|  |  |  |
| --- | --- | --- |
| 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 24к Документу 42-R** |
|  | **10 октября 2016 года** |
|  | **Оригинал: английский** |
|  |
| Администрации Африканского союза электросвязи |
| предлагаемое изменение резолюции 50 – Кибербезопасность |
|  |
|  |

|  |  |
| --- | --- |
| **Резюме**: | В настоящем вкладе предлагается внести поправки в Резолюцию 50 с целью просить о разработке Рекомендаций, технических документов и других публикаций, связанных с политикой, регуляторными и экономическими вопросами в области кибербезопасности и их влиянием, принимая во внимание возникающие технологии, включая большие данные, облачные вычисления и интернет вещей (IoT), а также перспективы использования Архитектуры цифровых объектов (DOA) для повышения кибербезопасности. |

# 1 Введение

Принимая во внимание, что существенные и возрастающие потери, которые несут пользователи систем электросвязи/ИКТ в связи с возрастающей во всем мире проблемой кибербезопасности и умышленного саботажа, являются предметом тревоги для всех без исключения развитых и развивающихся стран мира, следует предпринять необходимые действия в направлении киберпространства, вызывающего больше доверия. Отмечается также, что важнейшие инфраструктуры электросвязи/ИКТ взаимосвязаны между собой на глобальном уровне, и это означает, что низкий уровень безопасности инфраструктуры в одной стране может привести к большей степени уязвимости и риска в других странах.

Существует необходимость в проведении соответствующих действий и принятии превентивных мер на международном уровне против ненадлежащего использования киберпространства, включая сети электросвязи/ИКТ, а также противодействия терроризму во всех его формах и проявлениях в киберпространстве, включая сети электросвязи/ИКТ.

Очевидна важность обеспечения безопасности, последовательности и стабильности сетей электросвязи/ИКТ, а необходимость защищать сети электросвязи/ИКТ от угроз и уязвимости, при обеспечении неприкосновенности частной жизни и защиты личной информации и личных сведений, является в высшей степени желательной целью.

Важно подчеркнуть роль МСЭ в обеспечении защиты детей и содействии их развитию, а также необходимость активизировать деятельность по защите детей и молодежи от растления и защищать их права в контексте электросвязи/ИКТ, подчеркивая, что наилучшее обеспечение интересов ребенка имеет первостепенное значение.

Следует отметить, что Архитектура цифровых объектов (DOA) и один из ее элементов ‒ Система обработки данных – могли бы повысить безопасность и конфиденциальность в киберпространстве.

# 2 Предложение

В соответствии с этим, в предлагаемых поправках к Резолюции 50 рассматриваются обсуждаемые выше вопросы, и мы предлагаем 3-й Исследовательской комиссии МСЭ-T продолжать свою работу по разработке Рекомендаций, технических документов и других публикаций, связанных с политикой, регуляторными и экономическими вопросами в области кибербезопасности и их влиянием, принимая во внимание возникающие технологии, включая большие данные, облачные вычисления и интернет вещей (IoT), а также настоятельно рекомендуем исследовательским комиссиям МСЭ-T продолжать взаимодействовать с другими ОРС и органами, включая Фонд DONA.

MOD AFCP/42A24/1

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;

*l)* что МСЭ играет ведущую содействующую роль по Направлению деятельности С5 Тунисской программы для информационного общества (Укрепление доверия и безопасности при использовании ИКТ);

*m)* относящиеся к кибербезопасности положения Тунисского обязательства и Тунисской программы;

*n)* что МСЭ и Управление Организации Объединенных Наций по наркотикам и преступности (ЮНОДК) подписали Меморандум о взаимопонимании (МоВ), направленный на укрепление доверия и безопасности при использовании ИКТ,

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

*f)* 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;

*g)* 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;

*h)* 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;

*i)* 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) 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 Программа 2 по кибербезопасности, приложениям ИКТ и вопросам, связанным с сетями на основе IP, принятая на ВКРЭ (Дубай, 2014 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. Дубай, 2014 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;

*e)* необходимость в проведении соответствующих действий и принятии превентивных мер на международном уровне против злоупотреблений при использовании киберпространства, включая сети электросвязи/ИКТ, необходимость противодействия терроризму во всех его формах и проявлениях в киберпространстве, включая сети электросвязи/ИКТ, важность безопасности, последовательности и стабильности сетей электросвязи/ИКТ, а также необходимость защищать сети электросвязи/ИКТ от угроз и уязвимости (пункт 45 Тунисской программы), при обеспечении неприкосновенности частной жизни и защиты личной информации и личных сведений;

*f)* роль МСЭ в деле защиты детей и содействия их развитию и что следует активизировать деятельность по защите детей и молодежи от растления и защищать их права в контексте электросвязи/ИКТ, подчеркивая, что наилучшее обеспечение интересов ребенка имеет первостепенное значение;

*g)* что в Рекомендации МСЭ-Т X.1255, основанной на архитектуре цифровых объектов (DOA), представлена структура обнаружения информации по управлению определением идентичности;

*h)* что система обработки данных, являющаяся компонентом архитектуры DOA, имеет много преимуществ, включая хранение дескрипторов в качестве иерархических идентификаторов с безопасным доступом к атрибутам, который должен быть авторизован; функции управления являются самостоятельными, а изменения контролируются путем использования инфраструктуры открытых ключей (PKI), которая также является самостоятельной функцией в этой системе, а доступ к системе обработки данных может быть подписан и подтвержден пользователем,

признавая далее,

*а)* 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‑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)* что, как признается в Резолюции 130 (Пересм. Пусан, 2014 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 Х.800 − МСЭ-Т Х.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 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 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), Целевая группа по инженерным проблемам интернета (IETF) и Управление нумерации цифровых объектов (DONA);

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;

11 что 3-я Исследовательская комиссия должна продолжать свою работу по разработке Рекомендаций, Технических документов и других публикаций, связанных с политикой, регуляторными и экономическими вопросами в области кибербезопасности и их влиянием с учетом возникающих технологий, в том числе больших данных, облачных вычислений и интернета вещей (IoT),

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. 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.);

3 продолжать сотрудничать с Глобальной программой кибербезопасности (ГПК) Генерального секретаря, c 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. Пусан, 2014 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. Дубай, 2014 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.

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

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)