании в целях осуществления оценки соответствия и надзора за рынком;
- создание централизованной системы контроля оборудования могло бы существенно снизить количество контрафактных и некачественных устройств, поступающих на рынок;
- создание уполномоченных региональных центров тестирования могло бы послужить существенным подспорьем в осуществлении оценки соответствия за счет сертификации и представления поставщиком декларации о соответствии требованиям.

3.4 Национальный опыт (исследование конкретных ситуаций)

Важнейшую роль в подготовке этого отчета сыграли вклады, представленные Государствами-Членами и заинтересованными сторонами. Вклады составлены на основе национального опыта, данных и существующей практики в области борьбы с распространением контрафактных устройств.

Авторы вкладов единогласно поддерживают необходимость создания обязательных к исполнению политических и нормативно-правовых рамок.

Некоторые авторы предлагают использовать существующие технические решения, такие как международные стандарты и методы надзора за рынком, а также создавать централизованные базы данных и платформы для блокировки контрафактных устройств.

Кроме того, в некоторых вкладах предлагается расширить усилия и вывести их на региональный и субрегиональный уровни для сопряжения различных методов борьбы с производством контрафактных устройств.

3.4.1 Мадагаскар

На Мадагаскаре 25% активных устройств в сетях подвижной связи являются контрафактными¹². Несмотря на то, что эти устройства обладают некоторыми преимуществами, такими как доступность в ценовом отношении, обеспечение доступа к универсальным услугам и сокращение цифрового разрыва, они несут в себе намного больше опасностей для здоровья человека (опасный уровень излучения), для операторов (качество обслуживания, помехи и т. д.) и для экономики страны в целом.

Для того чтобы развитие цифровых технологий не наносило ущерб здоровью и экономике, Мадагаскар принимает следующие меры:

- повышение информированности пользователей об опасности контрафактных устройств;
- закрытие черных рынков и обеспечение применения таможенных мер;
- запрещение контрафактных терминалов и сертификация импортируемого оборудования ИКТ;
- использование платформы для анализа и идентификации кодов IMEI и блокировки контрафактных устройств начиная с 30 июня 2019 года.

¹² Документ 2/45 ИК2 МСЭ-D, Мадагаскар.

3.4.2 Гвинея

В своем вкладе Правительство Гвинеи подчеркивает обеспокоенность по поводу сертификации оборудования и инфраструктуры электросвязи, а также функциональной совместимости услуг электросвязи¹³. В период после 2015 года в Гвинею были приняты законы об электросвязи, которые способствовали реструктуризации сектора. Эти реформы позволили добиться положительных изменений, таких как увеличение телефонного пула, повышение качества обслуживания, увеличение вклада сектора в ВВП, а также осуществление контроля над цифровым рынком и сектором сертификации.

Правительство установило очень строгие правила в отношении сертификации оборудования электросвязи, предусмотрев ответные меры и санкции в целях предупреждения нарушений. Регуляторный орган почты и электросвязи (ARPT) проводит оценку соответствия окончательного оборудования основным требованиям, запрашивая подробную административную и техническую документацию перед выдачей сертификатов соответствия. К числу принятых в Гвинею мер относятся следующие:

- тщательный и непрерывный мониторинг работы МСЭ в области стандартизации;
- деятельность, осуществляемая широким кругом заинтересованных сторон, включая ARPT, таможенные службы, налоговые органы и министерства;
- выдача сертификатов одобрения оборудования электросвязи на пятилетний срок с возможностью продления;
- внедрение системы маркировки одобренного оборудования;
- изъятие оборудования или ликвидация объектов, связанных с производством контрафактной продукции, за счет нарушителя;
- конфискация контрафактного оборудования по решению уполномоченного суда;
- наказание за непрохождение регистрации: любое лицо, которое имеет окончательное оборудование или радиооборудование в понимании, предусмотренном законом, в целях продажи или бесплатного распространения либо распространения за вознаграждение, осуществляет продажу такого оборудования или подключает его к общественной сети электросвязи/ИКТ в нарушение режима сертификации или в отсутствие предварительного одобрения, наказывается штрафом в размере от 10 млн до 200 млн гвинейских франков;
- в случае повторного нарушения наказание удваивается.

3.4.3 Сенегал

Помимо эффективной борьбы с пиратством, контрафактным производством и хищением устройств электросвязи/ИКТ, а также осуществления мер по адаптации к изменениям в правовой среде, Правительство Сенегала в сотрудничестве с континентальными и межконтинентальными сообществами, транснациональными корпорациями, регуляторными органами электросвязи и ИКТ и поставщиками услуг интернета (ПУИ) осуществляет важные инициативы в целях противодействия этому бедствию нашего времени, которое препятствует развитию технологических инноваций, созданию рабочих мест и материальных ценностей, а также поступлению прямых иностранных инвестиций¹⁴.

Сенегал осуществляет законодательные и регуляторные меры, а также иные шаги по улучшению защиты индивидуальной собственности, к числу которых относятся следующие:

- законодательная база на основе ряда законов;
- нормативно-правовая база на основе серии указов;
- национальная бригада по борьбе с пиратством и контрафакцией;
- Сенегальское агентство промышленной собственности и технологических инноваций;
- Регуляторный орган электросвязи и почты (ARTP);
- национальные таможенные органы;

¹³ Документ [SG2RGQ/9\(Rev.1\)](#) ИК2 МСЭ-D, Гвинея.

¹⁴ Документ [SG2RGQ/66\(Rev.1\)](#) ИК2 МСЭ-D, Сенегал (на французском языке).

- участие национальных и международных производителей и дистрибьюторов телефонов, планшетов, смартфонов и декодеров.

3.4.4 Руанда

Осознавая опасность контрафактных устройств для потребителей, отрасли и экономики в целом, Правительство Руанды разработало стратегию по борьбе с распространением контрафактных устройств и утвердило план действий на региональном уровне совместно с государствами – членами Восточноафриканского сообщества (ВАС)¹⁵. Правительство выдвинуло следующие предложения:

- Взаимные соглашения между государствами – членами ВАС: пересмотр нормативно-правовых документов государств-членов в целях заключения соглашений о взаимном признании для осуществления оценки соответствия и улучшения надзора за рынком.
- Централизованная система мониторинга: создание системы контроля в реальном времени на основе технологии EIR SIM Lock, предварительной авторизации IMEI, авторизации IMEI и оповещения EIR в качестве наиболее эффективного подхода к борьбе с распространением незаконных устройств на региональном уровне.
- Региональные центры тестирования: создание аккредитованных региональных центров тестирования упростит осуществление оценки соответствия в Государствах – Членах ВАС за счет сертификации и представления поставщиками декларации о соответствии. Это позволит сократить расходы региональных сборочных заводов на сертификацию и снизить итоговую стоимость продукции. Заключение взаимных соглашений между государствами будет способствовать созданию специализированных лабораторий в разных странах.

3.4.5 Зимбабве

Все операторы сетей подвижной связи в Зимбабве имеют возможность обнаруживать контрафактные устройства с дублированными IMEI и отключать их от своих сетей. Однако, поскольку большинство устройств, подключенных к сетям, являются контрафактными, они служат важным источником дохода для операторов и на практике их отключение происходит редко¹⁶. Тем не менее в целях борьбы с распространением контрафактного оборудования и хищением мобильных устройств в Зимбабве были приняты следующие меры:

- запрет использования любого устройства, не отвечающего требованиям одобренного типа;
- обязанность абонентов сети подвижной связи регистрировать вновь приобретенные SIM-карты у оператора сети подвижной связи (MNO) перед их активацией в сети;
- формирование базы данных регистрации абонентов для обеспечения надлежащей регистрации всех SIM-карт, активированных в стране, что также способствует обнаружению контрафактных устройств и поддельных мобильных телефонов;
- тестирование и сертификация всех новых устройств ИКТ на региональном уровне усилиями независимой лаборатории по тестированию под руководством Независимого управления связи Южно-Африканской Республики (ICASA).

3.4.6 Гана

Защита устройств электросвязи/ИКТ, пользователей и сетей в Гане обеспечивается с помощью одобрения типа¹⁷. Национальным управлением связи (NCA) был создан режим одобрения типа для сертификации и тестирования оборудования связи в целях обеспечения соблюдения международных стандартов:

- осуществление процедуры одобрения на основе технической документации, которая содержит отчеты о тестировании и требования соответствия, касающиеся защиты прав потребителя, охраны окружающей среды, перебоев в работе сетей, целостности и функциональной совместимости, а также положения об обеспечении соответствия Национальному плану распределения частот;

¹⁵ Документ [SG2RGQ/69](#) ИК2 МСЭ-D, Руанда.

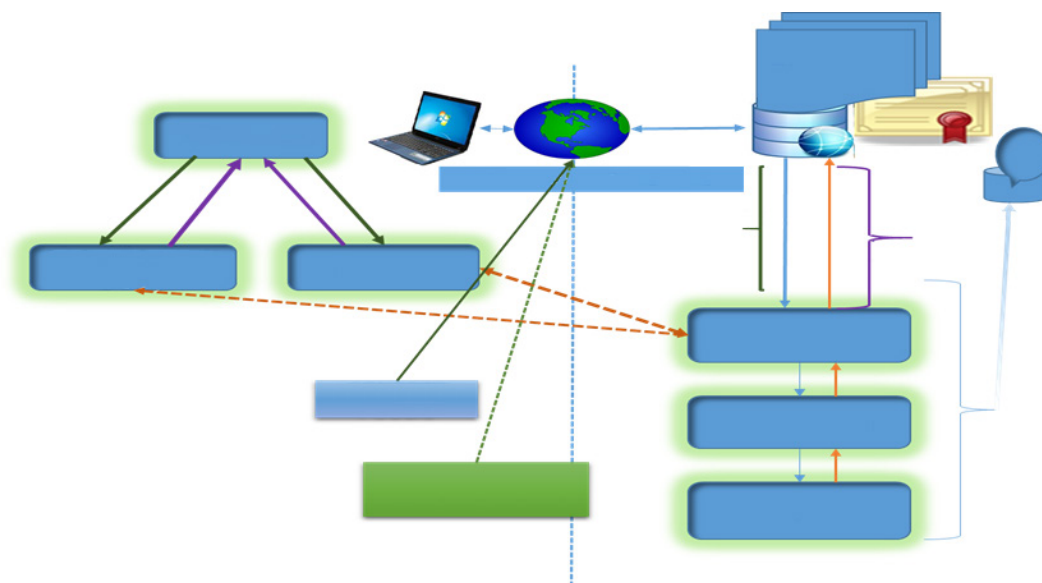
¹⁶ Документ [SG2RGQ/85](#) ИК2 МСЭ-D, Зимбабве.

¹⁷ Документ [SG2RGQ/82](#) ИК2 МСЭ-D, Гана.

Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость, а также в борьбе с использованием контрафактного оборудования информационно-коммуникационных технологий и хищением мобильных устройств

- присвоение сертификата одобрения типа (TAC) и маркировки NCA вместе с публикацией на веб-сайте NCA подробной информации об оборудовании;
- внедрение системы лицензирования дилеров, интегрированной в режим одобрения, в целях упорядочения деятельности продавцов электроники и оборудования связи, а также гарантии использования только одобренных устройств ИКТ;
- мероприятия по укреплению надзора за национальным рынком;
- развертывание лабораторий по тестированию для осуществления измерений, связанных с удельным коэффициентом поглощения (SAR), электромагнитным полем (ЭМП), цифровым наземным телевидением (ЦНТ), радиочастотами и сигнализацией (RF&Sig).

Рисунок 6: Процесс одобрения типа

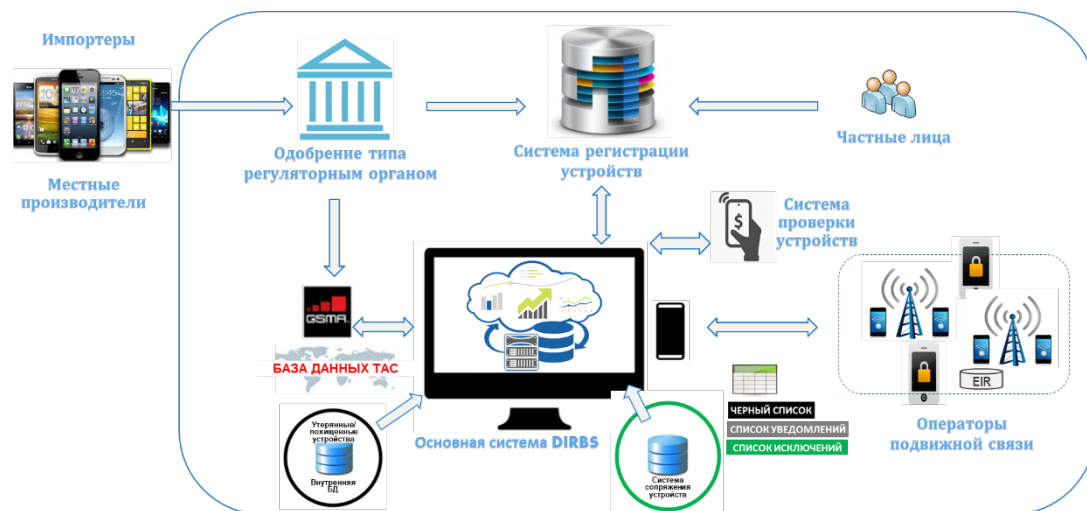


3.4.7 Пакистан

Управление электросвязи Пакистана (PTA) в сотрудничестве с Qualcomm внедрило технологическую платформу с открытым исходным кодом под названием "Система идентификации, регистрации и блокировки устройств" (DIRBS), чтобы обеспечить функционирование в сетях подвижной связи страны только утвержденных и законных устройств¹⁸. DIRBS позволяет идентифицировать все устройства; содержит установленную базу устройств; отслеживает все случаи активации новых устройств; фиксирует незаконные и контрафактные устройства, включая случаи кражи мобильных телефонов; а также допускает исключения/амнистию.

¹⁸ Более подробная информация о DIRBS представлена на веб-сайтах [Управления электросвязи Пакистана \(PTA\)](#) и [Федерального совета по доходам Пакистана](#).

Рисунок 7: Система идентификации, регистрации и блокировки устройств (DIRBS)



3.4.8 Ассоциация GSM

Ассоциация GSM (GSMA) обеспечивает работу "Международной базы данных идентификаторов мобильных устройств", которая является глобальной централизованной базой данных, содержащей основную информацию о серийных номерах (IMEI) миллионов мобильных устройств¹⁹.

GSMA предоставляет услугу "проверки устройств" продавцам, перерабатывающим предприятиям, страховщикам и правоохранительным органам (на некоторых рынках доступ к этой услуге также может предоставляться напрямую потребителям). Это позволяет пользователям моментально получать информацию о том, не заявлено ли то или иное устройство как утерянное или похищенное, на основе записи о его статусе согласно данным, предоставляемым GSMA ее членами из числа операторов сетей подвижной связи со всего мира.

GSMA стремится подключить к базе данных IMEI как можно больше MNO.

В сентябре 2016 года Ассоциация GSM и Всемирная таможенная организация (ВТамО) заключили партнерское соглашение по борьбе с контрафакцией и мошеннической торговлей мобильными устройствами. Интеграция базы данных IMEI позволит осуществлять перекрестную проверку и отфильтровывать контрафактные устройства, выявленные по их IMEI в пункте импорта.

3.4.9 Бразилия

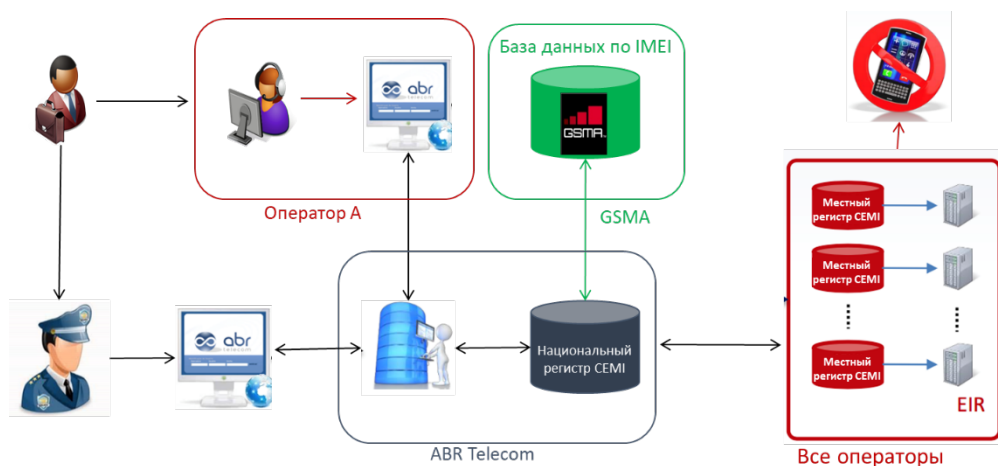
Для борьбы с использованием похищенных, поддельных и несертифицированных уникальных идентификаторов Правительство Бразилии запустило инициативу под названием "Celular Legal" с участием всех заинтересованных сторон при координирующей роли Национального агентства электросвязи (ANATEL)²⁰. Меры, осуществляемые в рамках этой инициативы, организованы вокруг двух модулей:

- Модуль СЕMI (Регистр заблокированных мобильных устройств) позволяет операторам подвижной связи и полиции блокировать похищенные устройства по просьбе пользователя.

¹⁹ Документ [SG2RGQ/80](#) ИК2 МСЭ-D, Ассоциация GSM.

²⁰ Жуан. Занон, "Борьба с использованием похищенных и контрафактных устройств ИКТ", семинар-практикум МСЭ-D по борьбе с контрафактными устройствами ИКТ, Женева, 4 октября 2018 года.

Рисунок 8: Схема работы CEMI



- Модуль SIGA (*Интегрированная система управления устройствами*) используется для выявления и блокировки устройств, связанных с другими видами мошенничества: подделкой, клонированием, использованием несертифицированных устройств, незаконных уникальных идентификаторов и т. д. Инициатива "Cellular Legal" включает в себя онлайн-инструмент, который позволяет проверить статус устройства по его коду IMEI²¹.

3.4.10 Оман

Почти два миллиона из всех мобильных устройств, зарегистрированных в национальной сети Омана, имеют недействительный код IMEI. Некоторые номера IMEI повторяются до 10 раз, поскольку существует более 10 устройств с одинаковым номером IMEI²². Это создает техническую проблему для регистрации этих устройств в местных сетях и повышает финансовую нагрузку на потребителей в целом, подрывая их доверие к этим продуктам.

Регуляторные органы заинтересованы в обеспечении того, чтобы все готовые устройства ИКТ, поставляемые дилерами или импортерами, полностью соответствовали постановлениям и решениям, принимаемым регуляторным органом в этом отношении. В этих целях контрольное подразделение Регуляторного органа электросвязи (TRA) следит за обеспечением совместимости и соблюдением применимых стандартов и технических спецификаций оборудования ИКТ, которое продается на национальном рынке.

TRA в сотрудничестве с местными операторами создал линию помощи для клиентов, чтобы они могли проверить коды IMEI. И все же организация сталкивается с трудностями, такими как отсутствие доступа к международной базе данных кодов IMEI, поскольку GSMA предоставляет полный доступ к своей базе данных только производителям и операторам в соответствующей стране, но не регуляторным органам.

3.4.11 Международные стандарты и рекомендации

- [ISO 12931:2012](#): Критерии эффективности для идентификационных растворов, используемых для борьбы с подделками материальных изделий;
- [ISO 16678:2014](#): Руководящие указания по идентификации функционально совместимых объектов и соответствующим системам аутентификации для ограничения контрафакции и незаконной торговли;
- [МСЭ-T Q.5050 \(03/2019\)](#): Борьба с контрафакцией и использованием похищенных устройств ИКТ;
- [МСЭ-T Y.4808 \(08/2020\)](#): Базовая архитектура цифрового объекта для борьбы с контрафакцией в IoT.

²¹ Agência Nacional de Telecomunicações (ANATEL). [Cellular Legal](#).

²² Документ [2/326](#) ИК2 МСЭ-D, Оман.

Глава 4 – Хищение мобильных устройств

4.1 Введение

Рост использования мобильных устройств во всем мире сопровождается увеличением масштабов распространения похищенных устройств как внутри стран, так и за их пределами. Для того чтобы не допускать подключения похищенных устройств к сетям в различных странах мира, необходимы инициативы глобального масштаба.

Масштабы ущерба, причиняемого всей экосистеме в результате использования незаконных устройств, заставили правительства и отрасли уделять все больше внимания поиску решений. Правительства внедряют нормы, регулирующие широкий круг вопросов, включая:

- хищение мобильных устройств;
- риски в области безопасности;
- потери доходов от сбора налогов;
- конфиденциальность потребителей;
- качество работы сетей;
- права интеллектуальной собственности.

В течение многих лет GSMA играет ведущую роль в отраслевых инициативах, связанных с обменом данными в целях блокирования доступа похищенных или утерянных мобильных устройств к сетям во всем мире. Используя уникальный код IMEI, GSMA поддерживает черный список вызывающих подозрение устройств (т. е. устройств, объявленных утерянными или похищенными), доступ к которому предоставляется операторам по всему миру²³.

4.2 Проблемы и задачи

Хищение устройств является проблемой глобального масштаба, которая требует согласования усилий и взаимодействия между государствами с целью сделать этот вид преступлений экономически непривлекательным. Несмотря на то, что отраслевые инициативы приносят положительные результаты, необходимы дополнительные усилия, поскольку до сегодняшнего дня большинство мероприятий основывались на глобальных общедоступных стандартах и некоторым странам еще предстоит согласовать свои усилия с глобальной отраслевой практикой. В связи с этим страны нуждаются в выработке единого подхода для обеспечения согласованности с усилиями отрасли на глобальной основе. Бездействие подрывает эффективность некоторых принятых мер.

Необходимые условия для решения проблемы хищения устройств можно разделить на следующие категории.

Нормативные положения и обеспечение их выполнения

- разработка нормативно-правовой базы;
- внедрение стандартных рабочих процедур;
- развертывание и администрирование технологических платформ для обеспечения выполнения норм;
- проведение кампаний по повышению осведомленности.

Техническая платформа

- классификация существующих устройств:
 - анализ данных об устройстве на основе сетевой информации;

²³ Документ [SG2RGQ/80](#) ИК2 МСЭ-D, Ассоциация GSM.

- классификация устройств по IMEI (действительные/недействительные, уникальные/дублированные),
- разрешение использования существующих устройств:
 - привязка существующих поддельных кодов IMEI к кодам международного идентификатора абонента подвижной связи (IMSI) и международному справочному номеру абонентской станции подвижной связи (MSISDN),
- регистрация новых устройств:
 - требование одобрения типа с уникальными идентификаторами устройств;
 - регистрация импортируемых и изготавливаемых в стране устройств только при наличии действующих и уникальных идентификаторов,
- выявление фальсификации кодов IMEI:
 - анализ данных сети;
 - выявление устройств с поддельными кодами IMEI,
- обеспечение возможности блокировки сети:
 - отслеживание доступа не соответствующих требованиям/незарегистрированных устройств с помощью управления сетью.

Внедрение технических систем²⁴

- удобство для всех заинтересованных сторон, особенно потребителей;
- создание автономной системы, избавляющей от необходимости интеграции сетей подвижной связи и обеспечения их функциональной совместимости, которые влекут за собой ненужные расходы, ограничение пропускной способности и нагрузку на операторов с точки зрения ресурсов;
- отсутствие требования строгой привязки устройства и клиента;
- гибкость/конфигурируемость для адаптации к национальным нормам без необходимости индивидуальной настройки.

4.2.1 Преступные и мошеннические действия, связанные с устройствами

Преступные и мошеннические действия, связанные с устройствами, имеют негативные последствия для различных групп заинтересованных сторон:

- потребителей: опасность причинения вреда в результате хищения, материальный ущерб, утрата личной информации;
- правительств: рост преступности, снижение налоговых поступлений;
- торговых предприятий: непреднамеренное приобретение похищенных товаров, проблемы функционирования сети;
- страховых организаций: повышение страховых тарифов, передача прав собственности на похищенные товары;
- операторов: отток абонентов, потеря субсидий, затраты на страхование;
- правоохранительных органов: организованная преступность, истощение ресурсов.

4.2.2 Задачи и ответственность заинтересованных сторон

Различные заинтересованные стороны могут играть важную роль в борьбе с хищением устройств.

²⁴ Мохаммад Рахиль Камаль. [CEIR с открытым кодом для борьбы с контрафактом и похищенными устройствами ИКТ. Третий региональный семинар-практикум 11-й Исследовательской комиссии МСЭ-Т для Африки по теме "Проблемы контрафактных устройств ИКТ, проверки на соответствие и функциональную совместимость в Африке"](#), Тунис, 30 сентября 2019 года.

Правительства могут разрабатывать нормативно-правовые рамки, вводить стандартные рабочие процедуры, внедрять технологические платформы для обеспечения соблюдения норм и обеспечивать их работу, а также проводить кампании по повышению осведомленности.

Производители/импортеры могут получать одобрение типа устройства от правительства/регуляторного органа, регистрировать импортируемые устройства, а также все устройства, произведенные в стране.

Операторы могут предоставлять правительству связанные с устройствами данные сети, обеспечивать поддержку регистра идентификации оборудования (EIR), вести черные списки действительных/недействительных кодов IMEI, допуская исключения, а также в случае необходимости уведомлять абонентов о статусе их устройств с помощью SMS.

Потребители могут проверять статус своих устройств (с помощью SMS, приложений или веб-сайтов), регистрировать устройства, импортированные в индивидуальном порядке, сообщать о хищении устройств органам власти и предоставлять доказательства (кассовые чеки) подлинности устройств, если это необходимо.

4.2.3 Важнейшие инструменты борьбы с хищением устройств

Для борьбы с хищением устройств могут приниматься различные меры как на уровне сетей, так и на уровне устройств.

Защита на уровне устройств:

- возможность удаления контактов и фотографий, а также блокировки мобильных платежей;
- возможность сброса параметров до заводских настроек для удаления всех данных;
- функция удаленной очистки.

Защита на уровне сетей:

- блокирование доступа похищенных телефонов к сети.

Проверка статуса устройства:

- проверка статуса устройства перед переработкой;
- создание условий, при которых хищение телефонов будет невыгодным.

4.3 Руководящие указания

Участие многих заинтересованных сторон

Пользователи могут сообщать о хищении устройств оператору сети и активировать функции защиты от кражи на своих устройствах, а в тех странах, где операторы имеют доступ к черному списку GSMA IMEI, можно призывать пользователей проверять статус IMEI подержанного устройства, которое они планируют приобрести²⁵.

Операторы сетей подвижной связи могут блокировать использование похищенных устройств в своих сетях и подключаться к черному списку GSMA IMEI для передачи и получения соответствующей информации, а также призывать поставщиков устройств обеспечивать надлежащую защиту целостности IMEI в их продукции.

Производители устройств/владельцы товарных знаков могут обеспечивать целостность кодов IMEI во всех своих продуктах, разрабатывать более надежные устройства (т. е. делать невозможным перепрограммирование кодов IMEI) и внедрять функцию блокировки, чтобы пользователи могли отключить похищенное или утерянное устройство в удаленном режиме.

²⁵ Джеймс Морган (GSMA). [Совместное противодействие преступным действиям, связанным с устройствами – передовой опыт в борьбе с похищением мобильных устройств](#). Семинар-практикум МСЭ по глобальным подходам к борьбе с контрафакцией и использованием похищенных устройств ИКТ, Женева, 23 июля 2018 года.

Операторы магазинов приложений могут получать от GSMA коды IMEI похищенных устройств и использовать их для того, чтобы закрывать доступ к своим магазинам для устройств, заявленных как похищенные.

Все заинтересованные стороны (правительства, производители, операторы сетей и потребители) должны вести совместную работу по борьбе с хищением мобильных устройств, в частности путем:

- привлечения правоохранительных органов и взаимодействия с ними;
- осуществления надзора за каналами распространения для пресечения торговли похищенными устройствами;
- законодательной и судебной поддержки инициатив по защите от краж;
- уделения первоочередного внимания устройствам, минимизации неудобств для пользователей;
- уделения большего внимания коллективным усилиям при активной роли всех государств;
- осуществления мер по поддержке существующих возможностей вместо их дублирования/ослабления;
- оценки результатов и представления отчетности об эффективности избранных подходов;
- анализа проделанной работы с целью определить, какая деятельность является эффективной, а какая нет;
- внедрения появляющихся технологий и решений для устранения разрывов.

Правительства и регуляторные органы должны вести совместную работу, чтобы обеспечить:

- внедрение операторами регистров EIR для блокировки использования похищенных устройств в местных сетях;
- следование руководящим указаниям на основе примеров передового опыта для блокировки устройств и обмена данными;
- подключение EIR операторов к базе данных IMEI для возможности международной блокировки;
- повышение уровня безопасности IMEI, информирование о проблемах и их устранение;
- проверку кодов IMEI сотрудниками правоохранительных органов, таможенными служащими, предприятиями розничной торговли и потребителями;
- принятие принудительных мер в отношении преступников (подделка IMEI, хищение и торговля);
- принятие мер по информированию пользователей и продвижению возможностей блокировки устройств;
- согласование измеряемых показателей для отслеживания прогресса по итогам этих усилий и ведение отчетности.

4.4 Национальный опыт (исследование конкретных ситуаций)

4.4.1 Центральноафриканская Республика

В рамках политики по развитию инфраструктуры ИКТ Правительство Центральноафриканской Республики открыло рынок ИКТ для четырех операторов подвижной связи и одного оператора фиксированной связи для обеспечения максимального покрытия территории страны и предоставления качественных услуг населению²⁶.

Просчеты Регуляторного органа электронных средств связи и почты (ARCEP) в осуществлении этой политики привели к нерегулируемому развитию инфраструктуры, возникновению сложностей с проверкой соответствия и функциональной совместимости оборудования ИКТ, а также росту контрафакции и хищения мобильных терминалов. Это сказалось на инвестициях и доходах отрасли.

²⁶ Документ [SG2RGQ/144](#) ИК2 МСЭ-D, Центральноафриканская Республика.

Для решения этих проблем Правительство Центральноафриканской Республики:

- приняло и ввело в действие Закон об электронной связи с соответствующими подзаконными актами;
- приняло и ввело в действие закон об учреждении Регуляторного органа электронных средств связи и почты (ARCEP);
- подготовило законопроект о киберпреступности и кибербезопасности;
- создало центр по противодействию незаконной торговле мобильными терминалами, определению их местонахождения и борьбе с мошенничеством;
- учредило Постоянный секретариат по управлению электронными средствами связи для обеспечения технологического мониторинга;
- завершило проект по развертыванию международной оптоволоконной магистральной инфраструктуры, соединяющей столицу ЦАР Банги с Республикой Конго и Камеруном;
- осуществило национальный проект цифровизации "Цифровая ЦАР – 2025";
- реализовало национальный стратегический план по развитию сверхвысокоскоростной широкополосной инфраструктуры;
- создало национальное агентство ИКТ и национальный центр обработки данных.

Центральноафриканская Республика рекомендует МСЭ оказывать содействие и поддержку странам в создании потенциала в области программ по соответствию и функциональной совместимости, а также в решении проблем, связанных с контрафактной продукцией и хищением мобильного оборудования.

4.4.2 Мексика

В целях борьбы с хищением оконечного оборудования подвижной связи Федеральный институт электросвязи (IFT), который является национальным регуляторным органом Мексики по вопросам электросвязи и радиовещания, установил регуляторные обязательства. Было запущено несколько инициатив по контролю за кодами IMEI на национальном и международном уровнях²⁷.

На международном уровне Правительство Мексики заключило двусторонние и региональные соглашения по линии министерств и департаментов в целях обмена информацией о кодах IMEI похищенных или утерянных устройств, а также запрещения их использования. Было заключено соглашение с GSMA в целях внедрения системы проверки устройств по IMEI, которая позволяет пользователям мобильных устройств осуществлять проверку номеров IMEI в базе данных GSMA в режиме реального времени.

Что касается усилий на национальном уровне, то IFT опубликовал в Официальном журнале техническое положение (IFT-011-2017) с руководящими указаниями по сотрудничеству в вопросах безопасности и правосудия, касающихся приостановки обслуживания мобильных терминалов или устройств, заявленных как похищенные или утерянные. Для укрепления этого сотрудничества IFT предусмотрел технические положения, включая спецификации для мобильных терминалов, подключенных к сетям электросвязи, а также контроль за их соблюдением:

- оценка соответствия;
- обновление сертификатов соответствия;
- база данных кодов IMEI одобренных устройств;
- контроль за соблюдением требований сертификации.

IFT осуществляет проверку соблюдения требований, предусмотренных в вышеупомянутом техническом положении, с помощью описанных в нем методов тестирования.

²⁷ Документ [2/166](#) ИК2 МСЭ-D, Мексика.

4.4.3 Научно-технологический университет Ирана

В целях предотвращения мошенничества и борьбы с продажей и использованием незаконных устройств, включая похищенные телефоны и телефоны, которые были ввезены без уплаты таможенных сборов, в 2017 году Исламская Республика Иран разработала план регистрации мобильных телефонов²⁸.

При включении устройства для доступа к сети производится его оценка: если информация об этом устройстве отсутствует в списке законных устройств, то оно будет определено как незаконное и добавлено в черный список.

В рамках всеобъемлющей торговой системы Исламской Республики Иран импортируемые телефоны регистрируются на таможенной границе и каждому устройству присваивается уникальный код активации. Научно-технологический университет Ирана разработал систему НАМТА – онлайн-базу данных, которая позволяет активировать устройство с помощью уникального кода и предоставляет пользователям две основные возможности:

- информирование о статусе активных мобильных телефонов на территории страны, подтверждение подлинности мобильного телефона и проверка законности и активации устройства;
- активация новых и законно импортированных телефонов.

Данные системы НАМТА о зарегистрированном оборудовании передаются Регуляторному органу связи Исламской Республики Иран и операторам подвижной связи. Только зарегистрированные устройства, подлинность которых подтверждена системой НАМТА, считаются законными и могут получать доступ к услугам, предоставляемым операторами; все остальные устройства попадают в черный список.

²⁸ Документ [2/83](#) ИК2 МСЭ-D, Исламская Республика Иран.

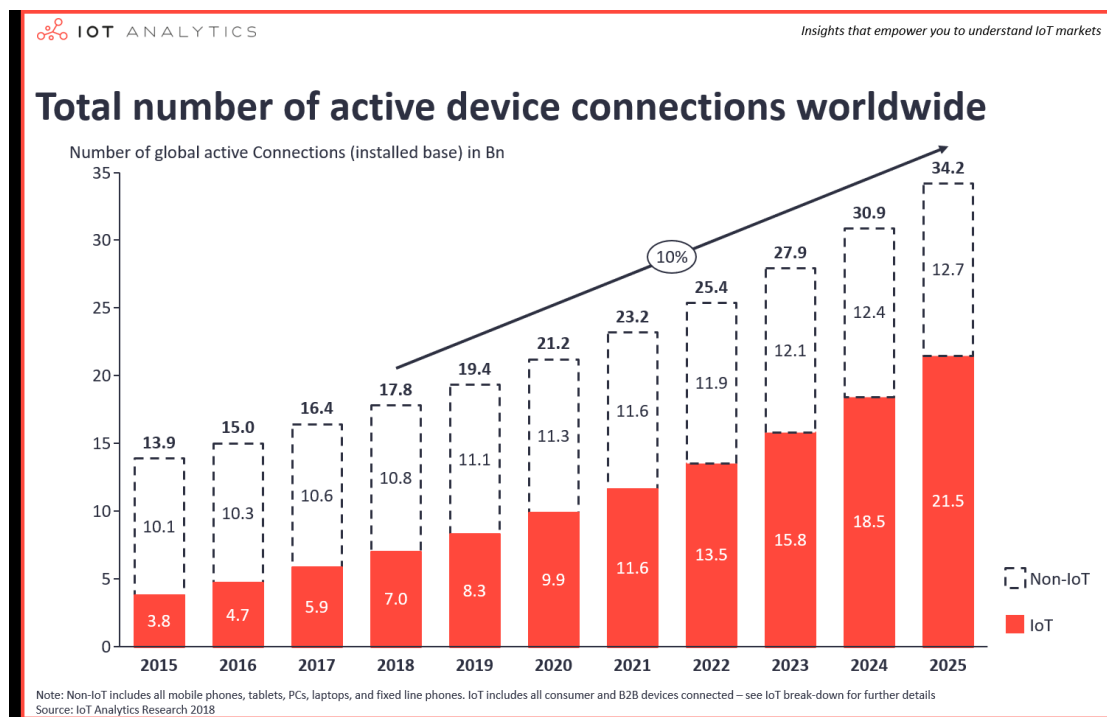
Глава 5 – Интернет вещей и C&I

5.1 Введение

МСЭ определяет интернет вещей (IoT) как "глобальную инфраструктуру для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий"^{29, 30}.

Технологии IoT применяются в различных отраслях и оказывают влияние на повседневную жизнь людей через платформы, осуществляющие обработку данных, генерируемых миллиардами подключенных устройств. Согласно исследованию, проведенному компанией IoT Analytics, ожидается резкий рост общемирового числа активных подключенных устройств. По состоянию на 2020 год из 21,2 млрд. активных подключений устройств в мире 9,9 млрд. приходилось на соединения IoT. К 2025 году эта цифра может вырасти до 21,5 млрд.³¹.

Рисунок 9: Число активных подключенных устройств в мире



5.2 Влияние IoT на C&I и разработку ИКТ

Для удовлетворения особых потребностей IoT, которые связаны с качеством, надежностью, покрытием и низким уровнем энергопотребления, необходимо решить ряд вопросов и проблем.

5.2.1 Задачи в области IoT

Наличия качественных датчиков сбора данных недостаточно; необходимо также обеспечить устойчивое подключение для передачи данных и предоставить платформу для их анализа и обработки.

Среди множества задач, связанных с IoT, наибольшего внимания заслуживают следующие.

²⁹ Рекомендация МСЭ-Т Y.2060 (06/2012), "Обзор интернета вещей".








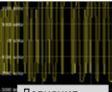

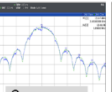
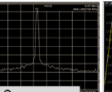
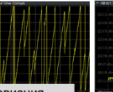
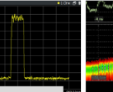

³⁰ Рекомендация МСЭ-Т Y.2069 (07/2012), "Термины и определения для интернета вещей".

³¹ IoT Analytics, "IoT по состоянию на 2018 год: Ускорение развития рынка – количество устройств IoT составляет 7 млрд.", август 2018 года.

Выбор технологии: залог успеха IoT

В будущем для приложений IoT, требующих полного покрытия и мобильности, будут преимущественно использоваться технологии сотовой связи, такие как технологии LTE-M и NB-IoT, работающие на базе 4G и 5G. Другие, в частности Sigfox или LoRaWAN, будут функционировать на основе энергосберегающих технологий, работающих в нелицензируемых полосах частот. Для большинства приложений будут использоваться беспроводные технологии малого и среднего радиуса действия, такие как Bluetooth®, WLAN/Wi-Fi и Zigbee. Беспроводные технологии, используемые для IoT, представлены на **Рисунке 10**³².

Рисунок 10: Беспроводные технологии, используемые для IoT

	 Bluetooth [®] Low Energy	 Wi-Fi ax	 ZigBee [®] 4THREAD	 sigfox	 LoRaWAN [™]	 NB-IoT	 LTE-M
Метод	FHSS	OFDMA	DSSS	UNB	CSS	OFDMA	OFDMA
Модуляция	GFSK	BPSK QPSK	O-QPSK	UL: DBPSK DL: GFSK	лчм	BPSK QPSK	QPSK 16QAM
Полоса пропускания	2 МГц	20 ... 160 МГц	2 МГц	100 Гц (ЕТСИ) 600 Гц (ФКС)	125, 250, 500 кГц	3,75; 15 кГц 180 кГц	1,4 МГц (M1) 5 МГц (M2)
Спектр	2,4 ГГц ISM	1.. 6 ГГц ISM	2,4 ГГц ISM	Ниже ГГц ISM	Ниже ГГц ISM	< 6 ГГц 3GPP	< 6 ГГц 3GPP
Характеристики							
	Девияция частоты	Спектр	Спектр	Спектр	Девияция частоты	Спектр	Спектр

Проектные решения, удовлетворяющие потребностям IoT, связанным с качеством, надежностью, расширенным покрытием, временем задержки и т. д.

Проектные решения должны также соответствовать ожиданиям пользователей, особенно в области конфиденциальности и защиты персональных данных, и способствовать формированию доверия за счет использования стандартов безопасности в экосистемах IoT.

Необходимость сертификации платформ и устройств IoT

Платформы и устройства должны проходить сертификацию на основе оценки их соответствия международным стандартам и регламентам.

5.2.2 Сложности в сфере IoT

Основными элементами IoT являются объект (датчик), сеть (подключение), данные и обслуживающие приложения. В связи с этим возникают следующие сложности:

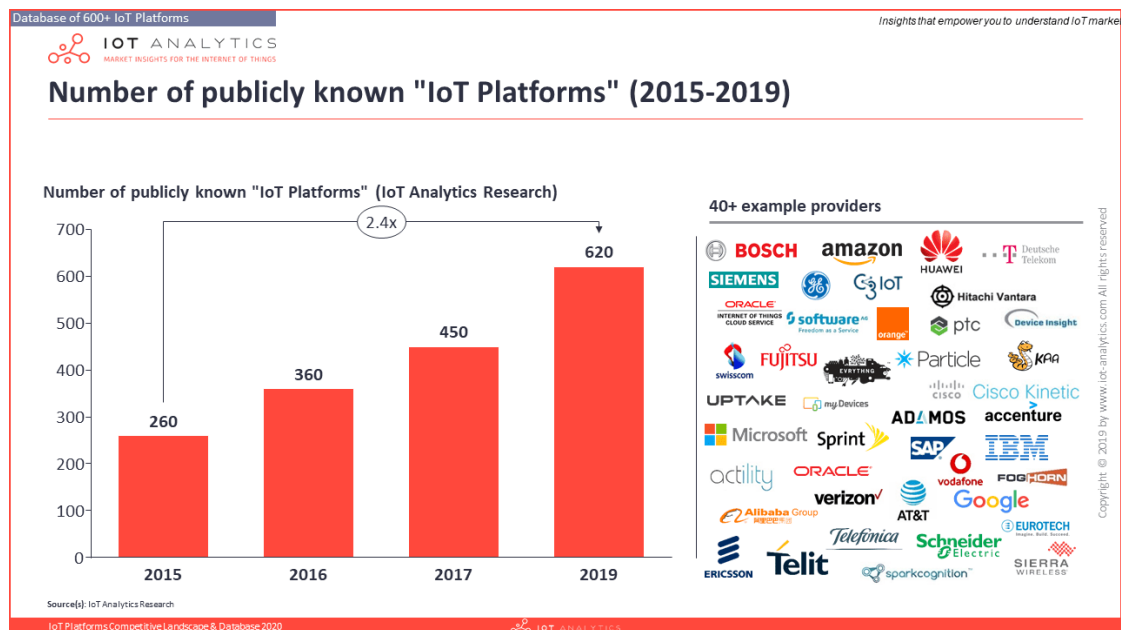
- **Многочисленные платформы IoT**: согласно статистике, ведущейся IoT Analytics, в 2019 году насчитывалось 620 платформ IoT и более 40 поставщиков (см. **Рисунок 11**)³³.

³² Йорг Кепп (Rohde & Schwarz, Германия) "Обеспечение безопасной и надежной связи в гиперсоединенном мире", сессия по Вопросу 4/2 МСЭ-D на тему "Соответствие и функциональная совместимость ИКТ: проблемы развивающихся стран", октябрь 2019 года.

³³ IoT Analytics, "IoT Platform Companies Landscape 2019/2020: 620 IoT Platforms globally", декабрь 2019 года.

Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость, а также в борьбе с использованием контрафактного оборудования информационно-коммуникационных технологий и хищением мобильных устройств

Рисунок 11: Число общеизвестных платформ IoT



- **Многочисленные протоколы IoT:** существует множество протоколов обмена данными, которые зависят от организаций по разработке стандартов (ОПС) и производителей продуктов IoT. У каждого стандарта IoT своя нормативная база, и специалистам в области ИТ приходится самим выбирать из многообразия имеющихся вариантов (см. **Рисунок 12**)³⁴.

Рисунок 12: Схематический обзор альянсов и организаций по разработке стандартов в области IoT (в вертикальной и горизонтальной плоскостях)



Источник: PG-3 Альянса для инноваций в IoT (AIOI) – Публикация 2.9

В настоящее время сфера IoT стандартизирована крайне слабо и в ней существует целое множество несовместимых стандартов и решений³⁵. Ввиду увеличения числа платформ и протоколов IoT, обеспечивающих связь между объектами, технические стандарты IoT разрабатываются в различных контекстах на основе разных приложений и с участием разных заинтересованных сторон с несопадающими задачами и потребностями. В связи с этим главная задача заключается в обеспечении функциональной

³⁴ Альянс по интернету вещей (AIOI), "IoT LSP Standard Framework Concepts", выпуск 2.9, 2019 год.

³⁵ Документ МСЭ-T SG20-TD1722 Вебинар "Ускорение преобразования городов с помощью стандартов", 25 июня 2020 года.

Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость, а также в борьбе с использованием контрафактного оборудования информационно-коммуникационных технологий и хищением мобильных устройств

совместимости, масштабируемости, наличия четких международных стандартов и сквозной безопасности (см. **Рисунок 13**).

Рисунок 13: Необходимость адаптированных схем сертификации



5.2.3 Пример: Тестирование IoT, применяемое в Rohde & Schwarz

Для обеспечения надлежащих показателей работы и соответствия регуляторным положениям в Rohde & Schwarz используются эфирные (OTA) измерения. Тестирование предполагает испытания в отношении показателей работы, сосуществования, помех и электромагнитных помех (EMI), а также измерение уровней побочных излучений (RSE) в полосе и вне полосы (см. **Рисунок 14**)³⁶.

Рисунок 14: Измерения OTA



5.2.4 Организации по разработке стандартов

Принятие единого подхода к системам IoT как к инструменту поддержки развития отрасли подтолкнуло OPC к тому, чтобы начать работу над созданием стандартной архитектуры, обеспечивающей функциональную совместимость систем, приложений, устройств и датчиков.

Международный союз электросвязи

МСЭ-Т занимается разработкой Рекомендаций серии Y, касающихся глобальной информационной инфраструктуры, аспектов межсетевых протоколов, сетей последующих поколений, интернета вещей и "умных" городов. 20-я Исследовательская комиссия (ИК20) ведет работу над международными стандартами, призванными содействовать функциональной совместимости между цифровыми инфраструктурами и приложениями IoT.

³⁶ Йорг Кенп (Rohde & Schwarz). Там же.

В марте 2020 года МСЭ опубликовал Рекомендацию МСЭ-Т Y.4459³⁷, в которой представлена архитектура цифрового объекта. Она определяет минимальный набор архитектурных компонентов и услуг, необходимых для обеспечения общей функциональной совместимости информации и услуг. Этот набор будет содействовать функциональной совместимости в части идентификации, описания, представления, доступа, хранения и безопасности устройств IoT. Данная базовая архитектура способствует использованию общего интерфейса безопасности и управления в различных приложениях IoT.

Что касается проверки на C&I, 11-я Исследовательская комиссия (ИК11) МСЭ-Т и Руководящий комитет по оценке соответствия ведут совместную работу с ИК20 над модельной сетью для тестирования IoT³⁸.

Международная организация по стандартизации и Международная электротехническая комиссия

В 2018 году Международная организация по стандартизации (ИСО) совместно с Международной электротехнической комиссией (МЭК) опубликовали стандарт ISO/IEC 30141, представляющий собой унифицирующий стандарт эталонной архитектуры для интернета вещей, который охарактеризован в нем как "сложная совокупность миллиардов 'умных' устройств, подключенных с помощью интернета"³⁹.

В 2019 году ИСО и МЭК опубликовали стандарт ISO/IEC 21823-1⁴⁰, в котором представлен обзор аспектов функциональной совместимости применительно к системам IoT.

Институт инженеров по электротехнике и радиоэлектронике

Институтом инженеров по электротехнике и радиоэлектронике (IEEE) был опубликован стандарт 2413-2019 – "Стандарт IEEE по архитектурной основе для интернета вещей (IoT)"⁴¹. В стандарте P2413.1 представлена архитектурная концепция создания "умных" городов на основе преимуществ межотраслевого взаимодействия и функциональной совместимости между различными компонентами и сферами "умного" города⁴². Этот стандарт разработан с опорой на архитектурную основу IoT, описанную в проекте стандарта IEEE P2413, который, в свою очередь, основан на международном стандарте ISO/IEC/IEEE 42010.

5.3 Регулирование и политика в области IoT и ИКТ

Регуляторные органы должны иметь представление о влиянии C&I на IoT. Несмотря на то, что лаборатории по тестированию вносят свой вклад в обеспечение надлежащего функционирования, соответствия и функциональной совместимости продуктов, регуляторные органы также должны быть вовлечены.

Сегодня развертывание технологий IoT осуществляется как государственными, так и частными организациями в различных секторах, включая здравоохранение, электросвязь, образование, сельское хозяйство, финансы и СМИ, а также "умные" города. В связи с этим исключительно важным является создание межсекторальной регуляторной среды, адаптированной для IoT, для чего требуется регулирование пятого поколения (к примеру, совместное регулирование).

5.3.1 Обзор совместного регулирования

Регулирование с первого по четвертое поколение уже претерпело существенные изменения: сперва на смену регулируемым монополиям пришли базовые реформы и либерализация рынка, а затем последовало регулирование среды, содействующее инновациям и доступу, сменившееся четвертым поколением интегрированного регулирования, в рамках которого первоочередное внимание уделяется вопросам, связанным с интернетом (см. **Рисунок 15**)⁴³.

³⁷ Рекомендация [МСЭ-Т Y.4459 \(12/2020\)](#) "Базовая архитектура цифрового объекта для обеспечения функциональной совместимости интернета вещей", март 2020 года.

³⁸ Кофи Нтим Йебоа-Кордие (Гана) "[Обзор работы и деятельность ИК11 МСЭ-Т](#)", семинар-практикум по Вопросу 4/2 МСЭ-D на тему "Соответствие и функциональная совместимость ИКТ: проблемы развивающихся стран", Женева, 16 октября 2019 года.

³⁹ ISO: [ISO/IEC 30141:2018](#), "Internet of Things (IoT) — Reference Architecture", август 2018 года.

⁴⁰ ISO: [ISO/IEC 21823-1:2019](#), "Internet of Things (IoT) — Interoperability for IoT systems — Part 1: Framework", февраль 2019 года.

⁴¹ IEEE [IEEE 2413-2019](#), "IEEE Standard for an Architectural Framework for the Internet of Things (IoT)", май 2019 года.

⁴² IEEE [IEEE P2413-1](#), "Standard for a Reference Architecture for Smart City (RASC)", август 2018 года.

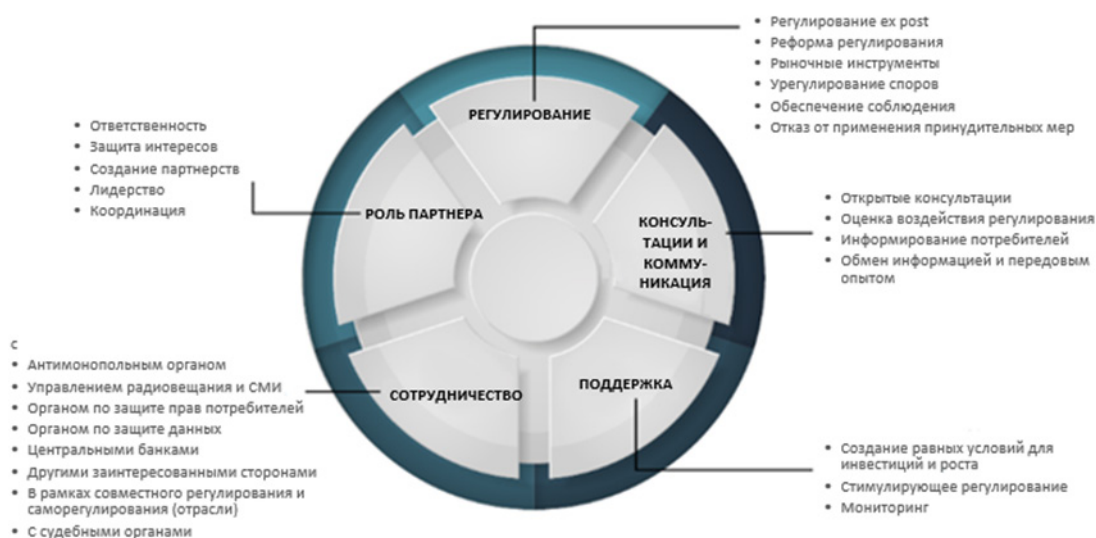
⁴³ МСЭ-D "[Глобальные перспективы регулирования в области ИКТ, 2017 год](#)", 2017 год.

Рисунок 15: Поколения регулирования в области ИКТ– концептуальная схема



Для регулирования пятого поколения, то есть совместного регулирования, характерны гибкость и ориентированность на консенсус. Совместное регулирование содействует инновациям, эффективности, повышению QoS, обмену данными и обеспечению безопасности, а также позволяет решать ряд проблем, в частности задачи функциональной совместимости. Кроме того, такое регулирование основывается на обмене специальными знаниями, руководящих принципах и передовом опыте и предполагает выявление механизмов межсекторального сотрудничества в целях более эффективного решения общих проблем (см. **Рисунок 16**)⁴⁴.

Рисунок 16: Совместное регулирование



В Руководящих указаниях на основе примеров передового опыта, принятых ГСР-19 МСЭ, совместное регулирование рассматривается как инструмент обеспечения успешной цифровой трансформации⁴⁵.

5.3.2 Регулирование IoT

Многие правительства поощряют инновации в сфере IoT и стремятся реформировать соответствующую нормативно-правовую базу таким образом, чтобы она не создавала препятствий для роста этой сферы. Однако с учетом того, что до сих пор существует некоторая степень неопределенности в отношении

⁴⁴ Там же.

⁴⁵ "Руководящие указания на основе примеров передового опыта Глобального симпозиума для регуляторных органов (ГСР) 2019 года", Порт-Вила, 2019 год.

регулирования рынка IoT, нововведения и корректировки в регуляторной сфере будут осуществляться поэтапно.

IoT отличается от соединений, возможность установления которых стремятся обеспечить регуляторные органы в области ИКТ. Соединения представляют собой базовую услугу, в то время как IoT также включает в себя соответствующие приложения, устройства и датчики.

В целом, несмотря на то что IoT подпадает под действие всех регуляторных норм, эта технология может обусловить необходимость установления дополнительных требований. Политика и регулирование должны предусматривать решение вопросов, характерных именно для IoT, таких как:

- конфиденциальность, защита данных и безопасность;
- стандарты и функциональная совместимость систем, платформ и соединенных объектов;
- управление использованием спектра и лицензирование спектра (во многих случаях устройства IoT работают на основе беспроводных технологий);
- нумерация и переносимость номера;
- необходимость перехода от IPv4 к IPv6;
- затраты, надежность, QoS и оценка пользователем качества услуг (QoE);
- меры по управлению конкуренцией.

Регулирование в области ИКТ становится все более сложным, что связано с вопросами безопасности, конфиденциальности и защиты данных. Многим странам, возможно, потребуется обновить устаревшее или чрезмерно ограничительное регулирование, в частности с учетом того, что проблемы функциональной совместимости сказываются на усилиях по расширению масштаба.

Специалисты призывают к созданию открытой экосистемы IoT на основе общедоступных платформ, приложений и стандартов с открытым исходным кодом в целях повышения функциональной совместимости и сокращения затрат, что, в свою очередь, будет способствовать экономическому росту и инновациям.

5.4 Заключение

Стандартизация имеет решающее значение для создания единого рынка IoT, который давал бы возможность подключать любое устройство и осуществлять с его помощью обмен данными из любой точки. Стандартизация позволяет обеспечить совместимость, в том числе функциональную совместимость, надежность и безопасность; способствует появлению новых экосистем и инноваций; и содействует повышению конкурентоспособности.

Регуляторные органы должны признать влияние новых технологий IoT и собственную значительную роль в разработке этих технологий и обеспечить создание новых возможностей за счет перехода к новой эпохе совместного регулирования, в рамках которого регуляторные органы в области ИКТ выполняют в большей степени функции содействующих организаций, сосредоточивая свои усилия на улучшении подключения и сотрудничестве с другими заинтересованными сторонами в целях поощрения использования ИКТ во всевозможных сферах.

Наконец, стратегия, которая опирается на прогрессивную регуляторную основу, может обеспечивать защиту и создавать стимулы для всех заинтересованных сторон благодаря предоставлению специальных знаний, а также финансовых и иных ресурсов. Кроме того, такая стратегия может содействовать развитию этой новой технологии и конкурентного рынка и высокому темпу инноваций.

Глава 6 – Передача информации, ноу-хау и знаний

6.1 Потребности в плане обучения и образовательные возможности в сфере С&I

Деятельность в области С&I требует набора узкоспециальных навыков, а реализацией программ С&I должны заниматься квалифицированные специалисты. Кроме того, этой сфере свойственны определенные проблемы, в частности:

- Отсутствие формальных комплексных программ обучения в области С&I. В крупных организациях персонал обучается навыкам в области С&I благодаря работе в паре с опытными сотрудниками. Несмотря на то, что это может быть полезным, такой подход в большинстве случаев обеспечивает лишь ограниченный круг знаний и не предполагает формального контроля качества обучения. Более того, он не может применяться в небольших организациях.
- Различные практикующие специалисты в области С&I, включая сотрудников регуляторных органов, лицензиатов, лиц, запрашивающих сертификаты (импортеры и производители), и специалистов по вопросам соответствия, должны также хорошо разбираться в соответствующих правовых, технических, внешнеторговых и экономических вопросах.
- Стремительное развитие технологических продуктов представляет собой постоянную проблему для систем С&I (например, в части конфигурации IoT и программного обеспечения).

В Резолюции 177 (Пересм. Дубай, 2018 г.) Полномочной конференции МСЭ была подчеркнута необходимость продолжения деятельности по наращиванию потенциала в области С&I без отрыва от производства в сотрудничестве с признанными учреждениями и с использованием преимуществ экосистемы Академии МСЭ, в том числе деятельности, связанной с предотвращением помех радиосвязи, создаваемых или принимаемых оборудованием ИКТ⁴⁶.

Опыт 2020 года показал, что существует насущная глобальная потребность в цифровом обучении с помощью надежных сетей ИКТ. На фоне пандемии COVID-19 использование ИКТ в образовательных целях все больше воспринимается как общественное благо. Как было отмечено в Резолюции 177 (Пересм. Дубай, 2018 г.), Академия МСЭ предлагает различные решения по онлайн-обучению для преподавателей, и глобальному сообществу С&I следует их изучить.

6.2 Удовлетворение потребностей, связанных с получением/сохранением знаний

В качестве одного из способов содействия развитию и расширению навыков следует рассмотреть создание совместной платформы на основе механизмов обеспечения качества по аналогии с предложением МСЭ для учебной программы по соответствию и функциональной совместимости (СІТР)⁴⁷.

Программа СІТР основана на предыдущем успешном опыте проведения учебных мероприятий по С&I, таких как региональные учебные занятия без отрыва от производства по программам и областям проверки на С&I, совместно с партнерскими лабораториями⁴⁸. В программе также учитываются выводы, почерпнутые из публикаций МСЭ, включая заключительный отчет по Вопросу 4/2 за предыдущий исследовательский период⁴⁹ и опубликованные руководящие указания⁵⁰.

Работа по составлению СІТР ведется на основе модели, которая установлена в рамках механизма обеспечения качества Академии МСЭ и включает в себя пакет материалов высокого уровня, подготовленных экспертами по соответствующим вопросам, процесс коллегиального обзора и шаблоны, разработанные

⁴⁶ МСЭ. [Резолюция 177 \(Пересм. Дубай, 2018 г.\)](#) Полномочной конференции о соответствии и функциональной совместимости.

⁴⁷ Эти концепции были представлены в октябре 2019 года в Документе ИК2 МСЭ-D [SG2RGQ/194 + Приложение](#) от координатора БРЭ по Вопросу 4/2.

⁴⁸ МСЭ-D. [Мероприятия по вопросу соответствия и функциональной совместимости](#).

⁴⁹ МСЭ-D. Заключительный отчет по Вопросу 4/2 2-й Исследовательской комиссии МСЭ-D за исследовательский период 2014–2017 годов. Там же.

⁵⁰ МСЭ-D. [Публикации и итоговые документы – С&I](#).

профессиональными преподавателями для планирования учебного процесса и написания программ обучения.

Ниже представлена предлагаемая структура обучения, которая предусматривает индивидуальный подбор учебного плана:

Рисунок 17: Учебные модули СИТР (ОМ – обязательные модули, ЭМ – элективные модули)



Структура обучения строится вокруг четырех основных тем, с разбивкой на подтемы в соответствии с избранным направлением обучения и принципом модульной передачи знаний, которая требуется студентам.

1 Разработка и внедрение режимов/систем обеспечения соответствия и функциональной совместимости

Целью данного модуля является обеспечить понимание минимальных технических требований и научить использовать существующие структуры C&I и их вспомогательные средства для достижения оптимального баланса между уровнем доверия и уровнем контроля устройств ИКТ.

2 Области тестирования, охватывающие широкий спектр услуг лабораторий

Охват областей тестирования потенциально безграничен; он может включать в себя такие вопросы как одобрение новых технологий и содействие молодым предпринимателям в целях обеспечения международного признания их продуктов.

Совершенно очевидно, что учебные модули должны разрабатываться с учетом существующих потребностей и приоритетов.

3 Региональное сотрудничество по вопросам стандартов и процессов одобрения типа и их согласование, включая соглашения о взаимном признании

Как отмечалось в предыдущей главе, ключевая роль принадлежит сотрудничеству; данный модуль направлен на поощрение совместного использования уже имеющихся ресурсов и механизмов для проведения сертификации соответствия продуктов ИКТ международным и национальным техническим требованиям.

4 Создание и техническое обслуживание лабораторий по тестированию

В данном модуле рассматриваются вопросы, касающиеся процедур проверки качества и стратегических оценок, как, например, оптимизация бизнес-планирования.

6.3 Выводы

Подводя итоги, следует отметить, что в комплексном анализе способов разработки учебной программы в области передачи информации, ноу-хау и знаний должны учитываться следующие аспекты:

- сотрудничество с экспертами в данной области, в том числе с исследовательскими комиссиями МСЭ (Группа Докладчика по Вопросу 4/2 ИК2 МСЭ-D и ИК11 МСЭ-T, а также авторы вкладов Бюро радиосвязи), профессионалы в сфере тестирования, специалисты по вопросам одобрения типа, эксперты по торговле;
- учебные материалы на основе публикаций МСЭ по программе C&I, включая руководящие указания и Рекомендации МСЭ, разработанные МСЭ-R и МСЭ-T;
- работа по обеспечению передачи знаний международными, региональными и национальными организациями;
- упрощение доступа к подготовке в области C&I и обеспечение ориентированного на перспективу профессионального подхода;
- общедоступный формат курса, понятный новичкам и специалистам;
- модульный гибкий подход, позволяющий обеспечить надлежащий уровень знаний для решения поставленных задач и соответствие материалов курса имеющимся потребностям в сфере C&I.

Annexes

Annex 1: Conformance and interoperability frameworks: country data

Understanding how countries organize themselves for guaranteeing proper conformance and interoperability levels for ICT networks and devices deployment can help C&I operators to establish efficient mechanisms for collaboration. This can be verified in effective technical collaboration agreements in some regions (e.g. Europe, APEC-MRA).

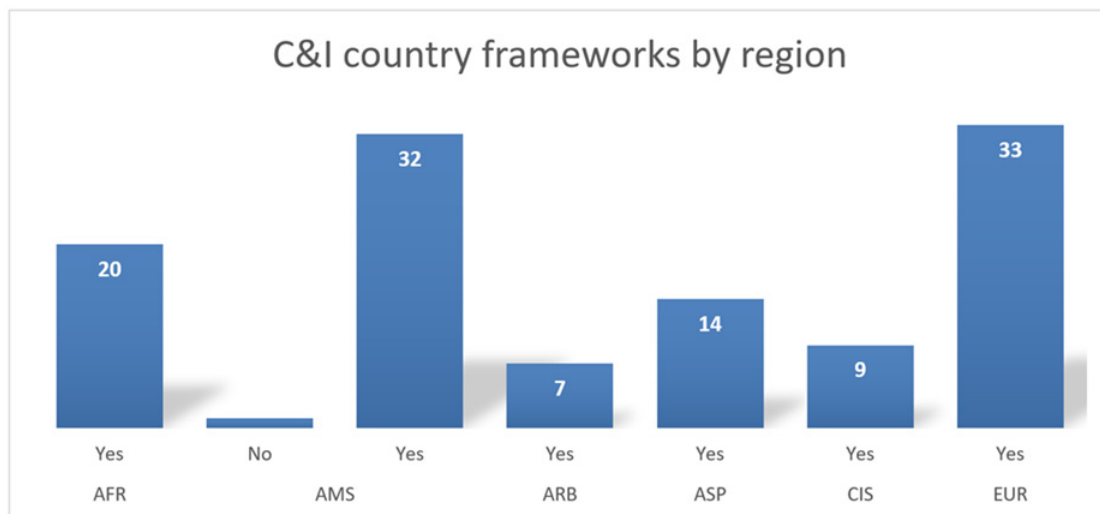
Data shows that most of the countries have in place a Conformance and Interoperability arrangement aiming to ascertain trust on a safe and interoperable use of ICT devices by networks and citizens. Noting that procedures and strictness levels of requirements (e.g., recognition of certification and use of proxies, self-declaration, local testing, etc.) can differ significantly.

Various events undertaken under the ITU C&I Programme Pillars 3 (capacity building) and 4 (assistance to developing countries)⁵¹ allowed to gather related information from 116 countries⁵².

Data research and organization of essential information considered different C&I infrastructure variables, such as:

1. Conformance and Interoperability Frameworks
2. ICT Standards and Technical Requirements
3. Conformance Assessment and Bodies
4. Testing Laboratories
5. Quality and metrology

Figure 1A: Legal C&I Frameworks from 114 countries that provided information



The figure above displays the number of C&I country framework per region from 116 countries: 115 countries informed the existence of legal document and a level of procedure for accepting ICT products in their markets (importation fees and taxes not included); only one country in the Americas informed about the absence of any legal procedures for ICT products.

The complete dataset display is a work in progress and complete analysis will be provided through the ITU-C&I development portal (https://itu.int/go/ci_development)

⁵¹ The source material used for the data research is currently available on the ITU website, from: [C&I events](#); [Assessment studies](#); ITU-D Study Group Question 4/2 inputs as national and regional case studies.

⁵² ITU-D SG2 Document [SG2RGQ/274 + Annex](#) from the BDT Focal Point for Question 4/2.

Annex 2: Counterfeiting – a survey of national frameworks and practices

Data from the annual ITU World Telecommunication/ICT Regulatory Survey (edition 2019) on regulatory practices related to the distribution and use of counterfeit ICTs.

The data series featured are as follows:

- 1) Responsibilities of telecom/ICT regulators related to ICT counterfeiting,
- 2) Types of counterfeit ICTs overseen by the telecom/ICT regulator,
- 3) Policy/legislation/regulation related to ICT counterfeiting adopted,
- 4) Areas covered in ICT counterfeiting regulations,
- 5) Plans to adopt a regulatory framework for ICT counterfeiting.⁵³

Table 1A: Summary of ITU World Telecommunication/ICT Regulatory Survey (edition 2019): Survey on regulatory practices related to the distribution and use of counterfeit ICTs

Summary								
Question	Answer	Africa	Arab States	Asia & Pacific	CIS	Europe	The Americas	Total
Does the Telecom/ICT regulator (or the entity in charge of regulation in the sector) have responsibilities related to ICT counterfeiting (e.g., fake mobile phones, smartphones, computers, any network or other computing equipment components)?	Yes	23	12	10	0	9	11	65
	No	10	3	10	2	28	14	67
Has your country adopted any policy/legislation/regulation related to ICT counterfeiting?	Yes	23	11	7	2	14	14	71
	No	10	5	15	3	20	12	65
If no, are there plans to adopt a regulatory framework for ICT counterfeiting?	Yes	3	3	4	0	3	3	16
	No	4	0	8	4	11	5	32
Region size		44	22	40	9	46	35	196
* This question allows multiple answers per country/economy								
Year: 2019 or latest available data.								
Source: ITU World Telecommunication/ICT Regulatory Database								
ITU ICT-Eye: http://www.itu.int/icteye								

⁵³ ITU-D SG2 Document [SG2RGQ/38 + Annex](#) from the BDT Focal Point for Question 3/1.

Figure 2A: Regional distribution of responses from survey – Question 1

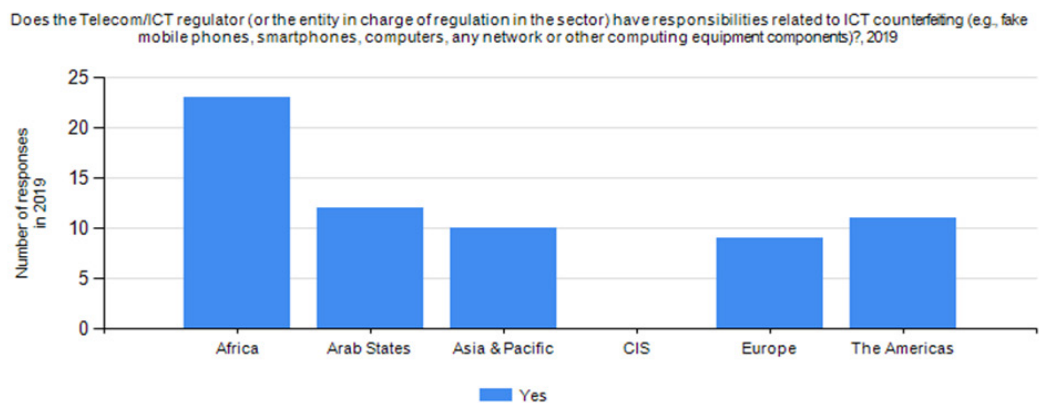


Figure 3A: Regional distribution of responses from survey – Question 2

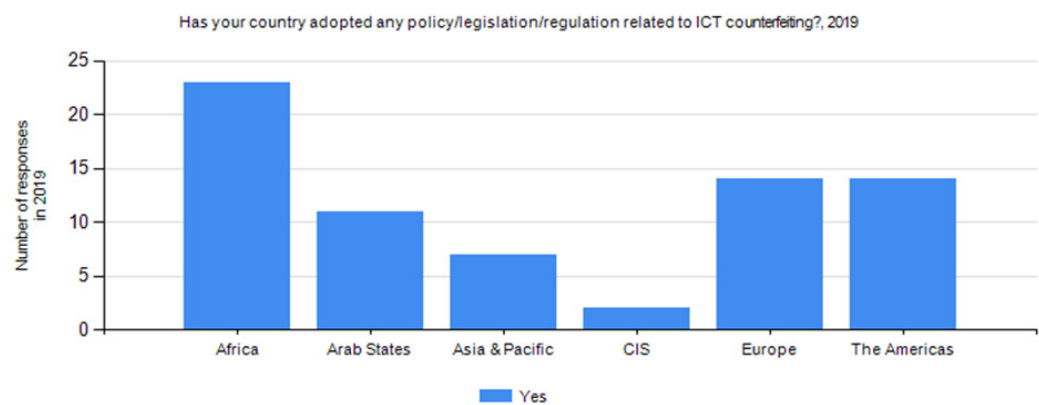
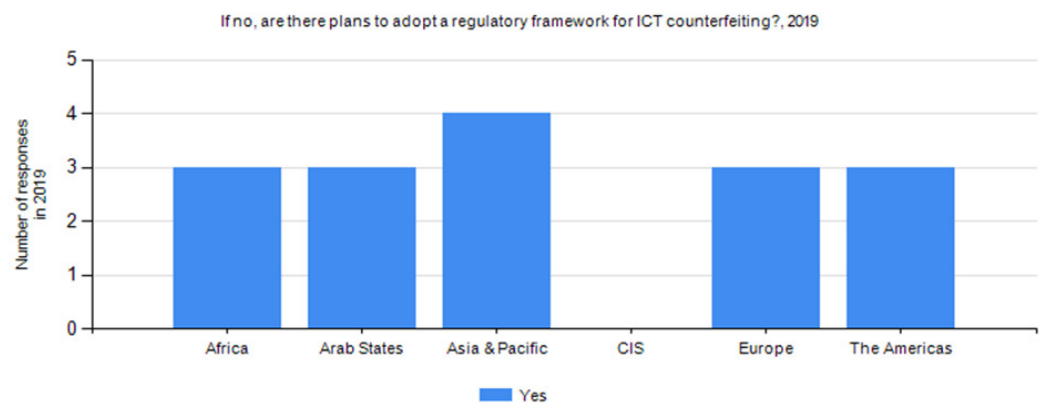


Figure 4A: Regional distribution of responses from survey – Question 3



Annex 3: Initiatives in the fight against equipment counterfeiting and mobile terminal theft in Burundi⁵⁴

A3.1 Introduction

Counterfeiting of mobile phones has numerous negative effects on industry, society, governments and in particular consumers of ICT services. Primarily, it leads to a lower quality of service of mobile telecommunications and safety hazards associated with the use of defective second-hand terminals due to inferior quality or unsuitable technical characteristics.

A3.2 Impact of the proliferation and use of counterfeit mobile terminals

The use of counterfeit mobile terminals by consumers and rising dissatisfaction among mobile subscribers faced with the growing phenomenon of mobile terminal theft has undesirable consequences in the short and long term, including:

- Lowering the QoS of mobile telecommunication services, which in turn has an impact on the experience of consumers and businesses
- Compromising the security of digital transactions and that of mobile terminal users
- Increasing evasion from applicable taxes and duties, which has a negative effect on tax revenues
- Creating risks to the environment and consumer health due to the use of hazardous substances recovered from waste electrical and electronic equipment (WEEE)
- Facilitating the drugs trade, terrorism and other local, regional and international criminal activity
- Infringing on manufacturers' trademarks
- Significantly affecting the ICT market by proposing poor-quality, low-cost products that tend to have a greatly reduced lifetime, whence the accumulation of WEEE.

A3.3 National initiatives in the fight against mobile terminal theft and equipment counterfeiting

To combat the use of counterfeit terminals more effectively, the *Agence de régulation et de contrôle des télécommunications* (ARCT) (Telecommunication Regulatory and Control Agency of Burundi) has instituted the following measures:

- 1) Creation of certification procedures for telecommunication equipment
- 2) Registration of the characteristics of telecommunication equipment
3. Issuance of import certificates for vendors of telecommunication equipment
- 4) Enforcement of the requirement that telecommunication equipment vendors be licensed and display their vendor's licence on the establishment's walls, that terminals be certified by ARCT, and that equipment be guaranteed for at least six months
- 5) Regular inspections to verify compliance and respect of technical standards and regulations
- 6) Creation of a toll-free number (151) for members of the public to report telephone sales where there is a problem with the IMEI number of the phone and that on the package
- 7) Organization of public awareness campaigns on the dangers of using counterfeit mobile terminals
- 8) Inspection of electronic communication terminal equipment in use by public and private organizations
- 9) Inspection of providers of value-added services who use numbering resources.

⁵⁴ ITU-D SG2 Document [2/390](#) from Burundi [in French].

To combat the use of stolen mobile terminals more effectively, ARCT has initiated the following activities:

- 1) Registration of all mobile telecommunication service subscribers: ARCT regularly assesses compliance with the circular on the registration of subscribers by the telecommunication operators, in order to combat fraud.
- 2) Automation of the service for requisitioning expert testimony: A management application for processing and managing requisitions for expert testimony in cases of mobile communication terminal theft has been designed and implemented.
- 3) Combating theft and crimes committed using mobile telephones: ARCT invites members of the public to report the numbers used to send suspicious messages and to forward them to ARCT for systematic verification and deactivation if necessary.

A3.4 Conclusion

It is crucial to put into action all effective means for combating counterfeit terminals being sold or connected to the telecommunication network, so as to protect the consumers of ICT services. This will also enhance security for users, improve the quality of service of networks and stimulate digital economy and financial growth of the country.

Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость, а также в борьбе с использованием контрафактного оборудования информационно-коммуникационных технологий и хищением мобильных устройств

Annex 4: Illustrations for chapters of the Output Report on Question 4/2

The following illustrations summarize concepts for Chapters 2, 3 and 5 of the Output Report.

Definitive, high-level resolution images of the illustrations are available at https://itu.int/go/CI_development.

Figure 5A: Illustration for Chapter 2 – What is conformance and interoperability (C&I)



Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость, а также в борьбе с использованием контрафактного оборудования информационно-коммуникационных технологий и хищением мобильных устройств

Figure 6A: Illustration for Chapter 2 – C&I frameworks



Figure 7A: Illustration for Chapter 3 – Combating the proliferation of counterfeit, substandard and tampered devices



Помощь развивающимся странам в выполнении программ по проверке на соответствие и функциональную совместимость, а также в борьбе с использованием контрафактного оборудования информационно-коммуникационных технологий и хищением мобильных устройств

Figure 8A: Illustration for Chapter 5 – The Internet of Things and C&I



Annex 5: Ideas for the future of the Question

Having regard to the role of C&I in a hyperconnected world where billions of people and objects connect with each other, the study group's work on C&I could focus on:

- **Efforts to manage the increasing number of devices sharing the same limited resources**
- **Measures to cover costs related to conformity procedures and controls of ICT products to allow only approved products to access markets**
- **Harmonization of procedures and collaboration**
 - Robust C&I frameworks: Making sure every country has or is part of a robust C&I framework at minimal cost (e.g. agreements on the shared use of national C&I infrastructure, such as testing facilities and certificates of conformity).
 - Collaboration: Are MRAs effective tools to pursue in the future? What aspects of MRAs need to be adapted to improve existing collaboration agreements or develop new ones? The group could focus on innovative collaboration structures to improve access to high-quality and safe ICT products.
- **Trends**
 - Future challenges for C&I, such as:
 - New technologies outpacing regulation/testing procedures
 - Regulatory aspects for open RAN and interoperability adoption related to 5G
 - Smart objects able to communicate through ICTs
 - Software tampering/hacking vulnerabilities
 - Effective harmonization of procedures and technical collaboration, etc.
 - Means of prioritizing device/type-approval models to achieve a good balance between trust and control.
 - C&I challenges and opportunities during the COVID-19 pandemic.
 - Ways in which new technologies (such as blockchain and artificial intelligence) can help to improve trust in the international C&I framework and trade in and use of ICT devices.

Annex 6: List of contributions and liaison statements received on Question 4/2

Contributions on Question 4/2

Web	Received	Source	Title
2/423	2021-03-18	Rapporteur for Question 4/2	Proposed liaison statement from ITU-D Study Group 2 Question 4/2 to ITU-T Study Group 11, ITU-R WP1A and WP6A, and ISO/CASCO
2/390	2021-02-03	Burundi	Initiatives de lutte contre les équipements de contre-façon et le vol des terminaux mobiles au Burundi
RGQ2/277	2020-09-22	Algérie Télécom SPA (Algeria)	Revisions to Draft Chapter 3 for the Final Report of Question 4/2
RGQ2/274 + Ann.1	2020-09-22	BDT Focal Point for Question 4/2	C&I Database- updated summary
RGQ2/269	2020-09-22	Rapporteur for Question 4/2	Draft text for new chapter (Ideas for the Future of the Question) of the Output Report for Question 4/2
RGQ2/265	2020-09-22	Rapporteur for Question 4/2	Draft text for Chapter 1 Section 1.4 on COVID-19 impact to type approval procedures
RGQ2/264	2020-09-22	Kenya	Proposed draft text for Chapter 4 of the Output Report for Question 4/2
RGQ2/233	2020-08-20	Algérie Télécom SPA (Algeria)	Proposed text for Chapter 5: Internet of Things and C&I
2/345	2020-02-11	BDT Focal Point for Question 4/2	ITU Conformance and Interoperability Training Programme
2/337	2020-02-11	Algérie Télécom SPA (Algeria)	Revisions to draft Chapter 3 for the Final Report of Q4/2
2/332 + Ann.1	2020-02-11	Kenya	Device Management System- Kenyan Case
2/326	2020-02-10	Oman	Problem of increasing use of fake IMEI
2/323 (Rev.1)	2020-02-07	Ghana	Achieving quality C&I regimes- Challenges from basic Infrastructure to legislative and regulatory frameworks. The experience of Ghana
2/311	2020-01-28	International Telecommunication Academy (Russian Federation)	Regulation on the system to confirm the compliance of communication facilities and services with the ITU standard
2/290	2020-01-08	Mauritania	Mauritania (Islamic Republic of)
2/261	2019-12-24	Guinea	Conformance and interoperability (C&I)
2/257	2019-12-20	Mauritania	Proposed draft text for Chapter 2 of the Final Report for Question 4/2
2/250	2019-12-08	Comoros	Progress of activities for implementing conformance and interoperability programmes in the Union of the Comoros
RGQ2/194 + Ann.1	2019-09-24	BDT Focal Point for Question 4/2	ITU Conformity and Interoperability Training Programme (CITP)
RGQ2/171	2019-09-18	Algérie Télécom SPA (Algeria)	Implementation of Plenipotentiary Conference (PP-18) Resolution 177 (Rev. Dubai, 2018)

(продолжение)

Web	Received	Source	Title
RGQ2/170	2019-09-15	Mauritania)	Conformité et interopérabilité des équipements TIC dans les pays en développement : normes et procédures- cas de la Mauritanie
RGQ2/144	2019-08-20	Central African Republic	Assistance to developing countries for implementing conformance and interoperability (C&I) programmes and combating counterfeit ICT equipment and theft of mobile devices
RGQ2/139	2019-08-06	Guinea	Assistance to developing countries for implementing conformance and interoperability (C&I) programmes and combating counterfeit ICT equipment
2/TD/24	2019-03-29	Rapporteur for Question 4/2	Proposed outgoing liaison statements from Q4/2
2/TD/22 + Ann.1-3	2019-03-27	Rapporteur for Question 4/2	Proposed updates to work plan, table of contents and areas of responsibilities, matrix of contributions received and proposal for second focus session
2/210	2019-03-12	BDT Focal Point for Question 4/2	C&I Programme- Pillars 3 & 4 implementation report
2/202 + Ann.1	2019-03-08	BDT Focal Point for Question 4/2	Summary on national C&I topics
2/177	2019-02-07	Rapporteur for Question 4/2	Draft Chapter 3 for Final Report on Question 4/2
2/166	2019-02-06	Mexico	Regulatory obligations to help combat the theft of mobile devices
2/149	2019-01-24	Guinea	Assistance to developing countries for implementing conformance and interoperability programmes, portability and combating counterfeit ICT equipment and theft of mobile devices
2/142	2019-01-16	Madagascar	Implementing conformance and interoperability programmes
2/133	2019-01-10	Comoros	Realization of a programme for assistance to developing countries for implementing conformance and interoperability programmes: case of Union of the Comoros
RGQ2/TD/8	2018-09-25	South Sudan	Challenges and proposals to deal with counterfeit ICT equipment and mobile device theft in South Sudan and region
RGQ2/TD/7	2018-10-01	Russian Federation	ITU-D SG1 and SG2 coordination: Mapping of ITU-D Study Group 1 and 2 Questions
RGQ2/86 + Ann.1	2018-09-18	BDT Focal Point for Question 4/2	ITU C&I programme: implementation update
RGQ2/85	2018-09-18	Zimbabwe	Actions to combat counterfeit and theft of mobile devices in Zimbabwe
RGQ2/82	2018-09-18	Ghana	Ghana's Type Approval Regime- a sustainable approach to connecting and protecting users of telecommunications/ICTs and networks through conformance assessment

(продолжение)

Web	Received	Source	Title
RGQ2/80	2018-09-18	GSM Association	GSMA's IMEI database and services
RGQ2/69	2018-09-17	Rwanda	Regional effort to fight illegal devices, improve the quality of services and minimize health hazard to consumers
RGQ2/66 (Rev.1)	2018-09-16	Senegal	Lutte contre la contrefaçon et le vol de téléphone
RGQ2/38 + Ann.1	2018-08-18	BDT Focal Point for Question 3/1	ITU data on regulatory practices related to counterfeit ICTs
RGQ2/9 (Rev.1)	2018-07-05	Guinea	Implementing conformance and interoperability programmes and combating counterfeit ICT equipment and theft of mobile devices
2/TD/10	2018-05-10	Rapporteur for Question 4/2	Draft reply liaison statements from ITU-D Study Group 2 Question 4/2
2/TD/8	2018-05-09	Rapporteur for Question 4/2	Draft work plan, Table of Contents (ToC) and responsibilities for ITU-D Question 4/2
2/97 (Rev.1)	2018-05-06	Chairman, ITU-D Study Group 2	List of proposed Rapporteurs and Vice-Rapporteurs of ITU-D Study Group 2 study Questions for the 2018-2021 period
2/92 + Ann.1	2018-04-24	BDT Focal Point for Question 4/2	ITU C&I Programme status- Pillars 3 and 4
2/90	2018-04-24	Mauritania	Draft work plan for ITU-D Study Group 2 Question 4/2
2/88 + Ann.1	2018-04-23	BDT	Implementation of ITU C&I Programme and ITU-T activities on combatting counterfeiting and stolen ICT devices
2/83	2018-04-23	Iran University of Science and Technology (Islamic Republic of Iran)	HAMTA: A system for combating counterfeit ICT equipment and theft of mobile devices
2/58	2018-03-22	Algérie Télécom SPA (Algeria)	Conformance and interoperability
2/45	2018-03-12	Madagascar	Monitoring counterfeit terminal devices, building a healthy network that brings in revenues for the State

Incoming liaison statements for Question 4/2

Web	Received	Source	Title
RGQ2/219	2020-08-06	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates on the current work at ITU-T Q15/11 "Combating counterfeit and stolen ICT equipment"
RGQ2/205 + Ann.1-2	2020-03-25	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates on the current work at ITU-T Q15/11 "Combating counterfeit and stolen ICT equipment"
RGQ2/204 + Ann.1	2020-03-25	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on contribution on conformance and interoperability

(продолжение)

Web	Received	Source	Title
RGQ2/115 + Ann.1	2019-06-14	ITU-T Study Group 5	Liaison statement from ITU-T SG5 to ITU-D SG2 Q4/2 and Q7/2 on work being carried out under study in ITU-T Study Group 5 Question 3/5
RGQ2/113	2019-05-29	ITU-T Study Group 20	Liaison statement from ITU-T SG20 to ITU-D SG2 Q4/2 on SG20 activities on IoT and Smart Cities & Communities
RGQ2/111 + Ann.1-3	2019-04-21	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on collaboration
2/TD/22 + Ann.1-3	2019-03-27	Rapporteur for Question 4/2	Proposed updates to work plan, table of contents and areas of responsibilities, matrix of contributions received and proposal for second focus session
2/TD/19 + Ann.1-3	2019-03-21	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on collaboration
2/TD/17 + Ann.1	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates to the Technical Report on the Combat of Counterfeit Devices
2/TD/16 + Ann.1	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on creation of new work item on "Reliability of IMEI identifier"
2/TD/15	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on impact of counterfeit mobile devices on Quality of Service
2/139	2019-01-16	ITU-T Study Group 20	Liaison statement from ITU-T SG20 on SG20 activities on IoT and Smart City & Community
RGQ2/16 + Ann.1-3	2018-08-02	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on progress and collaboration on the combat of counterfeit and mobile device theft
2/35	2017-12-01	ITU-T Study Group 11	Liaison Statement from ITU-T SG11 to ITU-D SG2 Question 4/2 on ongoing collaboration

**Канцелярия Директора
Международный союз электросвязи (МСЭ)
Бюро развития электросвязи (БРЭ)**
Place des Nations
CH-1211 Geneva 20 – Switzerland

Эл. почта: btdtdirector@itu.int
Тел.: +41 22 730 5035/5435
Факс: +41 22 730 5484

**Департамент цифровых сетей и
цифрового общества (DNS)**

Эл. почта: bdt-dns@itu.int
Тел.: +41 22 730 5421
Факс: +41 22 730 5484

**Департамент центра цифровых
знаний (DKH)**

Эл. почта: bdt-dkh@itu.int
Тел.: +41 22 730 5900
Факс: +41 22 730 5484

**Канцелярия заместителя Директора и региональное присутствие
Департамент координации операций на местах (DDR)**
Place des Nations
CH-1211 Geneva 20 – Switzerland

Эл. почта: bdtdeputydir@itu.int
Тел.: +41 22 730 5131
Факс: +41 22 730 5484

**Департамент партнерских отношений
в интересах цифрового развития (PDD)**

Эл. почта: bdt-pdd@itu.int
Тел.: +41 22 730 5447
Факс: +41 22 730 5484

Африка

Эфиопия

Региональное отделение МСЭ
Gambia Road
Leghar Ethio Telecom Bldg., 3rd floor
P.O. Box 60 005
Addis Ababa – Ethiopia

Эл. почта: itu-ro-africa@itu.int
Тел.: +251 11 551 4977
Тел.: +251 11 551 4855
Тел.: +251 11 551 8328
Факс: +251 11 551 7299

Камерун

Зональное отделение МСЭ
Immeuble CAMPOST, 3^e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun

Эл. почта: itu-yaounde@itu.int
Тел.: + 237 22 22 9292
Тел.: + 237 22 22 9291
Факс: + 237 22 22 9297

Сенегал

Зональное отделение МСЭ
8, Route des Almadies
Immeuble Rokhaya, 3^e étage
Boîte postale 29471
Dakar – Yoff – Senegal

Эл. почта: itu-dakar@itu.int
Тел.: +221 33 859 7010
Тел.: +221 33 859 7021
Факс: +221 33 868 6386

Зимбабве

Зональное отделение МСЭ
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare – Zimbabwe

Эл. почта: itu-harare@itu.int
Тел.: +263 4 77 5939
Тел.: +263 4 77 5941
Факс: +263 4 77 1257

Северная и Южная Америка

Бразилия

Региональное отделение МСЭ
SAUS Quadra 6 Ed. Luis Eduardo
Magalhães
Bloco E, 10^o andar, Ala Sul
(Anatel)
CEP 70070-940 Brasilia – DF – Brazil

Эл. почта: itubrasilia@itu.int
Тел.: +55 61 2312 2730-1
Тел.: +55 61 2312 2733-5
Факс: +55 61 2312 2738

Барбадос

Зональное отделение МСЭ
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Эл. почта: itubridgetown@itu.int
Тел.: +1 246 431 0343
Факс: +1 246 437 7403

Чили

Зональное отделение МСЭ
Merced 753, Piso 4
Santiago de Chile – Chile

Эл. почта: itusantiago@itu.int
Тел.: +56 2 632 6134/6147
Факс: +56 2 632 6154

Гондурас

Зональное отделение МСЭ
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cia
Apartado Postal 976
Tegucigalpa – Honduras

Эл. почта: itutegucigalpa@itu.int
Тел.: +504 2235 5470
Факс: +504 2235 5471

Арабские государства

Египет

Региональное отделение МСЭ
Smart Village, Building B 147
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo – Egypt

Эл. почта: itu-ro-arabstates@itu.int
Тел.: +202 3537 1777
Факс: +202 3537 1888

Азиатско-Тихоокеанский регион

Таиланд

Региональное отделение МСЭ
Thailand Post Training Center
5th floor
111, Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

Эл. почта: ituasiapacificregion@itu.int
Тел.: +66 2 575 0055
Факс: +66 2 575 3507

Индонезия

Зональное отделение МСЭ
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110 – Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110 – Indonesia

Эл. почта: ituasiapacificregion@itu.int
Тел.: +62 21 381 3572
Тел.: +62 21 380 2322/2324
Факс: +62 21 389 5521

СНГ

Российская Федерация

Региональное отделение МСЭ
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Эл. почта: itumoscow@itu.int
Тел.: +7 495 926 6070

Европа

Швейцария

Отделение для Европы МСЭ
Place des Nations
CH-1211 Geneva 20 – Switzerland

Эл. почта: eurregion@itu.int
Тел.: +41 22 730 5467
Факс: +41 22 730 5484

Международный союз электросвязи
Бюро развития электросвязи
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-34134-3



9 789261 341343

Опубликовано в Швейцарии
Женева, 2021 г.