|  |  |  |
| --- | --- | --- |
| itu_logo | **Всемирная ассамблея по стандартизации электросвязи (ВАСЭ-16) Хаммамет, 25 октября – 3 ноября 2016 года** | C:\Users\gaspari\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\logos-02.png |
|  |  |
| **ПЛЕНАРНОЕ ЗАСЕДАНИЕ** | **Пересмотр 1Документа 46(Add.19)-R** |
|  | **22 сентября 2016 года** |
|  | **Оригинал: английский** |
|  |
| Государства – члены Межамериканской комиссии по электросвязи (СИТЕЛ) |
| предлагаемые изменения к резолюции 50 васэ-12 – Кибербезопасность |
|  |
|  |

|  |  |
| --- | --- |
| **Резюме**: | В настоящем вкладе предлагаются редакционные поправки к Резолюции 50 (Пересм. Дубай, 2012 г.) для обновления текста в соответствии с Резолюцией 130 (Пересм. Пусан, 2014 г.) и Резолюцией 45 (Пересм. Дубай, 2014 г.). Эти поправки помогут обеспечить, чтобы данная резолюция отражала текущее состояние дел в мире в области укрепления доверия и безопасности при использовании ИКТ и чтобы вклад МСЭ-Т по этой теме соответствовал согласованным целям и приоритетам членского состава.  |

Введение

Информационно-коммуникационные технологии (ИКТ) являются неотъемлемой частью экономического и социального развития. Одним из важнейших элементов функционирования и использования ИКТ является безопасность, а для этого требуется, чтобы все заинтересованные лица были в курсе вопросов безопасности и действовали соответственно своей роли. Поскольку использование ИКТ продолжает расти, кибербезопасность остается одним из приоритетов для членского состава МСЭ. Последние четыре года 17-я Исследовательская комиссия МСЭ-Т продолжала свою работу в этой области, наряду со многими другими организациями и консорциумами по разработке стандартов, на национальном, региональном и международном уровнях. Кроме того, на Полномочной конференции МСЭ 2014 года и на Всемирной конференции по развитию электросвязи 2014 года были согласованы цели и приоритеты в области укрепления доверия и безопасности при использовании ИКТ, и ожидается, что МСЭ-Т внесет свой вклад в эту работу. В связи с этим СИТЕЛ считает целесообразным обновить Резолюцию 50 для того, чтобы она соответствовала таким изменениям.

Кибербезопасность заняла свое место в кругу проблем, вызывающих озабоченность экспертов, в том числе МСЭ, пользователей и, во многом, государств.

Со времени последней Ассамблеи и до сегодняшнего дня значение вопросов кибербезопасности не только сохранилось, но и увеличилось с точки зрения требуемого к ним внимания и участия со стороны сектора информационно-коммуникационных технологий. В связи с этим настоящая Резолюция, используемая в ней терминология и ее актуальность сохраняются в качестве одного из важнейших элементов для стандартизации и одного из значимых инструментов для Союза и его Членов.

В этом предложении о внесении изменений Аргентинская Республика считает, что терминологию Резолюции необходимо сохранить, и, в свою очередь, предлагает обновить ее, чтобы включить новые касающиеся кибербезопасности элементы, возникающие в связи с тенденциями в некоторых появляющихся областях и в основном с новыми угрозами. Кроме того, мы предлагаем включить элементы, связанные с последней по времени Всемирной конференцией по развитию электросвязи (ВКРЭ-14), которая утвердила вклад МСЭ-D в Стратегический план МСЭ на 2016−2019 годы, одобрив пять Задач, в том числе Задачу 3 – Повышать доверие и безопасность при использовании электросвязи/ИКТ, а также при развертывании соответствующих приложений и услуг; и Конечный результат 3.1 этой Задачи: Укрепление доверия и безопасности при использовании ИКТ и услуг, в рамках которых выполняется Программа в области кибербезопасности.

Среди таких элементов и новых появляющихся областей мы можем упомянуть возросшую ценность пользователей и/или устройств для злоумышленников, поскольку степень физического присоединения и обмена информацией увеличивается, что приводит к появлению новых областей использования, таких как электронный банкинг, аффидавиты и, в основном, приложения смартфонов.

Аналогичным образом, нынешний прогресс и развитие интернета вещей создают широкие перспективы для различных устройств и видов деятельности, но в то же время и увеличивают угрозы.

Предложение

СИТЕЛ предлагает внести изменения в Резолюцию 50 (Пересм. Дубай, 2012 г.) для обновления текста в соответствии с Резолюцией 130 (Пересм. Пусан, 2014 г.) и Резолюцией 45 (Пересм. Дубай, 2014 г.), а также чтобы отразить текущее состояние дел в мире в области укрепления доверия и безопасности при использовании ИКТ.

MOD IAP/46A19/1

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, 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. Дубай, 2014 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]](#footnote-1)1,

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

*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 для выявления инцидентов в сфере кибербезопасности, подготовки к ним, их устранения и восстановления после таких инцидентов;

*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,

*а)* что Рекомендация МСЭ-Т Х.1205 содержит определение, описание технологий и принципы защиты сетей;

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

*с)* что МСЭ-Т и Объединенный технический комитет по информационным технологиям (ОТК1) Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК), а также некоторые консорциумы и органы по стандартам, такие, например, как консорциум World Wide Web (W3C), Организация по развитию стандартов структурированной информации (OASIS), Целевая группа по инженерным проблемам интернета и Институт инженеров по электротехнике и радиоэлектронике, уже имеют значительный объем опубликованных материалов и ими проводится работа, непосредственно связанная с этой темой, что необходимо учитывать,

признавая

*а)* 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. Пусан, 2014 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;

*с)* что ВКРЭ-14 утвердила вклад в Стратегический план МСЭ на 2016−2019 годы, одобрив пять Задач, в том числе Задачу 3 – *Повышать доверие и безопасность при использовании электросвязи/ИКТ, а также при развертывании соответствующих приложений и услуг*; и Конечный результат 3.1 этой Задачи: *Укрепление доверия и безопасности при использовании ИКТ и услуг*, в рамках которых выполняются Программа в области кибербезопасности и Вопрос 3/2 Сектора развития электросвязи МСЭ (МСЭ-D);

*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,

*а)* что векторы кибератак, такие как фишинг, фарминг, скан/вторжение, распределенная атака типа отказ в обслуживании, искажение внешнего вида веб-сайта, несанкционированный доступ и пр., 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‑T 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

*а)* 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;

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

*d)* значительные совместные усилия со стороны правительств, частного сектора, гражданского общества, технического сообщества и академических организаций, а также между ними, по укреплению доверия и безопасности при использовании информационно-коммуникационных технологий,

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 укрепления и защиты информационных систем и систем 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;

3 что МСЭ-Т должен тесно взаимодействовать с МСЭ-D, в частности в контексте Вопроса 3/2;

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 Х и Добавления к ним, в частности МСЭ-Т Х.805, МСЭ-Т Х.1205, МСЭ-Т Х.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 киберугроз и 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. Пусан, 2014 г.), а также касающимся Рекомендаций МСЭ‑Т серии Х, включая Добавления к ним, в зависимости от случая,

поручает Директору Бюро стандартизации электросвязи

1 продолжать 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 ежегодно представлять отчет Совету МСЭ в соответствии с Резолюцией 130 (Пересм. Пусан, 2014 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. Дубай, 2014 г.) ВКРЭ;

3 принимая во внимание Резолюцию 45 (Пересм. Дубай, 2014 г.), оказывать содействие региональным и глобальным проектам в области кибербезопасности, таким, например, как FIRST, OAS, APCERT, LAC-CSIRT, и предложить всем странам, в особенности развивающимся странам, принять участие в данной деятельности,

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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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. [↑](#footnote-ref-1)