Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

ВСЕМИРНАЯ АССАМБЛЕЯ ПО СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ
Хаммамет, 25 октября – 3 ноября 2016 года

Резолюция 50 – Кибербезопасность

ПРЕДИСЛОВИЕ

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

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

РЕЗОЛЮЦИЯ 50 (Пересм. Хаммамет, 2016 г.)

Кибербезопасность

(Флорианополис, 2004 г.; Йоханнесбург, 2008 г.; Дубай, 2012 г.; Хаммамет, 2016 г.)

Всемирная ассамблея по стандартизации электросвязи (Хаммамет, 2016 г.),

напоминая

a) Резолюцию 130 (Пересм. Пусан, 2014 г.) Полномочной конференции о роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ);

b) Резолюцию 174 (Пересм. Пусан, 2014 г.) Полномочной конференции о роли МСЭ в связи с вопросами международной государственной политики, касающимися риска незаконного использования ИКТ;

c) Резолюцию 179 (Пересм. Пусан, 2014 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 (ГА ООН), устанавливающие нормативно-правовые рамки для борьбы с неправомерным использованием информационных технологий в преступных целях;

f) резолюцию 57/239 ГА ООН о создании глобальной культуры кибербезопасности;

g) резолюцию 58/199 ГА ООН о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур;

h) резолюцию 41/65 ГА ООН о принципах, касающихся дистанционного зондирования Земли из космоса;

i) резолюцию 70/125 ГА ООН об итоговом документе совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества;

j) Резолюцию 45 (Пересм. Дубай, 2014 г.) Всемирной конференции по развитию электросвязи (ВКРЭ) о механизмах совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним;

k) Резолюцию 52 (Пересм. Хаммамет, 2016 г.) настоящей Ассамблеи о противодействии распространению спама и борьбе со спамом;

l) Резолюцию 58 (Пересм. Дубай, 2012 г.) Всемирной ассамблеи по стандартизации электросвязи о поощрении создания национальных групп реагирования на компьютерные инциденты, в частности для развивающихся стран[1];

m) что МСЭ является ведущей содействующей организацией по Направлению деятельности С5 ВВУИО в Тунисской программе для информационного общества (Укрепление доверия и безопасности при использовании ИКТ);

n) касающиеся кибербезопасности положения итоговых документов ВВУИО,

учитывая

a) решающее значение инфраструктуры электросвязи/ИКТ и их приложений практически для всех видов социально-экономической деятельности;

---

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

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 кибербезопасность является сквозной темой, а среда кибербезопасности является сложной и разноплановой при наличии на национальном, региональном и глобальном уровнях многих различных заинтересованных сторон, которые несут ответственность за определение, рассмотрение вопросов, связанных с укреплением доверия и безопасности при использовании ИКТ, и решение этих вопросов;

f) что существенные и увеличивающиеся потери, которые несут пользователи систем электросвязи/ИКТ в связи с возрастающей во всем мире проблемой кибербезопасности, являются предметом тревоги для всех без исключения развитых и развивающихся стран мира;

g) что тот факт, среди прочих, что важнейшие инфраструктуры электросвязи/ИКТ взаимосвязаны между собой на глобальном уровне, означает, что низкий уровень безопасности инфраструктуры в одной стране может привести к большей степени уязвимости и риска в других странах, и что ввиду этого важно сотрудничество;

h) что увеличивается количество киберугроз и кибератак и появляются их новые методы, а также возрастает зависимость от интернета и других сетей, необходимых для получения доступа к услугам и информации;

i) что стандарты способны поддерживать аспекты безопасности интернета вещей (IoT) и "умных" городов и сообществ;

j) 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 для предотвращения инцидентов в сфере кибербезопасности, готовности к ним и реагирования на них, а также восстановления после них;

k) работу, предпринимаемую и проводимую в МСЭ, в том числе в 17-й Исследовательской комиссии МСЭ-Т, 2-й Исследовательской комиссии МСЭ-D, включая заключительный отчет по Вопросу 22/1-1 1-й Исследовательской комиссии МСЭ-D, и по Дубайскому плану действий, принятому ВКРЭ (Дубай, 2014 г.);

l) что Сектор стандартизации электросвязи МСЭ (МСЭ-Т) должен играть определенную роль в рамках своего мандата и своей компетенции с учетом пункта *j)* 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), а также ряд консорциумов и объединений по разработке стандартов, таких как Консорциум World Wide Web (W3C), Организация по развитию стандартов структурированной информации (OASIS), Целевая группа по инженерным проблемам интернета (IETF) и Институт инженеров по электротехнике и радиоэлектронике (IEEE), среди прочих, уже имеют значительный

объем опубликованных материалов и ими проводится работа, непосредственно связанная с этой темой, что необходимо учитывать;

d) значение текущей работы в области эталонной архитектуры безопасности для управления жизненным циклом данных по электронной коммерции,

признавая,

a) что в пункте постановляющей части Резолюции 130 (Пересм. Пусан, 2014 г.) Директору Бюро стандартизации электросвязи (БСЭ) поручается повысить интенсивность ведущейся в рамках существующих исследовательских комиссий МСЭ-Т работы;

b) что ВКРЭ-14 утвердила вклад в Стратегический план Союза на 2016–2019 годы, поддержав пять задач, в том числе Задачу 3 – *Повышать доверие и безопасность при использовании электросвязи/ИКТ, а также при развертывании приложений и услуг ИКТ*; и связанный с ней Намеченный результат деятельности 3.1 – *Укрепление доверия и безопасности при использовании ИКТ*, в рамках которой выполняются Программа в области кибербезопасности и Вопрос 3/2 МСЭ-D;

c) 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, принимая во внимание аспекты безопасности на протяжении всего жизненного цикла в ходе процесса разработки стандартов;

d) вызовы, с которыми сталкиваются государства, особенно развивающиеся страны, в связи с укреплением 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;

d) отмечая, что для борьбы с важнейшими угрозами кибербезопасности применительно к программному и аппаратному обеспечению может требоваться своевременное управление уязвимостями и своевременное обновление аппаратного и программного обеспечения;

e) что обеспечение безопасности данных является одним из ключевых компонентов кибербезопасности, поскольку данные зачастую являются мишенью кибератак;

f) что кибербезопасность является одним из элементов укрепления доверия и безопасности при использовании электросвязи/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 управления определением идентичности, 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) значительные совместные усилия со стороны правительств, частного сектора, гражданского общества, технического сообщества и академических организаций в рамках их соответствующих функций и обязанностей, а также между ними, по укреплению доверия и безопасности при использовании ИКТ,

решает

1 продолжать уделять этой работе в рамках МСЭ-Т первостепенное значение в соответствии с его компетенцией и специальными знаниями и опытом, в том числе содействовать достижению общего понимания среди правительств и других заинтересованных сторон вопросов укрепления доверия и безопасности при использовании ИКТ на национальном, региональном и международном уровнях;

2 что всем исследовательским комиссиям МСЭ-Т следует продолжать оценивать существующие и появляющиеся новые Рекомендации с точки зрения надежности их структуры и возможности использования злоумышленниками, и принимать во внимание новые услуги и появляющиеся приложения, которые должны поддерживаться глобальной инфраструктурой электросвязи/ИКТ (в том числе, например, облачными вычислениями и IoT, которые базируются на сетях электросвязи/ИКТ), в соответствии с их мандатами, установленными в Резолюции 2;

3 что МСЭ-Т в рамках своего мандата и своей компетенции следует продолжать пропагандировать необходимость укреплять и защищать информационные системы и системы электросвязи от киберугроз и кибератак и продолжать содействовать сотрудничеству между соответствующими международными и региональными организациями с целью расширения обмена технической информацией в области безопасности информационных сетей и сетей электросвязи;

4 что МСЭ-Т должен тесно взаимодействовать с МСЭ-D, в частности в контексте Вопроса 3/2 (Защищенность сетей информации и связи: Передовой опыт по созданию культуры кибербезопасности) МСЭ-D;

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

7 что 17-й Исследовательской комиссии, в тесном сотрудничестве со всеми другими исследовательскими комиссиями МСЭ-Т, следует разработать план действий для оценки существующих, изменяемых и новых Рекомендаций МСЭ-Т по противодействию уязвимостям в сфере безопасности и продолжать представлять отчеты по вопросам безопасности электросвязи/ИКТ для Консультативной группы по стандартизации электросвязи (КГСЭ);

8 что исследовательские комиссии МСЭ-Т должны продолжать поддерживать связи с организациями по разработке стандартов и другими органами, действующими в этой области;

9 что аспекты безопасности должны учитываться на протяжении всего процесса разработки стандартов МСЭ-Т,

поручает Директору Бюро стандартизации электросвязи

1 продолжать поддерживать и вести 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 вносить вклад в ежегодные отчеты Совету МСЭ по укреплению доверия и безопасности при использовании ИКТ, как указано в Резолюции 130 (Пересм. Пусан, 2014 г.);

3 представлять отчет Совету МСЭ о ходе работы по "Дорожной карте по стандартам безопасности ИКТ";

4 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;

5 продолжать осуществление и последующие меры в отношении соответствующих видов деятельности, связанной с ВВУИО, в области укрепления доверия и безопасности при использовании ИКТ в сотрудничестве с другими Секторами МСЭ и 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;

6 сотрудничать с ГПК Генерального секретаря 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;

7 оказывать поддержку Директору БРЭ в помощи Государствам-Членам в создании между развивающимися странами соответствующей структуры, которая позволяла бы оперативно реагировать на значительные инциденты, и предложить план действий, направленный на усиление их защиты с учетом механизмов и партнерств, в соответствующих случаях;

8 оказывать поддержку соответствующим видам деятельности исследовательских комиссий МСЭ-Т, связанным с укреплением и созданием доверия и безопасности при использовании ИКТ,

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

1 тесно взаимодействовать в рамках усиления регионального и международного сотрудничества, принимая во внимание Резолюцию 130 (Пересм. Пусан, 2014 г.) Полномочной конференции, с целью укрепления доверия и безопасности при использовании ИКТ для уменьшения рисков и угроз;

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

3 участвовать в соответствующих видах деятельности исследовательских комиссий МСЭ-Т по разработке стандартов и руководящих указаний по кибербезопасности в целях укрепления доверия и безопасности при использовании ИКТ;

4 применять соответствующие Рекомендации и Добавления МСЭ-Т.