|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **Международный союз электросвязи**  **Бюро стандартизации электросвязи** | | CCITT/ITU-T 60th Anniversary logo |
|  | |  | |

Женева, 26 мая 2016 года

|  |  |  |
| --- | --- | --- |
| Осн.: | **Дополнительный документ 1 к Коллективному письму 12/11 БСЭ** |  |
| Тел.: Факс: Эл. почта: | +41 22 730 5858 +41 22 730 5853 [tsbsg11@itu.int](mailto:tsbsg11@itu.int) | – Администрациям Государств – Членов Союза  – Членам Сектора МСЭ-Т  – Ассоциированным членам МСЭ-Т, принимающим участие в работе ИК11 МСЭ-Т  – Академическим организациям − Членам МСЭ |

|  |  |
| --- | --- |
| Предмет: | **Семинары-практикумы МСЭ-Т "Безопасность SS7" (29 июня 2016 г.) и "Борьба с контрафактной продукцией с использованием решений по проверке на соответствие и функциональную совместимость" (28 июня 2016 г.) в период собрания 11‑й Исследовательской комиссии МСЭ-Т (27 июня – 6 июля 2016 г.)** |

Уважаемая госпожа,  
уважаемый господин,

Настоящий дополнительный документ выпущен для представления дополнительной информации о соответствующих мероприятиях, организуемых в штаб-квартире МСЭ в период собрания 11‑й Исследовательской комиссии в Женеве, 27 июня – 6 июля 2016 года.

Хотел бы привлечь ваше внимание к нижеследующим мероприятиям:

**1 Семинар-практикум МСЭ-Т** **"**[**Безопасность SS7**](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx)**", 29 июня 2016 года (09 час. 00 мин. –12 час. 30 мин.)**

**Введение**

Система сигнализации № 7 (SS7) – это набор протоколов телефонной сигнализации, разработанный МСЭ-Т с 1970-х годов, который используется для установления и разъединения большинства телефонных соединений в мировом масштабе.

Стандарты SS7 широко применяются в коммутируемых телефонных сетях общего пользования (КТСОП) и широко известны как Рекомендации МСЭ-Т серии Q.700. Интеллектуальные сети, стандартизованные МСЭ, также относятся к SS7 (Рекомендации МСЭ-T Q.1200–Q.1699). В связи с ростом подвижной электросвязи ЕТСИ разработал протоколы MAP и CAP, которые также базируются на SS7 и пригодны для сухопутных подвижных сетей общего пользования (PLMN), например для сетей GSM. Кроме того, IETF опубликовала серию RFC, названную SIGTRAN, которая сделала возможным использование SS7 поверх IP-сетей.

SS7 была разработана так, чтобы находиться под управлением операторов, при том понимании что любой подсоединившийся к сети SS7 объект считается заслуживающим доверия. В современной сетевой среде, учитывая в том числе присоединение через интернет, базирующиеся на SS7 сети становятся уязвимыми и могут подвергаться атакам. В информационных материалах сообщалось о связанных с SS7 уязвимостях и проблемах безопасности, которые открывают возможность отслеживания местоположения пользователей и перехват их голосовой связи. Это подтвердили также некоторые операторы.

ИК11 МСЭ-Т исследует в настоящее время вопросы безопасности SS7, и данное мероприятие планируется как "мозговой штурм" для совместного поиска возможных действий по усилению механизмов обеспечения безопасности SS7.

**Задачи**

Перед семинаром-практикумом стоят следующие задачи:

• обмен информацией о проблемах безопасности SS7;

• анализ существующих стандартов SS7 и определение, какие из них затронуты;

• обсуждение путей совершенствования стандартов SS7 в аспекте безопасности;

• обсуждение предложений по усилению безопасности базирующихся на SS7 сетей в интересах пользователей и операторов;

• обсуждение сотрудничества с другими ОРС и организациями по вопросам безопасности SS7.

**Целевая аудитория**

К участию приглашаются члены и нечлены МСЭ. В частности, приветствуется участие операторов, продавцов, экспертов по безопасности, научно-исследовательских институтов и академических организаций, органов по стандартам, а также других аналогичных организаций.

**Перечень стандартов SS7 (не исчерпывающий)**

Рекомендации МСЭ-Т

− Рекомендации МСЭ-Т серии Q.700 (MTP, SCCP, TCAP, TUP, ISUP);

− Рекомендации МСЭ-Т Q.1200–Q.1699 (Интеллектуальные сети);

− Рекомендация МСЭ-Т Q.1912.5 (Взаимодействие между SIP-I и ISUP).

Спецификации ЕТСИ/3GPP

− 3GPP TS 09.02 (Прикладная подсистема подвижной связи, MAP);

− 3GPP TS 09.78, 3GPP TS 29.078 (Прикладная подсистема CAMEL, CAP).

RFC, выпущенные IETF

− RFC 4960, Протокол передачи с управлением потоком (SCTP);

− RFC 5133, Уровень адаптации пользователя ISDN (IUA);

− RFC 4165, Уровень адаптации пользователя (M2PA) подсистемы передачи сообщений 2 (MTP);

− RFC 3331, Уровень адаптации пользователя (M2UA) подсистемы передачи сообщений 2;

− RFC 4666, Уровень адаптации пользователя (M3UA) подсистемы передачи сообщений 3;

− RFC 3868, Уровень адаптации пользователя (SUA) подсистемы управления соединениями сигнализации (SCCP);

− RFC 3807, Уровень адаптации пользователя V5 (V5UA);

− RFC 4129, Уровень адаптации пользователя (DUA) DPNSS/DASS2.

**Веб-сайт**: <http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx>.

**2 Семинар-практикум МСЭ "**[**Борьба с контрафактной продукцией с использованием решений по проверке на соответствие и функциональную совместимость**](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Pages/default.aspx)**", 28 июня 2016 года (14 час. 00 мин. – 18 час. 00 мин.)**

**Введение**

В [Резолюции 188](http://www.itu.int/pub/S-CONF-ACTF-2014) (Пусан, 2014 г.) Полномочной конференции МСЭ "Борьба с контрафактными устройствами электросвязи/информационно‑коммуникационных технологий" содержится решение поручить Директорам трех Бюро оказывать содействие Государствам-Членам в решении проблем, связанных с контрафактными устройствами электросвязи/ИКТ, с помощью обмена информацией на региональном или глобальном уровне, в том числе систем оценки соответствия.

Кроме того, на состоявшемся в ноябре 2014 года семинаре-практикуме МСЭ "[Борьба с контрафактными и некачественными устройствами ИКТ](http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx)" были выявлены масштабы и негативные последствия проблемы контрафактной продукции, к которым относятся потери налоговых поступлений, роялти и других доходов; уменьшение уровня продаж, снижение цен и сокращение объема операций; подрыв ценности торгового знака, престижа и репутации; уменьшение стимулов для инноваций и инвестиций; сокращение занятости и темпов экономического роста; нарушение функционирования сетей и проблемы функциональной совместимости, приводящие к низкому качеству доставки и приема услуг; и риски для здоровья, безопасности и окружающей среды.

В качестве дальнейших шагов необходимо принять меры по борьбе с контрафактными продуктами ИКТ. В связи с этим [Вопрос 8 (В8) ИК11 МСЭ-Т](http://www.itu.int/en/ITU-T/studygroups/2013-2016/11/Pages/q8.aspx) в настоящее время возглавляет исследования для определения любых возможных технических решений для борьбы с контрафактными устройствами ИКТ. В рамках Вопроса 8 был опубликован [Технический отчет о контрафактных устройствах ИКТ](http://www.itu.int/pub/T-TUT-CCICT) и созданы новые направления работы, в том числе разработка проекта новой Рекомендации "[Основы для решения проблемы контрафактных устройств ИКТ](http://web.itu.int/ITU-T/workprog/wp_item.aspx?isn=10502)".

Кроме того, в МСЭ и повсюду в мире обсуждается вопрос о том, могут ли программы по оценке соответствия и проверке на функциональную совместимость стать одним из технических решений для борьбы с контрафактными устройствами ИКТ.

**Задачи**

Перед семинаром-практикумом стоят следующие задачи:

• предоставить информацию об исследованиях, проводимых в настоящее время в рамках Вопроса 8 ИК11 МСЭ-T, и, в частности, активизировать разработку технической Рекомендации "[Основы для решения проблемы контрафактных устройств ИКТ](http://web.itu.int/ITU-T/workprog/wp_item.aspx?isn=10502)";

• определить, могут ли программы по оценке соответствия и проверке на функциональную совместимость содействовать борьбе с контрафактными устройствами ИКТ;

• понять новые тенденции и механизмы, связанные с производством контрафактной продукции ИКТ, подделкой и/или дублированием уникальных идентификаторов устройств ИКТ;

• понять механизмы обеспечения безопасности управления цепочкой поставок (от производства до ввоза, распределения и сбыта) для обеспечения прослеживаемости и безопасности продукции и сетей, а также конфиденциальности и доверия людей;

• продолжить повышение информированности о проблеме контрафактных устройств ИКТ и связанных с ними опасностях; и

• просить экспертов из МСЭ и разных стран представить мнения, предложения и идеи о дальнейших исследованиях в течение следующего исследовательского периода.

**Целевая аудитория**

К участию приглашаются члены и нечлены МСЭ. В частности, приветствуется участие продавцов и производителей, научно-исследовательских институтов и академических организаций, лабораторий, регуляторных органов, операторов, НПО, таможенных органов и служб безопасности, органов по стандартам и оценке соответствия, а также других аналогичных организаций.

**Веб-сайт**: <http://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Pages/default.aspx>.

Желаю вам плодотворного и приятного собрания.

С уважением,

Чхе Суб Ли  
Директор Бюро  
стандартизации электросвязи