|  |  |  |  |
| --- | --- | --- | --- |
| 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** | | **Дополнительный документ 13 к Документу 44-R** | |
|  | | **3 октября 2016 года** | |
|  | | **Оригинал: английский** | |
|  | | | |
| Администрации стран – членов Азиатско-Тихоокеанского сообщества электросвязи | | | |
| предлагаемое изменение резолюции 50 васэ‑12 − Кибербезопасность | | | |
|  | | | |
|  | | | |

|  |  |
| --- | --- |
| **Резюме**: | В настоящем документе администрации стран – членов Азиатско-Тихоокеанского сообщества электросвязи предлагают изменения к Резолюции 50. |

Введение

Со времени проведения ВАСЭ-12 МСЭ-T добился успеха в деятельности, связанной с кибербезопасностью. В обстановке, связанной с угрозами кибербезопасности, произошли некоторые изменения. Необходимо активизировать деятельность и изучить возникающие вопросы безопасности в следующем исследовательском периоде (2017−2020 годы).

Необходимо обновить Резолюцию 50 для отражения изменений и тенденций, появившихся с 2012 года.

Предложение

Администрации стран – членов АТСЭ хотели бы предложить поправки к Резолюции 50 по кибербезопасности, представленные в Приложении.

MOD APT/44A13/1

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

*c)* соответствующие резолюции Генеральной Ассамблеи Организации Объединенных Наций, в том числе резолюцию 57/239, резолюцию 58/199 и резолюцию 64/211, о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур;

*d)* 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;

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

*f)* 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 и их приложений практически для всех видов социально-экономической деятельности, в том числе для новых тенденций, таких как четвертая промышленная революция (ЧПР) и интернет вещей;

*b)* что увеличивается количество киберугроз и кибератак, а также возрастает зависимость от интернета и других сетей, необходимых для получения доступа к услугам и информации;

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

*d)* что Сектор стандартизации электросвязи МСЭ (МСЭ-T) принял около 300 стандартов, касающихся укрепления доверия и безопасности при использовании ИКТ;

*e)* заключительный отчет по Вопросу 22-1/1 (Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности) Сектора развития электросвязи МСЭ (МСЭ-D);

*f)* что работа по стандартизации по вопросам безопасности, связанным с приложениями интернета вещей (IoT) и "умных" городов и сообществ (SCC), оказывает воздействие на безопасность пользователей интернета;

*g)* 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 случаев нарушения безопасности, готовности к ним и реагирования на них, а также восстановления после них, и что МСЭ-Т играет в связи с этим определенную роль в рамках своего мандата и своей компетенции;

*h)* динамичный характер глобальной экономики, где предложение электронного и компьютерного оборудования от экосистемы поставщиков во многом носит разрозненный характер и оказывает решающее влияние на управление угрозами кибербезопасности;

*i*) работу, предпринимаемую и проводимую в МСЭ, в том числе в 17‑й Исследовательской комиссии МСЭ-T, 2-й Исследовательской комиссии МСЭ-D и по Дубайскому плану действий, принятому ВКРЭ (Дубай, 2014 г.);

*j)* что Сектор стандартизации электросвязи МСЭ (МСЭ-Т) должен играть определенную роль в рамках своего мандата и своей компетенции в укреплении доверия и безопасности при использовании ИКТ и с учетом пункта *g)* 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) уже имеют значительный объем опубликованных материалов и ими проводится работа, непосредственно связанная с этой темой, что необходимо учитывать,

отдавая себе отчет в том,

*a)* что МСЭ-T и другие международные организации в рамках различных видов деятельности анализируют вопросы, относящиеся к укреплению доверия и безопасности при использовании ИКТ, включая стабильность и меры по борьбе со спамом, вредоносным программным обеспечением, контрафактными устройствами и т. п., и по защите информации, позволяющей установить личность;

*b)* что 17-я Исследовательская комиссия МСЭ-Т, 1-я и 2-я Исследовательские комиссии МСЭ-D и другие соответствующие исследовательские комиссии МСЭ продолжают работать над техническими средствами обеспечения безопасности информационных сетей и сетей связи в соответствии с Резолюциями 50 и 52 (Пересм. Дубай, 2012 г.) и Резолюциями 45 и 69 (Пересм. Дубай, 2014 г.);

*с)* что МСЭ-Т также помогает развивающимся странам в укреплении доверия и безопасности при использовании ИКТ и поддерживает создание CIRT, в том числе групп CIRT, ответственных за межправительственное сотрудничество, и важность координации усилий всех соответствующих организаций в соответствии с Резолюцией 58 (Пересм. Дубай, 2012 г.),

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" и вновь подтвержденные заседанием высокого уровня Генеральной Ассамблеи ООН по общему обзору выполнения решений ВВУИО в декабре 2015 года;

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

*с)* 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 характер и виды случаев нарушения кибербезопасности многочисленны и разнообразны (к ним, в том числе, относятся атаки методами социальной инженерии, целенаправленные устойчивые угрозы и т. п.) и продолжают со временем меняться, а также что источники кибератак порой сложно выявить;

*b)* что угрозы кибербезопасности возникают в связи с уязвимостями в коде, программном и аппаратном обеспечении, которые могут оказывать решающее влияние на национальную инфраструктуру и даже причинять вред жизни человека, вследствие чего требуется своевременное управление уязвимостями и при необходимости произведение корректировок программного/аппаратного обеспечения;

*c)* что данные становятся основными ресурсами сетей передачи информации и сетей электросвязи, а также основной мишенью атак на кибербезопасность,

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 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;

*с)* что МСЭ-D может играть определенную роль в оказании развивающимся странам помощи в деятельности по созданию потенциала в области кибербезопасности в соответствии с конкретными условиями и потребностями каждой страны;

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

решает,

1 продолжать уделять этой работе в рамках МСЭ-Т высокий приоритет 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, изменяемые и новые Рекомендации в отношении надежности их структуры и возможности их использования злоумышленниками, в частности инфраструктуры новых услуг и приложений (включая, в том числе, аналитику больших данных, облачные вычисления, "умные" города, цифровые финансовые услуги, мобильные периферийные вычисления, квантовые вычисления, сети подвижной связи 5‑го поколения, электронное здравоохранение, интернет вещей, организацию сетей с программируемыми параметрами, виртуализацию сетевых функций, промышленный интернет, "умные" электросети и интеллектуальные транспортные системы, базирующиеся на таких сетях электросвязи/ИКТ, как IMT-2020), которые должны поддерживаться глобальной инфраструктурой электросвязи/ИКТ, и по мере необходимости представлять отчеты КГСЭ;

3 что МСЭ-T следует начать исследования по стандартам, связанным с безопасностью больших данных, уделяя основное внимание стандартам и практике защиты данных на протяжении всего срока эксплуатации и оценки безопасности данных;

4 что МСЭ-Т в рамках своего мандата и своей компетенции 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;

5 что МСЭ-Т должен тесно взаимодействовать с МСЭ-D, в частности в контексте Вопроса 3/2, Передовой опыт в области защищенности сетей информации и связи: передовой опыт по созданию культуры кибербезопасности;

6 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";

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

8 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-T по уязвимостям в сфере безопасности и продолжать представлять отчеты по вопросам безопасности электросвязи/ИКТ для Консультативной группы по стандартизации электросвязи (КГСЭ);

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 исследовательским комиссиям МСЭ-T следует заниматься вопросами управления угрозами кибербезопасности, которое охватывает функции и обязанности поставщиков оборудования, поставщиков программного обеспечения, поставщиков услуг и конечных пользователей, при условии обеспечения эффективности управления киберугрозами и четкой многосторонней ответственности за уменьшение угроз кибербезопасности;

11 что 17-я Исследовательская комиссия должна продолжать свою работу по техническим средствам обеспечения безопасности сетей ИКТ, в частности по соответствующим темам, поднятым в Резолюции 130 (Пересм. Пусан, 2014 г.),

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 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 публиковать ежегодный отчет Совету МСЭ о ходе работы по "Дорожной карте по стандартам безопасности ИКТ", как указано в Резолюции 130 (Пересм. Пусан, 2014 г.), и оценивать эффективность текущей работы и плана будущих работ, ориентиров или дорожной карты;

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 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 БРЭ по любым вопросам, касающимся кибербезопасности, в частности выполнения Резолюции 45 (Пересм. Дубай, 2014 г.) ВКРЭ;

7 продолжать совместную работу в рамках Глобальной программы кибербезопасности (ГПК), в зависимости от случая, развивать отношения и партнерские связи с различными региональными и международными организациями и инициативами, занимающимися вопросами кибербезопасности;

8 поощрять сотрудничество с МСЭ-D в развитии системы и принципов управления кибербезопасностью для информирования Государств-Членов;

9 определять и документально оформлять практические меры по укреплению безопасности при использовании ИКТ на международном уровне, основываясь на широко распространенных практике, руководящих указаниях и рекомендациях, которые Государства-Члены могут решить применять в целях расширения своих возможностей по борьбе с киберугрозами и атаками и усиления международного сотрудничества в деле укрепления доверия и безопасности при использовании ИКТ, и учитывая Глобальную программу кибербезопасности (ГПК) МСЭ, а также в рамках имеющихся финансовых ресурсов,

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 совместно работать над разработкой стандартов и руководящих указаний в области кибербезопасности для защиты от кибератак;

4 использовать соответствующие Рекомендации МСЭ-Т, в частности серию Х Рекомендаций МСЭ-Т и Добавления к ней.

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

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)