Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

ВСЕМИРНАЯ АССАМБЛЕЯ ПО СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ
Дубай, 20–29 ноября 2012 года

Резолюция 50 – Кибербезопасность

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за исследование технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, разрабатывают Рекомендации по этим темам.

© ITU 2013

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

РЕЗОЛЮЦИЯ 50 (Пересм. Дубай, 2012 г.)

Кибербезопасность

(Флорианополис, 2004 г.; Йоханнесбург, 2008 г.; Дубай, 2012 г.)

Всемирная ассамблея по стандартизации электросвязи (Дубай, 2012 г.),

напоминая

a) Резолюцию 130 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции о роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ);

b) Резолюцию 174 (Гвадалахара, 2010 г.) Полномочной конференции о роли МСЭ в связи с вопросами международной государственной политики, касающимися риска незаконного использования ИКТ;

c) Резолюцию 179 (Гвадалахара, 2010 г.) Полномочной конференции о роли МСЭ в защите ребенка в онлайновой среде;

d) Резолюцию 181 (Гвадалахара, 2010 г.) Полномочной конференции об определениях и терминологии, связанных с укреплением доверия и безопасности при использовании ИКТ;

e) резолюции 55/63 и 56/121 Генеральной Ассамблеи Организации Объединенных Наций, устанавливающие нормативно-правовые рамки для борьбы с неправомерным использованием информационных технологий в преступных целях;

f) резолюцию 57/239 Генеральной Ассамблеи Организации Объединенных Наций о создании глобальной культуры кибербезопасности;

g) резолюцию 58/199 Генеральной Ассамблеи Организации Объединенных Наций о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур;

h) резолюцию 41/65 Генеральной Ассамблеи Организации Объединенных Наций о принципах, касающихся дистанционного зондирования Земли из космоса;

i) Резолюцию 45 (Пересм. Хайдарабад, 2010 г.) Всемирной конференции по развитию электросвязи (ВКРЭ);

j) Резолюцию 52 (Пересм. Дубай, 2012 г.) настоящей Ассамблеи о противодействии распространению спама и борьбе со спамом; и

k) Резолюцию 58 (Пересм. Дубай, 2012 г.) настоящей Ассамблеи о поощрении создания национальных групп реагирования на компьютерные инциденты, в частности для развивающихся стран[1],

---

[1] К таковым относятся наименее развитые страны, малые островные развивающиеся государства, развивающиеся страны, не имеющие выхода к морю, а также страны с переходной экономикой.

учитывая

a) решающее значение инфраструктуры ИКТ практически для всех видов социально-экономической деятельности;

b) что традиционная коммутируемая телефонная сеть общего пользования (КТСОП) обладает определенным уровнем присущих ей защитных свойств в силу ее иерархической структуры и встроенных систем управления;

c) что IP-сети обеспечивают более низкий уровень разделения между пользовательскими и сетевыми компонентами, если не принимать надлежащие меры при проектировании защиты и сферы управления;

d) что, таким образом, претерпевающие конвергенцию традиционные сети и IP-сети в большей степени уязвимы в отношении вторжений, если не принимать надлежащие меры при проектировании защиты и сферы управления такими сетями;

e) что имеют место киберинциденты, создаваемые кибератаками, например, злонамеренными вторжениями или нападениями искателей острых ощущений, использующими вредоносные программные средства (такие как "черви" и вирусы), которые распространяются различными способами, например, через интернет и бот-инфицированные компьютеры;

f) что для того, чтобы защитить глобальные инфраструктуры электросвязи/ИКТ от угроз и проблем, связанных с меняющейся средой кибербезопасности, требуются согласованные действия на национальном, региональном и международном уровнях, чтобы обеспечить защиту от различных наносящих вред событий и реагировать на них;

g) что Сектор стандартизации электросвязи МСЭ (МСЭ-Т) должен играть определенную роль в рамках своего мандата и своей компетенции с учетом пункта *f)* раздела *учитывая*,

учитывая далее,

a) что Рекомендация МСЭ-Т X.1205 содержит определение, описание технологий и принципы защиты сетей;

b) что Рекомендация МСЭ-Т X.805 обеспечивает систематизированную основу для выявления уязвимых мест, а в Рекомендации МСЭ-Т X.1500 представлена модель обмена информацией о кибербезопасности (CYBEX) и рассматриваются методы, которые можно было бы использовать для содействия обмену информацией о кибербезопасности;

c) что МСЭ-Т и Объединенный технический комитет по информационным технологиям (ОТК1) Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК) уже имеют значительный объем опубликованных материалов и ими проводится работа, непосредственно связанная с этой темой, что необходимо учитывать,

признавая

a) соответствующие результаты Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), определившие МСЭ в качестве ведущей и содействующей организации для Направления деятельности С5 "Укрепление доверия и безопасности при использовании ИКТ";

b) что в разделе *решает* Резолюции 130 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции предусматривается усилить роль МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий, а также повысить интенсивность ведущейся в рамках существующих исследовательских комиссий МСЭ-Т работы первостепенной важности;

c) что Программа 2 по кибербезопасности, приложениям ИКТ и вопросам, связанным с сетями на основе IP, принятая на ВКРЭ (Хайдарабад, 2010 г.), включает кибербезопасность в качестве одного из своих приоритетных видов деятельности, а также соответствующую деятельность, осуществляемую Бюро развития электросвязи (БРЭ), и что Вопрос 22/1 Сектора развития электросвязи МСЭ (МСЭ-D) затрагивает проблему обеспечения безопасности информационно-коммуникационных сетей путем выявления передового опыта для развития культуры кибербезопасности, а также была принята Резолюция 45 (Пересм. Хайдарабад, 2010 г.) о механизмах совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним;

d) что Глобальная программа кибербезопасности (ГПК) МСЭ содействует международному сотрудничеству, целью которого является предложение стратегий для поиска решений по укреплению доверия и безопасности при использовании ИКТ,

признавая далее,

a) что возникают кибератаки, такие как фишинг, фарминг, скан/вторжение, распределенная атака типа отказ в обслуживании, искажение внешнего вида веб-сайта, несанкционированный доступ и пр., которые имеют серьезные последствия;

b) что ботнеты используются для распределения вредоносных бот-программ и осуществления кибератак;

c) что источники атак иногда трудно определить (например, атаки с использованием ложных IP-адресов);

d) что кибербезопасность является одним из элементов укрепления доверия и безопасности при использовании электросвязи/ИКТ;

e) что в соответствии с Резолюцией 181 (Гвадалахара, 2010 г.) Полномочной конференции признается важность исследования вопроса о терминологии, связанной с укреплением доверия и безопасности при использовании ИКТ, что в этот базовый перечень задач необходимо включить другие важные вопросы, в дополнение к кибербезопасности, и что в определение кибербезопасности, возможно, потребуется периодически вносить изменения, отражающие перемены в политике;

f) что в Резолюции 181 (Гвадалахара, 2010 г.) решено учитывать определение термина "кибербезопасность", которое принято в Рекомендации МСЭ-Т X.1205, в деятельности МСЭ-Т, связанной с укреплением доверия и безопасности при использовании ИКТ;

g) что, как признается в Резолюции 181 (Гвадалахара, 2010 г.), 17-я Исследовательская комиссия МСЭ-Т отвечает за разработку ключевых Рекомендаций по вопросам безопасности электросвязи и ИКТ,

отмечая

a) энергичные действия и заинтересованность в разработке стандартов и Рекомендаций в области безопасности электросвязи/ИКТ в 17-й Исследовательской комиссии, ведущей исследовательской комиссии МСЭ-Т по вопросам безопасности, и в других органах по стандартизации, включая Группу "Глобальное сотрудничество по стандартам" (ГСС);

b) что нужно обеспечить, по мере возможности, согласование национальных, региональных и международных стратегий и инициатив, чтобы избежать дублирования и использовать ресурсы оптимальным образом;

c) что сотрудничество и взаимодействие между организациями, занимающимися вопросами безопасности, может содействовать достижению положительных результатов и вносить вклад в укрепление и поддержание культуры кибербезопасности;

d) что, как признается в Резолюции 130 (Пересм. Гвадалахара, 2010 г.), в рамках 17-й Исследовательской комиссии изучается вопрос о национальных центрах информационной безопасности открытых сетей на базе IP для развивающихся стран и завершена определенная работа в этой области, в частности разработаны Рекомендации серии МСЭ-Т X.800 − МСЭ-Т X.849 и Добавления к ним,

решает,

1 что всем исследовательским комиссиям МСЭ-Т следует продолжать оценивать существующие и появляющиеся новые Рекомендации и в особенности Рекомендации относительно протоколов по сигнализации и электросвязи с точки зрения надежности их структуры и возможности использования злоумышленниками с целью разрушительного вторжения, способного помешать их внедрению в рамках глобальной инфраструктуры информационных сетей и сетей электросвязи, разрабатывать Рекомендации для появляющихся вопросов в области безопасности, а также принимать во внимание новые услуги и приложения, которые должны будут поддерживаться глобальной инфраструктурой электросвязи/ИКТ (например, облачные вычисления, "умные" электросети и интеллектуальные транспортные системы, которые базируются на сетях электросвязи/ИКТ);

2 что МСЭ-Т в рамках своей деятельности и своего влияния следует продолжать пропагандировать необходимость защищать информационные системы и системы электросвязи от угрозы кибератаки и продолжать содействовать сотрудничеству между соответствующими международными и региональными организациями с целью расширения обмена технической информацией в области безопасности информационных сетей и сетей электросвязи;

3 что МСЭ-Т должен тесно взаимодействовать с МСЭ-D, в частности в контексте Вопроса 22/1;

4 что при оценке уязвимости безопасности сетей и протоколов и содействии обмену информацией по кибербезопасности следует принимать во внимание и применять, в соответствующих случаях, Рекомендации МСЭ-Т, включая Рекомендации МСЭ-Т серии X и Добавления к ним, в частности МСЭ-Т X.805, МСЭ-Т X.1205, МСЭ-Т X.1500, стандарты ИСО/МЭК и другие соответствующие результаты деятельности других организаций;

5 что МСЭ-Т должен продолжить работу по разработке и совершенствованию терминов и определений в области укрепления безопасности и доверия при использовании электросвязи/ИКТ, включая термин "кибербезопасность";

6 что заинтересованным сторонам предлагается совместно работать над разработкой стандартов и руководящих принципов в целях защиты от кибератак и облегчения обнаружения источника атаки;

7 что следует содействовать глобальным согласованным и совместимым процессам обмена информацией, касающейся реагирования на инциденты;

8 что все исследовательские комиссии МСЭ-Т должны продолжать представлять отчеты по вопросам безопасности электросвязи/ИКТ для Консультативной группы по стандартизации электросвязи (КГСЭ) и о ходе работ по оценке существующих и разрабатываемых новых Рекомендаций;

9 что исследовательские комиссии МСЭ-Т должны продолжать поддерживать связи с организациями по разработке стандартов (ОРС) и другими органами, действующими в этой области, такими как ОТК1 ИСО/МЭК, Организация экономического сотрудничества и развития (ОЭСР), Рабочая группа по электросвязи и информации Азиатско-Тихоокеанского экономического сотрудничества (АТЭС-ТЕЛ), а также Целевая группа по инженерным проблемам интернета (IETF);

10 что 17-я Исследовательская комиссия должна продолжать свою работу по вопросам, поднятым в Резолюции 130 (Пересм. Гвадалахара, 2010 г.), а также касающимся Рекомендаций МСЭ-Т серии X, включая Добавления к ним, в зависимости от случая,

поручает Директору Бюро стандартизации электросвязи

1 подготовить перечень национальных, региональных и международных инициатив и деятельности на основе информационной базы, относящейся к "Дорожной карте по стандартам безопасности ИКТ", и на основе деятельности МСЭ-D в области кибербезопасности, а также с помощью других соответствующих организаций, чтобы содействовать в максимально возможной степени всемирному согласованию стратегий и подходов в этой чрезвычайно важной области;

2 ежегодно представлять отчет Совету МСЭ в соответствии с Резолюцией 130 (Пересм. Гвадалахара, 2010 г.) о прогрессе, достигнутом в рамках изложенной выше деятельности;

3 продолжать и далее признавать ту роль, которую играют другие организации, обладающие опытом и техническими знаниями в области стандартов безопасности, и координировать свою деятельность с этими организациями, в соответствующих случаях,

далее поручает Директору Бюро стандартизации электросвязи

1 продолжать осуществлять связанную с ВВУИО последующую деятельность в области укрепления доверия и безопасности при использовании ИКТ в сотрудничестве с соответствующими заинтересованными сторонами, что является одним из способов обмена информацией по национальным, региональным и международным инициативам по вопросам кибербезопасности, носящим недискриминационный характер на глобальном уровне;

2 сотрудничать с БРЭ по любым вопросам, касающимся кибербезопасности, в соответствии с Резолюцией 45 (Пересм. Хайдарабад, 2010 г.) ВКРЭ;

3 продолжать сотрудничать с Глобальной программой кибербезопасности (ГПК) Генерального секретаря, с ИМПАКТ, FIRST и с другими глобальными или региональными проектами в области кибербезопасности, в зависимости от случая, развивать отношения и партнерские связи с различными региональными и международными организациями и инициативами, занимающимися вопросами кибербезопасности, в зависимости от случая, и предложить всем Государствам-Членам, особенно развивающимся странам, принимать участие в этой деятельности и обеспечивать координацию между этими различными видами деятельности;

4 принимая во внимание Резолюцию 130 (Пересм. Гвадалахара, 2010 г.), работать во взаимодействии с Директорами других Бюро с целью оказания поддержки Генеральному секретарю в подготовке документа, касающегося возможного меморандума о взаимопонимании (МоВ) (согласно Резолюции 45 (Пересм. Хайдарабад, 2010 г.)) между заинтересованными Государствами-Членами, направленного на укрепление кибербезопасности и на борьбу с киберугрозами, чтобы защитить развивающиеся страны и любую страну, заинтересованную в присоединении к этому возможному МоВ,

предлагает Государствам-Членам, Членам Сектора, Ассоциированным членам и академическим организациям, в зависимости от обстоятельств,

сотрудничать и активно участвовать в выполнении настоящей Резолюции и в связанной с ней деятельности.