|  |  |  |
| --- | --- | --- |
| C:\Users\ponder\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\BDT-25th_anniversary_2017-Logo_411959-3_transparent.png | **Всемирная конференция по развитию электросвязи 2017 года (ВКРЭ-17)**  **Буэнос-Айрес, Аргентина, 9–20 октября 2017 года** | C:\Users\murphy\Documents\WTDC17\bd_R_25Years_Horizontal-411959.jpg |
|  | |  |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | | **Дополнительный документ 15 к Документу WTDC-17/21-R** |
|  | | **18 сентября 2017 года** |
|  | | **Оригинал: английский** |
| Арабские государства | | |
| предложения для работы конференции | | |
|  | | |
|  | | |
| **Приоритетная область**: − Резолюции и Рекомендации | | |

**MOD** ARB/21A15/1

РЕЗОЛЮЦИЯ 45 (Пересм. буэнос-айрес, 2017 г.)

Механизмы совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним

Всемирная конференция по развитию электросвязи (Буэнос-Айрес, 2017 г.),

напоминая

*a)* Статьи 6 и 7 Регламента международной электросвязи (РМЭ) МСЭ;

*b)* Резолюцию 130 (Пересм. Пусан, 2014 г.) Полномочной конференции "Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий";

*c)* Резолюцию 174 (Пересм. Пусан, 2014 г.) Полномочной конференции "Роль МСЭ в связи с вопросами международной государственной политики, касающимися риска незаконного использования информационно-коммуникационных технологий";

*d)* Резолюцию 179 (Пересм. Пусан, 2014 г.) Полномочной конференции "Роль МСЭ в защите ребенка в онлайновой среде";

*e)* Резолюцию 181 (Пересм. Пусан, 2014 г.) Полномочной конференции "Определения и терминология, связанные с укреплением доверия и безопасности при использовании информационно-коммуникационных технологий";

*f)* Резолюцию 45 (Пересм. Дубай, 2014 г.) Всемирной конференции по развитию электросвязи (ВКРЭ);

*g)* Резолюцию 50 (Пересм. Хаммамет, 2016 г.) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) "Кибербезопасность";

*h)* Резолюцию 52 (Пересм. Хаммамет, 2016 г.) ВАСЭ "Противодействие распространению спама и борьбе со спамом";

*i)* Резолюцию 58 (Пересм. Дубай, 2012 г.) ВАСЭ "Поощрение создания национальных групп реагирования на компьютерные инциденты, в частности для развивающихся стран";

*j)* Резолюцию 61 (Пересм. Дубай, 2012 г.) ВАСЭ о противодействии неправомерному присвоению и использованию ресурсов нумерации международной электросвязи и борьбе с неправомерным присвоением и использованием";

*k)* Резолюцию 69 (Пересм. Дубай, 2014 г.) настоящей Конференции "Создание национальных и региональных групп реагирования на компьютерные инциденты, в частности в развивающихся странах, и сотрудничество между ними";

*l)* Резолюцию 67 (Пересм. Дубай, 2014 г.) настоящей Конференции "Роль Сектора развития электросвязи МСЭ в защите ребенка в онлайновой среде";

*m)* Резолюцию 78 (Дубай, 2014 г.) ВКРЭ о создании потенциала для противодействия неправомерному присвоению телефонных номеров в соответствии с Рекомендацией МСЭ-T E.164;

*n)* благородные принципы, цели и задачи, воплощенные в Уставе Организации Объединенных Наций и во Всеобщей декларации прав человека;

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

*p)* относящиеся к кибербезопасности положения Тунисского обязательства и Тунисской программы, а также Итоговый документ совещания высокого уровня ГА ООН по общему обзору выполнения решений ВВУИО;

*q)* цель Стратегического плана Союза на 2016−2019 годы, утвержденного в Резолюции 71 (Пересм. Пусан, 2014 г.) Полномочной конференции, в котором МСЭ-D признает важность международного сотрудничества в вопросах повышения надежности, доступности и безопасности при использовании ИКТ;

*r)* Вопрос 22 1-й Исследовательской комиссии Сектора развития электросвязи МСЭ (МСЭ-D), в работе по которому в течение прошлого исследовательского периода участвовали многие члены для составления отчетов, в том числе учебных материалов, предназначенных для использования в развивающихся странах, таких как сборник по национальному опыту, образцы передового опыта для партнерств государственного и частного секторов, образцы передового опыта по созданию групп реагирования на компьютерные инциденты‎ (CIRT) с сопроводительными учебными материалами и образцы передового опыта для основ управления группами CIRT;

*s)* Вопрос 3 2-й Исследовательской комиссии МСЭ-D, в рамках которого особое внимание уделяется защите сетей информации и связи и развитию культуры кибербезопасности и будет указано, что защищенные сети информации и связи неразрывно связаны с построением информационного общества и с социально-экономическим развитием всех стран;

*t)* что в Глобальной программе кибербезопасности (ГПК) МСЭ поощряется международное сотрудничество с целью предложения стратегий для решений по укреплению доверия и безопасности при использовании электросвязи/ИКТ;

*u)* 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)* роль электросвязи/ИКТ как эффективных инструментов содействия делу мира, безопасности и стабильности экономического развития, укрепления демократии, социальной сплоченности, надлежащего управления и верховенства права, а также необходимость противодействовать нарастающим проблемам и угрозам, возникающим в результате злоупотребления этими технологиями, в том числе в преступных и террористических целях, обеспечивая при этом соблюдение прав человека (см. также пункт 15 Тунисского обязательства);

*b)* необходимость обеспечения доверия и безопасности при использовании электросвязи/ИКТ путем укрепления основы для доверия (пункт 39 Тунисской программы) и необходимость того, чтобы правительства в сотрудничестве с другими заинтересованными сторонами в рамках своих соответствующих функций разработали необходимое законодательство, предусматривающее проведение расследования и уголовное преследование киберпреступности, на национальном уровне, и сотрудничали на региональном и международном уровнях с учетом существующих баз;

*c)* что разработанная ВВУИО+10 концепция ВВУИО на период после 2015 года определила, среди прочего, в качестве приоритетных областей, подлежащих рассмотрению при реализации концепции ВВУИО, следующее:

− укрепление доверия и безопасности при использовании ИКТ, в первую очередь по таким темам, как защита персональных данных, конфиденциальность, безопасность и устойчивость сетей;

− содействие культуре онлайновой безопасности и защищенности, расширение прав и возможностей пользователей и поощрение национальных, региональных и международных стратегий кибербезопасности для защиты пользователей, в том числе детей;

*d)* что в резолюции 64/211 Генеральной Ассамблеи Организации Объединенных Наций (ГА ООН) государствам-членам предлагается использовать, если и когда они сочтут это целесообразным, прилагаемый к этой Резолюции инструмент добровольной самооценки национальных усилий;

*e)* необходимость разработки Государствами-Членами национальных программ кибербезопасности, опирающихся на национальный план, партнерские отношения между частным и государственным секторами, прочную правовую основу, возможности управления, наблюдения за инцидентами, оповещения, реагирования и восстановления после них, а также на культуру информирования, используя в качестве ориентира отчеты о передовом опыте для разработки национального подхода к вопросам обеспечения кибербезопасности: основы управления для организации национальных мероприятий по обеспечению кибербезопасности, подготовленный в течение двух исследовательских периодов изучения Вопроса 22 1‑й Исследовательской комиссии МСЭ-D;

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

*g)* причины, предопределившие принятие настоящей Конференцией Резолюции 37 (Пересм. Дубай, 2014 г.) "Преодоление цифрового разрыва", принимая во внимание важность осуществления с участием многих заинтересованных сторон на международном уровне и направления деятельности, указанные в пункте 108 Тунисской программы, в том числе "Укрепление доверия и безопасности при использовании ИКТ";

*h)* результаты некоторых видов деятельности МСЭ, относящихся к кибербезопасности, особенно, среди прочего, виды деятельности, которые координирует Бюро развития электросвязи, в целях выполнения мандата МСЭ как содействующей организации в осуществлении Направления деятельности С5 (Укрепление доверия и безопасности при использовании ИКТ);

*i)* что различные организации из всех секторов общества совместно работают для обеспечения кибербезопасности электросвязи/ИКТ;

*j)* что Задача 3 МСЭ-D, которая установлена Стратегическим планом Союза на 2016‑2019 годы, содержащимся в Резолюции 71 (Пересм. Пусан, 2014 г.), нацелена на укрепление доверия и безопасности при использовании электросвязи/ИКТ, а также при разработке соответствующих приложений и услуг;

*k)* 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;

*l)* различная информация, материалы, передовой опыт и финансовые ресурсы, в зависимости от случая, доступны Государствам-Членам через национальные, региональные и другие соответствующие международные организации в соответствии с их конкретным функциями;

*m)* что результаты обследования по вопросам информированности о кибербезопасности, проведенного БРЭ и Вопросом 22-1/1 в предыдущем исследовательском периоде, показали, что наименее развитым странам требуется значительная помощь в этой области;

*n)* что в Глобальной программе кибербезопасности (ГПК) МСЭ поощряется международное сотрудничество с целью предложения стратегий для решений по укреплению доверия и безопасности при использовании электросвязи/ИКТ,

признавая,

*a)* что для смягчения последствий незаконного использования киберпространства на глобальном уровне, в частности в развивающихся странах, необходимо выработать коллективные превентивные меры;

*b)* что меры, принимаемые для обеспечения стабильности и безопасности сетей электросвязи/ИКТ, для защиты от киберугроз/киберпреступности и противодействия спаму, в том числе в виде голосовых сообщений и SMS в сетях подвижной телефонной связи, а также с использованием таких приемов, как Bip Call, фишинг, массовая рассылка SMS международного происхождения, должны обеспечивать защиту и соблюдение положений о неприкосновенности частной жизни и о свободе слова, которые содержатся в соответствующих частях Всеобщей декларации прав человека (см. также пункт 42 Тунисской программы) и [Международного пакта о гражданских и политических правах](http://unterm.un.org/DGAACS/EDP_DOC.nsf/8fa942046ff7601c85256983007ca4d8/ad0320763899550a85256a630081ac90?OpenDocument);

*c)* что в резолюции 68/167 ГА ООН "Право на неприкосновенность личной жизни в цифровой век" подтверждается, что те же права, которые человек имеет в офлайновой среде, должны также защищаться и в онлайновой среде, включая право на неприкосновенность личной жизни;

*d)* необходимость в проведении соответствующих действий и принятии превентивных мер, определяемых законодательством и направленных на борьбу со злоупотреблениями электросвязью/ИКТ, в соответствии с этическими аспектами информационного общества, предусмотренными в Женевских декларации принципов и плане действий (пункт 43 Тунисской программы), необходимость противодействия терроризму во всех его формах и проявлениях в сетях электросвязи/ИКТ при соблюдении прав человека и в соответствии с другими обязательствами по международному праву, которые упоминаются в п. 81 постановляющей части резолюции 60/1 Генеральной Ассамблеи ООН по итогам Всемирного саммита 2005 года, и 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, будь то посредством принятия законодательства, реализации совместных рамочных программ, использования передового опыта и применения саморегулируемых и технических мер торгово-промышленным сектором и пользователями (пункт 46 Тунисской программы);

*e)* что необходимо бороться с неправомерным присвоением и использованием ресурсов нумерации международной электросвязи, распределенных в соответствии с Рекомендацией МСЭ-T E.164, с целью предотвращения перемаршрутизации трафика, используемого для производства спама во всех его форматах;

*f)* необходимость эффективного противодействия вызовам и угрозам, возникающим в результате использования электросвязи/ИКТ, например в целях, которые несовместимы с задачами по поддержанию международной стабильности и безопасности и могут оказать негативное воздействие на целостность инфраструктуры в рамках отдельных государств в ущерб их безопасности, и совместной работы с целью предотвращения злоупотребления информационными ресурсами и технологиями в преступных, террористических, мошеннических и вводящих в заблуждение целях, соблюдая при этом права человека;

*g)* роль электросвязи/ИКТ 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;

*h)* стремление и решимость всех заинтересованных сторон построить ориентированное на интересы людей, открытое для всех и защищенное информационное общество, направленное на развитие на основе целей и принципов Устава Организации Объединенных Наций, международного права и принципа многосторонних отношений, соблюдая в полном объеме и поддерживая Всеобщую декларацию прав человека, с тем чтобы люди во всем мире могли создавать информацию и знания, иметь к ним доступ, пользоваться и обмениваться ими в полной безопасности, для того чтобы в полной мере раскрыть свой потенциал и реализовать согласованные на международном уровне цели и задачи в области развития, включая Цели развития тысячелетия;

*i)* положения пунктов 4, 5 и 55 Женевской декларации принципов и что свобода слова и свободный поток информации, идей и знаний благоприятствуют развитию;

*j)* что Тунисский этап ВВУИО явился уникальной возможностью для повышения уровня информированности о преимуществах, которые электросвязь/ИКТ могут дать человечеству, и о том, как они могут изменить деятельность, взаимоотношения и жизнь людей и, таким образом, укрепить уверенность в будущем при условии безопасного использования электросвязи/ИКТ, как показала реализация решений Встречи на высшем уровне;

*k)* что спам в виде голосовых сообщений и SMS в сетях подвижной связи представляет собой проблему и по-прежнему содержит угрозу для пользователей и сетей. Это явление отрицательно сказываться на клиентах и не способствует укреплению климата доверия в условиях цифровой экономики;

*l)* необходимость принять эффективные меры для решения существенной проблемы, связанной со спамом, о чем говорится в пункте 41 Тунисской программы, а также, в том числе, со спамом, киберпреступностью, вирусами, червями и сетевыми атаками с целью отказа в обслуживании;

*m)* необходимость эффективной координации деятельности по Программам и Вопросам МСЭ‑D;

*n)* значение сотрудничества и обмена информацией между регуляторными органами для противодействия спаму при передаче сообщений на мобильные устройства,

признавая далее,

*a)* что количество кибератак увеличивается, а сами они становятся все более изощренными, и в то же время растет наша зависимость от интернета и других сетей, необходимых для получения важнейших услуг и информации;

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

отмечая

*a)* продолжающуюся работу 17-й Исследовательской комиссии (Безопасность) Сектора стандартизации электросвязи МСЭ (МСЭ-Т) и других организаций по разработке стандартов по различным аспектам безопасности электросвязи/ИКТ и противодействию спаму;

*b)* что спам представляет собой важную проблему и по-прежнему содержит угрозу для пользователей, сетей и интернета в целом. Широко распространена практика использования спама в виде международных голосовых сообщений и SMS в подвижных сетях в мошеннических целях, приводящая к существенному оттоку твердой валюты из развивающихся стран;

*c)* что вопрос кибербезопасности следует решать на соответствующем национальном, региональном и международном уровнях;

*d)* что сотрудничество и совместная деятельность Государств-Членов, Членов Сектора и соответствующих заинтересованных сторон способствуют созданию и поддержанию культуры кибербезопасности,

решает

1 по-прежнему признавать кибербезопасность одним из приоритетных видов деятельности МСЭ и продолжать рассматривать в сфере своей основной компетенции вопрос обеспечения безопасности и укрепления доверия при использовании электросвязи/ИКТ путем повышения осведомленности, выявления передового опыта и разработки соответствующих учебных материалов в целях содействия созданию культуры кибербезопасности;

2 укреплять взаимодействие и сотрудничество, а также обмениваться информацией со всеми соответствующими международными и региональными организациями по вопросам, касающимся инициатив в области кибербезопасности и борьбы со спамом, в сферах компетенции МСЭ, учитывая необходимость в оказании помощи развивающимся странам;

3 разработать дорожную карту по кибербезопасности, в которой будут определены роли и обязанности Государств-Членов по борьбе с кибератаками,

поручает Директору Бюро развития электросвязи

1 продолжать организовывать в сотрудничестве с соответствующими организациями, в соответствующих случаях, совместно с Программами по Намеченным результатам деятельности Задачи 3, на основе вкладов членов и во взаимодействии с Директором Бюро стандартизации электросвязи (БСЭ), собраний Государств-Членов, Членов Сектора и других заинтересованных сторон для обсуждения путей и средств повышения кибербезопасности, противодействия спаму и борьбы с неправомерным использованием ресурсов нумерации;

2 продолжать в сотрудничестве с соответствующими организациями и заинтересованными сторонами проводить исследования по укреплению кибербезопасности в развивающихся странах на региональном и международном уровнях на основании четкого определения их потребностей, в первую очередь относящихся к использованию электросвязи/ИКТ, в том числе к защите детей и молодежи;

3 поддерживать инициативы Государств-Членов, особенно в развивающихся странах, касающиеся механизмов совершенствования сотрудничества в области кибербезопасности и борьбы со спамом;

4 помогать развивающимся странам в повышении их степени подготовленности, с тем чтобы обеспечить высокий уровень и эффективность безопасности их важнейших инфраструктур электросвязи/ИКТ;

5 оказывать поддержку Государствам-Членам в установлении нормативных актов по борьбе со спамом с целью предотвращения установки и эксплуатации платформ, рассылающих спам, в том числе в виде голосовых сообщений и SMS в сетях подвижной телефонной связи;

6 помогать Государствам-Членам в создании соответствующей структуры между развивающимися странами, позволяющей быстро обнаруживать и реагировать на значительные инциденты, и предложить план действий, направленный на усиление их защиты с учетом механизмов и партнерств, в соответствующих случаях;

7 сотрудничать с Директором БСЭ в целях выполнения настоящей Резолюции;

8 представить отчет о результатах выполнения настоящей Резолюции следующей ВКРЭ,

предлагает Генеральному секретарю в координации с Директорами Бюро радиосвязи, Бюро стандартизации электросвязи и Бюро развития электросвязи

1 представить отчет о МоВ между странами, а также о существующих формах сотрудничества, обеспечивая анализ их статуса, сферы применения, а также использования этих механизмов сотрудничества, с целью укрепления кибербезопасности и борьбы с киберугрозами и спамом, с тем чтобы обеспечить Государствам-Членам возможность определения необходимости в дополнительных меморандумах и механизмах;

2 оказывать содействие региональным и глобальным проектам в области кибербезопасности, таким, как, например ИМПАКТ, FIRST, OAS, APCERT, и предложить всем странам, в особенности развивающимся странам, принять участие в данной деятельности,

просит Генерального секретаря

1 незамедлительно приступить к обсуждению вопроса о разработке относящейся к кибербезопасности глобальной хартии с учетом работы, которая проводится в Секторах МСЭ;

2 довести настоящую Резолюцию до сведения следующей Полномочной конференции в целях рассмотрения и принятия необходимых мер, в соответствующих случаях;

3 представить отчет о результатах этой деятельности Совету и Полномочной конференции в 2018 году,

предлагает Государствам-Членам, Членам Сектора, Ассоциированным членам и академическим организациям

1 обеспечить необходимую поддержку осуществлению настоящей Резолюции и активно участвовать в ее осуществлении;

2 признать кибербезопасность, противодействие спаму и борьбу со спамом одной из высокоприоритетных задач и принять соответствующие меры, а также содействовать укреплению доверия и безопасности при использовании электросвязи/ИКТ на национальном, региональном и международном уровнях;

3 стимулировать поставщиков услуг защищаться от выявленных рисков, стремиться обеспечивать непрерывность предоставляемых услуг и уведомлять о нарушениях безопасности,

предлагает Государствам-Членам

1 создать соответствующую международную структуру, позволяющую быстро реагировать на значительные инциденты, и предложить план действий, направленный на предупреждение таких инцидентов и смягчение их последствий;

2 разработать на национальном и международном уровнях стратегии и средства для обеспечения защиты национальной важнейшей инфраструктуры, в том числе усиления способности к восстановлению инфраструктуры электросвязи/ИКТ.

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