Технологическая основа построения многополярного мира

С.В. МЕЛЬНИК, технический директор ООО "НТЦ КОМТЕСТ", руководитель рабочей группы МАС "Сертификация и метрология" кандидат технических наук, Е.Н. ПЕТРОВА, академик МАС, В.А. СУДОВЦЕВ, президент Женевского отделения МАС

Введение

В штаб-квартире МСЭ в Женеве с 30 октября по 3 ноября т.г. проходило собрание Исследовательской комиссии 2 (ИК-2) Сектора развития электросвязи (МСЭ-D). В работе ИК-2 приняли участие более 290 делегатов от государств и организаций членов МСЭ, включая представителей администрации связи Российской Федерации и Международной академии связи (МАС). От МАС в работе участвовали В.А. Судовцев, президент Женевского отделения МАС, А.С. Бородин, академик МАС, С.В. Мельник, руководитель РГ "Сертификация и метрология" МАС, Е.Н. Петрова, академик МАС.

На заседании по вопросу 4/2 "Подтверждение соответствия средств связи и борьба с использованием контрафактного ИКТ-оборудования", которое проходило под руководством председателя Ава Коко Валери Надеж Гуэ (Котд'Ивуар) и заместителя председателя С.В. Мельника (Российская Федерация), был представлен материал МАС о необходимости внедрения механизма систем национальной экспертизы при введении новых ИКТ.

Материал был активно поддержан странами Африканского союза и Арабскими государствами.

Представление материалов

Собрание Исследовательской комиссии 2 Сектора развития электросвязи провело большую работу. Были рассмотрены последовательно все 7 вопросов (от семи рабочих групп). Группы работали по темам:

"Устойчивые "умные" города и сообщества" (вопрос 1/2);

"Опорные технологии для электронных услуг и приложений, в том числе для электронного здравоохранения и электронного образования" (вопрос 2/2);

"Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности" (вопрос 3/2);

"Подтверждение соответствия средств связи и борьба с использованием контрафактного ИКТ-оборудования" (вопрос 4/2);

"Внедрение электросвязи и ИКТ и совершенствование цифровых навыков" (вопрос 5/2);

"ИКТ для окружающей среды" (вопрос 6/2);

"Стратегии и политика, касающиеся воздействия электромагнитных полей на человека" (вопрос 7/2).

Наибольший интерес представляло заседание по вопросу 4/2 "Подтверждение соответствия средств связи и борьба с использованием контрафактного ИКТ-оборудования", на котором были рассмотрены доклады от Либерии и Шри-Ланки по вопросу борьбы с использованием похищенных и контрафактных мобильных телефонов.

Так, отмечено, что в Либерии регистрация SIM-карт является обязательным условием для всех абонентов, что помогает выявлять похищенные и клонированные мобильные телефоны. Однако не существует политики по возвращению украденных телефонов, а клонированные устройства попадают в страну через пограничные пункты. Похищенные телефоны зачастую отправляются на заводы для воспроизведения, а физические рынки позволяют торговать контрафактной и пиратской продукцией. К недостаткам украденных и клонированных телефонов относятся ухудшение сигнала, более высокий уровень потери данных и проблемы для поставщиков услуг. Для того чтобы решить эту проблему, страны, в которых осуществляется производство, должны прекратить производство контрафактных устройств, а компаниям GSM следует поощрять использовать блокировку (Kill Switch) для дистанционного отключения похищенных телефонов.

В Шри-Ланке устройства с поддержкой IMEI, такие как мобильные телефоны, все чаще становятся целями преступников из-за содержащейся в них конфиденциальной информации. Правительства внедрили правила и системы, позволяющие свести к минимуму использование похищенных мобильных телефонов. Контрафактные устройства вызывают негативные последствия для пользователей, производителей, поставщиков, операторов сетей и правительств. Сектор электросвязи Шри-Ланки значительно вырос, и Комиссия по регулированию электросвязи Шри-Ланки контролирует импорт и регулирование использования мобильных устройств. Внедрение Национального реестра идентификации оборудования может помочь предотвратить использование похищенных или контрафактных устройств, но при этом возникают такие проблемы, как конфиденциальность, производительность сети и соблюдение законодательства. Эффективные решения включают блокировку устройств, наблюдение и правоприменение, законодательные реформы и повышение осведомленности потребителей.

Статью целиком читайте в бумажной версии журнала