|  |  |  |
| --- | --- | --- |
| Logo, company name  Description automatically generated | A close up of a sign  Description automatically generated**Всемирная конференция по развитию электросвязи (ВКРЭ-22)**  **Кигали, Руанда, 6–16 июня 2022 года** | |
|  | |  |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | | **Дополнительный документ 25 к Документу WTDC-22/24-R** |
|  | | **2 мая 2022 года** |
|  | | **Оригинал: английский** |
| Государства – члены Межамериканской комиссии по электросвязи (СИТЕЛ) | | |
| предложение о внесении изменений в Резолюцию 45 ВКРЭ о Механизмах совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним | | |
|  | | |
|  | | |
| **Приоритетная область**: − Резолюции и Рекомендации  Резюме  СИТЕЛ предлагает внести изменения в Резолюцию 45 ВКРЭ, повторно выдвигая предложения, представленные ВКРЭ-17, и дополняя их важными соображениями относительно использования результатов расчета Глобального индекса кибербезопасности для направления деятельности БРЭ и содействия обмену информацией. Предлагаемые изменения касаются постановляющей части Резолюции, и СИТЕЛ воздержалась от внесения каких-либо изменений в преамбулу. Предложение направлено на обновление Резолюции 45 ВКРЭ с учетом изменения ситуации и новых тенденций в этой области с момента последнего обновления Резолюции в 2014 году.  Ожидаемые результаты  ВКРЭ-22 предлагается рассмотреть и утвердить предложение, представленное в настоящем документе.  Справочные документы  Резолюция 45 ВКРЭ | | |

**MOD** IAP/24A25/1

РЕЗОЛЮЦИЯ 45 (Пересм. кигали, 2022 г.)

Механизмы совершенствования сотрудничества   
в области кибербезопасности

Всемирная конференция по развитию электросвязи (Кигали, 2022 г.),

напоминая

*a)* Резолюцию 130 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции "Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий";

*b)* Резолюцию 174 (Гвадалахара, 2010 г.) Полномочной конференции "Роль МСЭ в связи с вопросами международной государственной политики, касающимися риска незаконного использования информационно-коммуникационных технологий";

*c)* Резолюцию 179 (Гвадалахара, 2010 г.) Полномочной конференции "Роль МСЭ в защите ребенка в онлайновой среде";

*d)* Резолюцию 181 (Гвадалахара, 2010 г.) Полномочной конференции "Определения и терминология, связанные с укреплением доверия и безопасности при использовании информационно-коммуникационных технологий";

*e)* Резолюцию 45 (Пересм. Хайдарабад, 2010 г.) Всемирной конференции по развитию электросвязи (ВКРЭ);

*f)* Резолюцию 50 (Пересм. Дубай, 2012 г.) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) "Кибербезопасность";

*g)* Резолюцию 52 (Пересм. Дубай, 2012 г.) ВАСЭ "Противодействие распространению спама и борьбе со спамом";

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

*i)* 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";

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

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

*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)* цель Стратегического плана Союза на 2012−2015 годы, утвержденного в Резолюции 71 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции, в которой к Сектору развития обращен призыв оказывать содействие обеспечению доступности инфраструктуры и стимулировать создание благоприятной среды для развития, а также безопасного и защищенного использования инфраструктуры электросвязи/информационно-коммуникационных технологий (ИКТ);

*o)* 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;

*p)* отчет председателя Группы экспертов высокого уровня (HLEG) о Глобальной программе кибербезопасности (ГПК), созданной Генеральным директором МСЭ в соответствии с требованиями Направления деятельности С5 об укреплении доверия и безопасности при использовании ИКТ, и согласно Резолюции 140 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции о роли МСЭ в качестве единственной содействующей организации по Направлению деятельности С5 Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) и Резолюции 58 (Пересм. Дубай, 2012 г.) ВАСЭ о поощрениисоздания национальных групп CIRT, в частности для развивающихся стран;

*q)* 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 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;

*d)* 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;

*e)* 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;

*f)* 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";

*g)* 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);

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

*i)* что Задача 3 МСЭ-D, которая установлена Стратегическим планом Союза на 2012−2015 годы, содержащимся в Резолюции 71 (Пересм. Гвадалахара, 2010 г.), заключалась в содействии разработке стратегий, направленных на активизацию развертывания и обеспечение безопасного, защищенного и приемлемого в ценовом отношении использования приложений и услуг ИКТ в целях включения электросвязи/ИКТ в более широкую экономику и общество;

*j)* 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;

*k)* 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;

*l)* 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;

*m)* 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 меры, принимаемые для обеспечения стабильности и безопасности сетей электросвязи/ИКТ, для защиты от киберугроз/киберпреступности и противодействия спаму, 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;

*b)* 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;

*c)* 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);

*d)* 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 и террористических целях, соблюдая при этом права человека;

*e)* 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;

*f)* 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;

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

*h)* 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;

*i)* необходимость принять эффективные мерыдля 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;

*j)* необходимость эффективной координации деятельности по Программам и Вопросам 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;

*b)* что спам представляет собой важную проблему и по-прежнему содержит угрозу для пользователей, сетей и интернета в целом и что вопрос кибербезопасности следует решать на соответствующем национальном, региональном и международном уровнях;

*c)* 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 обмена им, а также разработки соответствующих учебных материалов и руководств 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, в сферах компетенции МСЭ, учитывая необходимость в оказании помощи развивающимся странам,

поручает Директору Бюро развития электросвязи

1 продолжать организовывать в сотрудничестве с соответствующими организациями, в соответствующих случаях, совместно с Программой по Намеченному результату деятельности 3.1 Задачи 3, на основе вкладов членов и во взаимодействии с Директором Бюро стандартизации электросвязи (БСЭ), собрания Государств-Членов, Членов Сектора и других заинтересованных сторон для обсуждения путей и средств повышения кибербезопасности;

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, включая новые и появляющиеся технологии, а также к защите детей и молодежи в онлайновой среде;

3 учитывать результаты расчета Глобального индекса кибербезопасности (GCI) для ориентирования инициатив БРЭ, связанных с кибербезопасностью, уделяя особое внимание потребностям развивающихся стран, выявленным в процессе определения GCI;

4 поддерживать инициативы Государств-Членов, особенно в развивающихся странах, касающиеся механизмов совершенствования сотрудничества в области кибербезопасности;

5 помогать развивающимся странам в повышении их степени подготовленности, с тем чтобы обеспечить высокий уровень и эффективность безопасности и устойчивости их важнейших инфраструктур электросвязи/ИКТ, в том числе путем проведения семинаров и курсов подготовки, направленных, помимо прочего, на содействие развитию кибергигиены;

6 помогать Государствам-Членам в создании соответствующей структуры между развивающимися странами, позволяющей быстро реагировать на значительные инциденты, в том числе оказывая содействие добровольному обмену информацией между заинтересованными органами, и предложить план действий, направленный на усиление их защиты с учетом механизмов и партнерств, в соответствующих случаях;

7 параллельно с работой по Вопросу 3/2 2-й Исследовательской комиссии МСЭ-D осуществлять сбор информации и обмен информацией, касающейся правил, политики и других мер, разработанных и/или реализуемых национальными регуляторными органами в сфере электросвязи и другими заинтересованными организациями в целях укрепления доверия и безопасности при использовании электросвязи/ИКТ;

8 сотрудничать с Директором БСЭ в целях выполнения настоящей Резолюции;

9 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, с тем чтобы обеспечить Государствам-Членам возможность определения необходимости в дополнительных меморандумах и механизмах;

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

2 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 принимать активное участие 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;

4 сотрудничать друг с другом на национальном уровне для активизации процесса выработки решений по обеспечению безопасности и устойчивости сетей,

предлагает Государствам-Членам

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

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

3 содействовать внутрисекторальному, межсекторальному и межучрежденческому обмену информацией об угрозах кибербезопасности, уязвимостях и соответствующих инцидентах на национальном, региональном и международном уровнях.

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