|  |  |
| --- | --- |
| **Полномочная конференция (ПК-22)** **Бухарест, 26 сентября – 14 октября 2022 г.** |  |
|  |  |
|  |  |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | **Дополнительный документ 5 к Документу 68-R** |
|  | **18 августа 2022 года** |
|  | **Оригинал: русский** |
|  | |
| Государства – Члены МСЭ, члены Регионального содружества в области связи (РСС) | |
| ПРЕДЛОЖЕНИЯ ПО ПЕРЕСМОТРУ РЕЗОЛЮЦИИ 130 | |
| УСИЛЕНИЕ РОЛИ МСЭ В УКРЕПЛЕНИИ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ | |
|  | |

|  |
| --- |
| Резюме  Выполняемые МСЭ работы по определению для Государств-Членов Глобального индекса кибербезопасности (GCI), несомненно, являются значительным вкладом в защиту интересов пользователей инфокоммуникационных сетей и систем во всем мире. В то же время представляется вероятным наличие определенных затруднений у развивающихся стран в части интерпретации результатов определения Глобального индекса кибербезопасности и принятия решений о дальнейшем совершенствовании с учетом имеющихся данных.  В этой связи является целесообразным расширить деятельность МСЭ в части популяризации расчетов Глобального индекса кибербезопасности и проведения широкого круга мероприятий по содействию во внедрении практических рекомендаций экспертов МСЭ.  В свою очередь, организация регулярной обратной связи по данному вопросу позволит МСЭ оценить результативность своей деятельности и подготовить почву для дальнейшего совершенствования методологии расчетов Глобального индекса кибербезопасности.  Также предлагается по тексту резолюции заменить слова "компьютерная безопасность" на "кибербезопасность".  Определение "компьютерная безопасность" не является в настоящее время исключительным и способным охватить все сферы применения информационно-коммуникационных технологий (серверные кластеры, сети интернета вещей, облачные платформы и т. д.).  Одним из элементов безопасного использования ИКТ является вопрос использования цифровой подписи. В настоящий момент механизмы доверия в части использования электронной подписи в значительной степени отличаются от страны к стране. Например, подтверждение полномочий предпринимателя в некоторых странах может осуществляться сертификатом, выданным предпринимателю как субъекту отношений, в других – как физическому лицу, а в третьих, требуется сертификат полномочий (атрибутивный сертификат) совместно с электронной подписью физического лица. Существенное различие способов реализации доверия на основе инфраструктуры открытого ключа от страны к стране создает значительные сложности для ведения предпринимательской деятельности.  Возможным путем разрешения такой ситуации стало бы ведение общего реестра аккредитованных удостоверяющих центров с соответствующей информацией Ведение общего реестра аккредитованных удостоверяющих центров с информацией об их сферах деятельности, используемых криптографических алгоритмах, идентификаторах и типах выдаваемых сертификатов в значительной степени способно упросить взаимоотношения между субъектами предпринимательской деятельности различных стран.  В связи с вышеуказанным РСС предлагает внести некоторые поправки в Резолюцию 130.  Необходимые действия  Полномочной конференции предлагается рассмотреть это предложение и внести необходимые изменения в Резолюцию 130 "Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий" ПК.  \_\_\_\_\_\_\_\_\_\_\_\_  Справочные документы  − |

MOD RCC/68A5/1

РЕЗОЛЮЦИЯ 130 (ПЕРЕСМ. БУХАРЕСТ, 2022 Г.)

Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий

Полномочная конференция Международного союза электросвязи (Бухарест, 2022 г.),

напоминая

*а)* о резолюции 68/198 Генеральной Ассамблеи Организации Объединенных Наций (ГА ООН) об использовании информационно-коммуникационных технологий (ИКТ) в целях развития;

*b)* о резолюции 71/199 ГА ООН о праве на неприкосновенность личной жизни в цифровой век;

*c)* о резолюции 68/243 ГА ООН о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности;

*d)* о резолюции 57/239 ГА ООН о создании глобальной культуры кибербезопасности;

*e)* о резолюции 64/211 ГА ООН о создании глобальной культуры кибербезопасности и оценке национальных усилий по защите важнейших информационных инфраструктур;

*f)* о Заявлении ВВУИО+10 о выполнении решений ВВУИО и разработанной ВВУИО+10 Концепции ВВУИО на период после 2015 года, принятых на мероприятии высокого уровня ВВУИО+10 (Женева, 2014 г.), которое координировалось МСЭ, было организовано совместно с другими учреждениями Организации Объединенных Наций на основе подготовительной платформы с участием многих заинтересованных сторон (МРР) и было открыто для всех заинтересованных сторон ВВУИО, одобренных Полномочной конференцией (Пусан, 2014 г.) и представленных ГА ООН для проведения общего обзора;

*g)* о резолюции 70/125 ГА ООН об итоговом документе совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений ВВУИО;

*h)* о Резолюции 174 (Пересм. Пусан, 2014 г.) Полномочной конференции о роли МСЭ в связи с вопросами международной государственной политики, касающимися риска незаконного использования ИКТ;

*i)* о Резолюции 179 (Пересм. Дубай, 2018 г.) настоящей Конференции о роли МСЭ в защите ребенка в онлайновой среде;

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

*k)* о Резолюции 196 (Пересм. Дубай, 2018 г.) настоящей Конференции о защите пользователей/потребителей услуг электросвязи;

*l)* о Резолюции 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;

*m)* о Резолюции 140 (Пересм. Дубай, 2018 г.) настоящей Конференции о роли МСЭ в выполнении решений ВВУИО и в общем обзоре их выполнения, проводимом ГА ООН;

*n)* о Резолюции 58 (Пересм. Дубай, 2012 г.) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) о поощрении создания национальных групп реагирования на компьютерные инциденты (CIRT), в частности для развивающихся стран[[1]](#footnote-1)1;

*o)* о Резолюции 67 (Пересм. Буэнос-Айрес, 2017 г.) ВКРЭ о роли Сектора развития электросвязи МСЭ (МСЭ-D) в защите ребенка в онлайновой среде;

*p)* о Резолюции 69 (Пересм. Буэнос-Айрес, 2017 г.) ВКРЭ о создании национальных групп CIRT, в частности в развивающихся странах, и сотрудничестве между ними;

*q)* что в Резолюции 1305 Совета МСЭ, принятой на его сессии 2009 года, защита, безопасность, целостность, жизнеспособность и устойчивость интернета определены как вопросы государственной политики, относящиеся к сфере компетенции МСЭ,

учитывая,

*a)* что координировавшееся МСЭ мероприятие высокого уровня ВВУИО+10 вновь подтвердило значение укрепления доверия и безопасности при использовании ИКТ, о чем говорится в соответствующих пунктах итоговых документов ВВУИО+10 (Женева, 2014 г.);

*b)* решающее значение информационно-коммуникационных инфраструктур и их применений для практически всех видов социально-экономической деятельности;

*c)* относящиеся к кибербезопасности положения Тунисского обязательства и Тунисской программы, а также итоговый документ совещания высокого уровня ГА ООН, посвященного общему обзору хода осуществления решений ВВУИО;

*d)* что при применении и развитии ИКТ возникали новые угрозы из различных источников, которые оказывали воздействие на доверие и безопасность при использовании ИКТ всеми Государствами-Членами, Членами Секторов и другими заинтересованными сторонами, включая всех пользователей ИКТ, а также воздействовали на сохранение мира и социально-экономическое развитие всех Государств-Членов; и что угрозы инфраструктуре, сетям и устройствам и их уязвимость продолжают создавать проблемы все большего масштаба, невзирая на национальные границы, в отношении безопасности для всех стран, в частности для развивающихся стран, при этом в данном контексте отмечаются усиление роли МСЭ в укреплении доверия и безопасности при использовании ИКТ и необходимость дальнейшего укрепления международного сотрудничества и создания потенциала, а также развития надлежащих существующих национальных, региональных и международных механизмов (например, соглашений, передового опыта, меморандумов о взаимопонимании и т. п.);

*e)* что Генеральному секретарю МСЭ было предложено поддержать другие глобальные и региональные проекты в области кибербезопасности, в зависимости от случая, и что всем странам, в частности развивающимся странам, предложено принять участие в их видах деятельности, актуальных для МСЭ;

*f)* Глобальную программу кибербезопасности (ГПК) МСЭ, которая поощряет международное сотрудничество с целью предложения стратегий для выработки решений по укреплению доверия и безопасности при использовании электросвязи/ИКТ;

*g)* что для защиты таких инфраструктур, решения этих проблем и противодействия этим угрозам требуются скоординированные действия на национальном, региональном и международном уровнях, направленные на предотвращение, подготовку, а также реагирование в связи с тем или иным инцидентом кибербезопасности и на восстановление после него со стороны органов государственного управления на национальном (включая создание национальных групп CIRT) и субнациональном уровнях, со стороны частного сектора, граждан и пользователей, в дополнение к международному и региональному сотрудничеству и координации, и что МСЭ должен играть ведущую роль в этой области в соответствии со своими мандатом и компетенцией;

*h)* что итерационный и основанный на оценке рисков подход к вопросам кибербезопасности позволяет разрабатывать и применять практические методы обеспечения кибербезопасности таким образом, который необходим для устранения постоянно меняющихся угроз и уязвимостей, и что обеспечение безопасности является непрерывным и итерационным процессом, который должен быть включен в процессы разработки и развертывания технологий и их приложений с самого начала и не прекращаться на протяжении всего их жизненного цикла;

*i)* необходимость постоянного развития новых технологий для обеспечения раннего обнаружения событий или инцидентов, ставящих под угрозу кибербезопасность, а также скоординированного и своевременного реагирования на них, или инцидентов с безопасностью компьютерных сетей, которые могут поставить под угрозу доступность, целостность и конфиденциальность важнейших инфраструктур в Государствах − Членах МСЭ, и необходимость разработки стратегий, которые сведут к минимуму воздействие таких инцидентов и снизят растущие риски и угрозы, которым подвергаются такие платформы;

*j)* что в резолюции 70/125 ГА ООН об итоговом документе совещания высокого уровня ГА ООН, посвященного общему обзору хода осуществления решений ВВУИО, признаются проблемы, с которыми сталкиваются государства, в особенности развивающиеся страны, в своей деятельности по укреплению доверия и безопасности при использовании информационно-коммуникационных технологий, и содержится призыв вновь сосредоточиться на наращивании потенциала, образовании, обмене знаниями и нормативной практике, поощрении сотрудничества между широким кругом заинтересованных сторон на всех уровнях и повышении осведомленности пользователей ИКТ, особенно из числа наиболее обездоленных и незащищенных;

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

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

*m)* заключительный отчет по Вопросу 3/2 МСЭ-D "Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности";

*n)* что характер среды стандартов кибербезопасности требует сотрудничества между МСЭ и другими национальными, региональными, глобальными и отраслевыми организациями;

*o)* что многие развивающиеся страны разрабатывают или реализуют национальные стратегии в области кибербезопасности;

*p)* что вопрос кибербезопасности приобрел весьма важное значение на международном уровне и что, вследствие этого, существенное значение имеет роль и участие Организации Объединенных Наций, а также ее соответствующих специализированных учреждений, таких как МСЭ, в укреплении доверия и безопасности при использовании ИКТ;

*q)* что всем заинтересованным сторонам отведены различные роли и обязанности в обеспечении доверия и безопасности при использовании ИКТ;

*r)* что некоторые малые и средние предприятия (МСП) сталкиваются с дополнительными проблемами при реализации практики обеспечения кибербезопасности,

признавая,

*a)* что кибербезопасность является одним из основополагающих элементов обеспечения защиты инфраструктуры электросвязи/ИКТ и необходимым фундаментом социального и экономического развития;

*b)* что развитие ИКТ имело и продолжает иметь решающее значение для роста и развития глобальной экономики, в том числе цифровой экономики, на основе безопасности и доверия;

*c)* что ВВУИО подтвердила большое значение укрепления доверия и безопасности при использовании ИКТ, чрезвычайную важность осуществления решений при участии многих заинтересованных сторон на международном уровне и разработала Направление деятельности С5 (Укрепление доверия и безопасности при использовании ИКТ), по которому МСЭ назван в Тунисской программе ведущей/содействующей организацией для этого направления деятельности и что Союз выполнял эту задачу в последние годы, например, в рамках ГПК;

*d)* что ВКРЭ-17 приняла План действий Буэнос-Айреса и его Задачу 2, в частности Намеченный результат деятельности 2.2 по укреплению доверия и безопасности при использовании ИКТ, в которой кибербезопасность определяется в качестве одного из приоритетных направлений деятельности Бюро развития электросвязи (БРЭ) и устанавливаются основные направления работы, которые должно осуществлять БРЭ; ВКРЭ-14 приняла Резолюцию 45 (Пересм. Дубай, 2014 г.) о механизмах совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним, в которой Генеральному секретарю предлагается довести Резолюцию до сведения следующей полномочной конференции с целью ее рассмотрения и принятия необходимых мер и представить отчет о результатах этих основных направлений работы Совету и Полномочной конференции в 2018 году, в соответствующих случаях; ВКРЭ‑17 также приняла Резолюцию 69 (Пересм. Буэнос-Айрес, 2017 г.) о содействии созданию национальных групп CIRT, в частности в развивающихся странах, и сотрудничестве между ними;

*e)* что в Декларации Буэнос-Айреса, принятой ВКРЭ-17, указано, что "укрепление доверия, уверенности и безопасности при использовании электросвязи/ИКТ, а также защита персональных данных являются приоритетными направлениями, при этом необходимы международное сотрудничество и координация между правительствами, соответствующими организациями, частными компаниями и объединениями для создания потенциала и обмена передовым опытом в целях разработки соответствующей государственной политики, правовых, регуляторных и технических мер, касающихся, в частности, защиты персональных данных, и что заинтересованным сторонам следует взаимодействовать в целях обеспечения надежности и безопасности сетей и услуг ИКТ";

*f)* что в целях поддержки создания национальных групп CIRT в Государствах-Членах, в которых существует необходимость в наличии таких групп и где они в настоящее время отсутствуют, ВАСЭ-16 приняла Резолюцию 58 (Пересм. Дубай, 2012 г.) о поощрении создания национальных групп CIRT, в частности в развивающихся странах, а ВКРЭ-17 приняла Резолюцию 69 (Пересм. Буэнос-Айрес, 2017 г.) о содействии созданию национальных групп CIRT, в том числе групп CIRT, ответственных за межправительственное сотрудничество, в частности в развивающихся странах, сотрудничестве между ними и о важности координации между всеми соответствующими организациями;

*g)* п. 15 Тунисского обязательства, где говорится: "Признавая принципы универсального и недискриминационного доступа всех стран к ИКТ, необходимость принятия во внимание уровня социально-экономического развития каждой страны и уважая ориентированные на развитие аспекты информационного общества, мы подчеркиваем, что ИКТ являются эффективным инструментом содействия делу мира, безопасности и стабильности, усиления демократии, социальной сплоченности, надлежащего управления и верховенства права на национальном, региональном и международном уровнях. ИКТ могут использоваться для содействия экономическому росту и развитию предприятий. Для достижения этих целей ключевое значение имеет развитие инфраструктуры, создание человеческого потенциала, информационная безопасность и безопасность сетей. Мы далее признаем необходимость эффективного противодействия проблемам и угрозам, возникающим в результате использования ИКТ 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. Необходимо предотвращать злоупотребление информационными ресурсами и технологиями в преступных и террористических целях и соблюдать права человека", и что после ВВУИО проблемы, возникающие в результате этого ненадлежащего использования ресурсов ИКТ, только продолжают возрастать;

*h)* что в ходе координировавшегося МСЭ мероприятия высокого уровня ВВУИО+10 был выявлен ряд проблем в реализации направлений деятельности ВВУИО, которые сохраняются до сих пор и которые будет необходимо решать в период после 2015 года;

*i)* что Государствам-Членам, в особенности развивающимся странам, при разработке соответствующих осуществимых правовых мер, касающихся защиты от киберугроз на национальном, региональном и международном уровнях, может потребоваться помощь МСЭ, в том что касается разработки технических и процедурных мер, направленных на защиту национальной инфраструктуры ИКТ, которая предоставляется по просьбе этих Государств-Членов, при этом отмечается, что существует ряд региональных и международных инициатив, в рамках которых этим странам может оказываться поддержка в разработке таких правовых мер;

*j)* Мнение 4 (Лиссабон, 2009 г.) Всемирного форума по политике в области электросвязи/ИКТ о совместных стратегиях по укреплению доверия и безопасности при использовании ИКТ;

*k)* соответствующие результаты работы ВАСЭ-16, а именно:

i) Резолюцию 50 (Пересм. Хаммамет, 2016 г.) о кибербезопасности;

ii) Резолюцию 52 (Пересм. Хаммамет, 2016 г.) о противодействии распространению спама и борьбе со спамом;

*l)* что защищенные и надежные сети будут укреплять доверие и поощрять обмен информацией и данными и их использование;

*m)* что повышение квалификации специалистов и создание потенциала играют ключевую роль в усилении защиты информационных сетей;

*n)* что Государства-Члены направляют усилия на улучшение институциональной среды;

*o)* что оценка и анализ рисков обеспечивают более глубокое понимание рисков в области кибербезопасности, с которыми сталкиваются организации, и способов их смягчения,

отдавая себе отчет в том,

*a)* что МСЭ 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 противодействию спаму, вредоносным программным средствам и т. п. и по защите персональных данных и неприкосновенности частной жизни;

*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. Хаммамет, 2016 г.) и Резолюциями 45 (Пересм. Дубай, 2014 г.) и 69 (Пересм. Буэнос-Айрес, 2017 г.);

*с)* что МСЭ должен играть основополагающую роль в укреплении доверия и безопасности при использовании ИКТ;

*d)* что 2-я Исследовательская комиссия МСЭ-D продолжает проводить исследования, предусмотренные в Вопросе 3/2 МСЭ-D (Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности), которые отражены в резолюции 64/211 ГА ООН;

*e)* что МСЭ 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;

*f)* что в соответствии с Резолюцией 1336 Совета, принятой на его сессии 2011 года, создана Рабочая группа Совета по вопросам международной государственной политики, касающимся интернета (РГС-Интернет), круг ведения которой состоит в том, чтобы выявлять, изучать и разрабатывать темы, связанные с вопросами международной государственной политики, касающимися интернета, включая те вопросы, которые были определены в Резолюции 1305 (2009 г.) Совета, такие как защита, безопасность, целостность, жизнеспособность и устойчивость интернета;

*g)* что ВКРЭ‑17 приняла Резолюцию 80 (Буэнос-Айрес, 2017 г.) о создании и продвижении пользующихся доверием информационных структур в развивающихся странах для содействия и поощрения обмена информацией экономического характера в электронной форме между экономическими партнерами;

*h)* что имеются Статья 6 о безопасности и устойчивости сетей и Статья 7 о незапрашиваемых массовых электронных сообщениях Регламента международной электросвязи, принятого Всемирной конференцией по международной электросвязи (Дубай, 2012 г.),

отмечая,

*а)* что в качестве межправительственной организации, участие в работе которой принимает частный сектор, МСЭ занимает надлежащее положение, для того чтобы играть важную роль совместно с другими соответствующими международными органами и организациями в противодействии угрозам и уязвимостям, которые влияют на усилия по укреплению доверия и безопасности при использовании ИКТ;

*b)* пп. 35 и 36 Женевской декларации принципов и п. 39 Тунисской программы, касающиеся укрепления доверия и безопасности при использовании ИКТ;

*с)* что, хотя отсутствуют общепринятые определения спама и других терминов в этой области, спам был охарактеризован 2-й Исследовательской комиссией МСЭ-Т на ее собрании в июне 2006 года как термин, обычно используемый для обозначения незапрашиваемой массовой рассылки электронных сообщений по электронной почте или на мобильные телефоны (SMS, MMS), как правило, с целью продвижения товаров и услуг коммерческого характера;

*d)* инициативы Союза по сотрудничеству с Форумом групп реагирования на инциденты и обеспечения безопасности,

памятуя

о работе МСЭ, закрепленной в Резолюциях 50 и 52 (Пересм. Хаммамет, 2016 г.) и Резолюции 58 (Пересм. Дубай, 2012 г.), Резолюции 45 (Пересм. Дубай, 2014 г.) и Резолюции 69 (Пересм. Буэнос‑Айрес, 2017 г), Задаче 2 Плана действий Буэнос-Айреса; соответствующих Вопросах МСЭ-Т, касающихся технических аспектов безопасности информационных сетей и сетей связи; и Вопросе 3/2 МСЭ‑D,

решает

1 продолжать уделять этой работе в рамках МСЭ высокий приоритет в соответствии с его компетенцией и техническими 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 придать высокий приоритет работе МСЭ, описанной в разделе *памятуя*, выше, в соответствии с его сферами компетенции и опытом, и продолжать тесное сотрудничество, в надлежащих случаях, с соответствующими органами/учреждениями системы Организации Объединенных Наций и с другими соответствующими международными органами, учитывая конкретные мандаты и сферы компетенции различных учреждений, принимая во внимание при этом необходимость избегать дублирования работы между организациями и в рамках Бюро и Генерального секретариата;

3 что МСЭ следует сосредоточить ресурсы и программы на тех национальных, региональных и международных областях кибербезопасности, которые соответствуют его основному мандату и опыту, в особенности в технической сфере и сфере развития, и не включать области, относящиеся к применению Государствами-Членами правовых или политических принципов, связанных с национальной обороной, национальной безопасностью, контентом и киберпреступностью, которые относятся к их суверенным правам, хотя это не исключает выполнение МСЭ своего мандата по разработке технических рекомендаций, предназначенных для уменьшения уязвимости инфраструктуры ИКТ, и не препятствует предоставлению всей той помощи, которая была согласована на ВКРЭ-17, в том числе в рамках Задачи 2 и видов деятельности в соответствии с Вопросом 3/2;

4 развивать культуру, в рамках которой безопасность рассматривается как непрерывный и итерационный процесс, изначально встраиваемый в продукты и сохраняющийся на протяжении всего срока их службы, и которая также является доступной и понятной для пользователей;

5 способствовать повышению осведомленности членов МСЭ о деятельности, осуществляемой в МСЭ и других соответствующих структурах, принимающих участие в укреплении кибербезопасности, в том числе о создании потенциала, а также повышать осведомленность таких структур о конкретных проблемах в области укреплении доверия и безопасности при использовании ИКТ, с которыми сталкиваются развивающиеся страны;

6 вносить вклад в дальнейшее укрепление основ доверия и безопасности в соответствии с ролью МСЭ как ведущей содействующей организации по Направлению деятельности С5 ВВУИО с учетом Резолюции 140 (Пересм. Дубай, 2018 г.);

7 продолжать поддерживать и вести перечень национальных, региональных и международных инициатив и видов деятельности на основе информационной базы, относящейся к "Дорожной карте по стандартам безопасности ИКТ" и деятельности МСЭ-D в области кибербезопасности, а также с помощью других соответствующих организаций, чтобы содействовать разработке общих подходов в области кибербезопасности;

8 в сотрудничестве с членами и соответствующими организациями разрабатывать исследования конкретных институциональных механизмов, связанных с кибербезопасностью;

9 рассматривать конкретные проблемы в области кибербезопасности, с которыми сталкиваются МСП, и включать результаты этого рассмотрения в деятельность МСЭ в сфере укрепления доверия и безопасности при использовании ИКТ;

10 учитывать последствия внедрения появляющихся в области кибербезопасности технологий и включить этот фактор в деятельность МСЭ в сфере укрепления доверия и безопасности при использовании ИКТ;

11 поддерживать разработку инфраструктуры, которая является основой происходящей цифровой трансформации мировой экономики, укрепляя доверие и безопасность при использовании ИКТ, в частности при решении вопросов, связанных с существующими и будущими угрозами, в рамках мандата МСЭ;

12 использовать структуру ГПК для того, чтобы далее направлять работу Союза по укреплению доверия и безопасности при использовании ИКТ,

поручает Генеральному секретарю и Директорам Бюро

1 продолжать анализировать:

i) работу, проделанную к настоящему времени тремя Секторами в рамках ГПК и другими соответствующими организациями, и инициативы по противодействию существующим и будущим угрозам и укреплению защиты от них, для того чтобы укрепить доверие и безопасность при использовании ИКТ;

ii) ход работы по выполнению настоящей Резолюции, при том что МСЭ продолжает играть руководящую роль в качестве ведущей/содействующей организации по Направлению деятельности С5 при помощи консультативных групп в соответствии с Уставом МСЭ и Конвенцией МСЭ;

iii) результаты проделанной к настоящему времени работы по поддержке, в частности, развивающихся стран в создании потенциала и развитии навыков в области кибербезопасности для обеспечения того, чтобы МСЭ эффективно направлял свои ресурсы на решение проблем развития;

2 в соответствии с Резолюцией 45 (Пересм. Дубай, 2014 г.) представлять отчеты Совету о деятельности в рамках МСЭ и других соответствующих организаций и объединений по укреплению сотрудничества и взаимодействия на региональном и глобальном уровнях, в целях укрепления доверия и безопасности при использовании ИКТ Государствами-Членами, в частности развивающимися странами, с учетом любой информации, предоставляемой Государствами-Членами, включая информацию о ситуации в рамках их юрисдикций, которая может влиять на данное сотрудничество;

3в соответствии с Резолюцией 45 (Пересм. Дубай, 2014 г.) представить отчет о меморандумах о взаимопонимании (МоВ) между странами, а также о существующих формах сотрудничества, обеспечивая анализ их статуса, сферы применения и того, каким образом механизмы сотрудничества могут применяться для укрепления кибербезопасности и борьбы с киберугрозами, с тем чтобы обеспечить Государствам-Членам возможность определять необходимость в дополнительных меморандумах и механизмах;

4 повышать осведомленность о деятельности, осуществляемой в МСЭ и других соответствующих структурах, занимающихся укреплением кибербезопасности, в том числе о создании потенциала, и о конкретных проблемах в области укрепления доверия и безопасности при использовании ИКТ, с которыми сталкиваются развивающиеся страны, в соответствии с пунктом 5 раздела *решает*;

5 способствовать доступу к инструментам и ресурсам в пределах имеющегося бюджета, необходимым для укрепления доверия и безопасности при использовании ИКТ, для всех Государств-Членов в соответствии с разработанными ВВУИО положениями об универсальном и недискриминационном доступе к ИКТ для всех стран;

6 продолжать обмен знаниями и информацией о существующих и планируемых национальных, региональных и международных инициативах, связанных с кибербезопасностью во всем мире, используя веб-страницу МСЭ, посвященную кибербезопасности, и призывать все заинтересованные стороны участвовать в этой деятельности, учитывая имеющиеся порталы;

7 ежегодно представлять Совету отчет об этой деятельности и в надлежащих случаях вносить предложения;

8 далее укреплять координацию между соответствующими исследовательскими комиссиями и программами,

поручает Директору Бюро стандартизации электросвязи

1 активизировать работу в существующих исследовательских комиссиях МСЭ‑Т, с тем чтобы:

i) противодействовать существующим и будущим угрозам и уязвимости, которые влияют на усилия по укреплению доверия и безопасности при использовании ИКТ с учетом новых услуг и появляющихся приложений на основе сетей электросвязи/ИКТ, разрабатывая, в надлежащих случаях, отчеты и рекомендации, с тем чтобы выполнить резолюции ВАСЭ, в частности Резолюции 50 и 52 (Пересм. Хаммамет, 2016 г.) и Резолюцию 58 (Пересм. Дубай, 2012 г.), допуская начало работы до утверждения Вопроса;

ii) изыскивать способы расширения обмена технической информацией в этих областях, содействовать принятию протоколов и стандартов, укрепляющих безопасность, и способствовать международному сотрудничеству между соответствующими объединениями;

iii) содействовать осуществлению проектов, разработанных во исполнение решений ВАСЭ, в частности:

• Резолюции 50 (Пересм. Хаммамет, 2016 г.) о кибербезопасности;

• Резолюции 52 (Пересм. Дубай, 2012 г.) о противодействии распространению спама и борьбе со спамом;

2 рассмотреть в МСЭ-Т вопрос о содействии формированию культуры, в рамках которой безопасность рассматривается как непрерывный и итерационный процесс, и в случае целесообразности представить Совету предложения;

3 продолжать сотрудничать с соответствующими организациями с целью обмена передовым опытом и распространения информации, например путем проведения совместных семинаров‑практикумов и курсов профессиональной подготовки и участия в группах по совместной координационной деятельности, а также посредством письменных вкладов, представляемых соответствующими организациями на основе сделанного им предложения,

поручает Директору Бюро развития электросвязи

1 в соответствии с результатами ВКРЭ-17 и во исполнение Резолюций 45 (Пересм. Дубай, 2014 г.) и 69 (Пересм. Буэнос-Айрес, 2017 г.), Резолюции 80 (Буэнос-Айрес, 2017 г.) и Задачи 2 Плана действий Буэнос-Айреса поддерживать текущие проекты в области кибербезопасности на региональном и глобальном уровнях и поощрять участие всех стран в этой деятельности;

2 в ответ на поступающие просьбы оказывать поддержку Государствам – Членам МСЭ в их работе по созданию потенциала путем упрощения доступа Государств-Членов к ресурсам, созданным другими соответствующими международными организациями, которые занимаются разработкой национального законодательства для борьбы с киберпреступностью; поддержки усилий, предпринимаемых Государствами – Членами МСЭ на национальном и региональном уровнях, по созданию потенциала для защиты от киберугроз/киберпреступности при сотрудничестве между ними; в соответствии с национальным законодательством Государств-Членов, упомянутым выше, путем оказания помощи Государствам-Членам, в частности развивающимся странам, в разработке надлежащих и осуществимых правовых мер, связанных с защитой от киберугроз на национальном, региональном и международном уровнях; введения технических и процедурных мер, направленных на защиту национальной инфраструктуры ИКТ, с учетом работы соответствующих исследовательских комиссий МСЭ-Т и, в надлежащих случаях, других соответствующих организаций; создания организационных структур, таких как группы CIRT, для выявления киберугроз, управления ими и реагирования на них, а также механизмов сотрудничества на региональном и международном уровнях;

3 оказывать необходимую финансовую и административную поддержку этим проектам в пределах имеющихся ресурсов и изыскивать дополнительные ресурсы (в денежной и натуральной формах) для осуществления этих проектов в рамках соглашений о партнерстве;

4 обеспечивать координацию работы по этим проектам в контексте общей деятельности МСЭ в роли ведущей/содействующей организации по Направлению деятельности С5 ВВУИО, и исключить любое дублирование деятельности по этой важной проблематике с Генеральным секретариатом и МСЭ‑Т;

5 координировать работу по этим проектам с работой исследовательских комиссий МСЭ-D по этой теме, а также с деятельностью в рамках соответствующих программ и деятельностью Генерального секретариата;

6 продолжать сотрудничать с соответствующими организациями с целью обмена передовым опытом и распространения информации, например путем проведения совместных семинаров-практикумов и курсов профессиональной подготовки;

7 содействовать работе 17-й Исследовательской комиссии и других исследовательских комиссий МСЭ-Т, поощряя и поддерживая реализацию утвержденных Рекомендаций МСЭ-Т, касающихся безопасности, Государствами – Членами МСЭ и Членами Секторов, в особенности из развивающихся стран;

8 поддерживать Государства – Члены МСЭ в разработке их национальных и/или региональных стратегий в области кибербезопасности для создания национальных средств защиты от киберугроз и борьбы с ними в соответствии с принципами международного сотрудничества согласно Задаче 2 Плана действий Буэнос-Айреса;

9 поддерживать членов в деятельности по повышению квалификации специалистов и созданию потенциала в целях укрепления кибербезопасности;

10 поддерживать членов в деятельности по оценке рисков, связанных с кибербезопасностью;

11 ежегодно представлять Совету отчет об этой деятельности и в надлежащих случаях вносить предложения,

поручает далее Директору Бюро стандартизации электросвязи и Директору Бюро развития электросвязи в рамках сферы ответственности каждого

1 выполнять соответствующие Резолюции ВАСЭ-16 и ВКРЭ-17, в том числе намеченный результат деятельности 2.2 Задачи 2 Плана действий Буэнос‑Айреса, с особым вниманием к потребностям развивающихся стран в их усилиях по повышению уровня кибербезопасности и укреплению доверия и безопасности при использовании ИКТ;

2 выявлять наличие и содействовать доступности для Государств-Членов, Членов Секторов и соответствующих организаций информации об укреплении доверия и безопасности при использовании ИКТ, включая инфраструктуру ИКТ;

3 не допуская дублирования работы в рамках Вопроса 3/2 МСЭ-D, продолжать выявлять примеры передового опыта, относящиеся к Вопросу 3/2, в том числе в области создания групп CIRT, и осуществить пересмотр справочного руководства для Государств-Членов, а также, в надлежащих случаях, участвовать в работе по Вопросу 3/2;

4 взаимодействовать с соответствующими организациями и, при необходимости, с другими соответствующими международными и национальными экспертами, с тем чтобы выявлять примеры передового опыта в области укрепления доверия и безопасности при использовании ИКТ, в том числе в том, что касается создания CIRT;

5 принимать меры к тому, чтобы новые Вопросы изучались исследовательскими комиссиями в рамках Секторов в аспекте формирования доверия и безопасности при использовании ИКТ;

6 определять и документально оформлять практические меры по поддержке развивающихся стран в деле создания потенциала и развития навыков кибербезопасности, принимая во внимание конкретные проблемы, с которыми они сталкиваются;

7 принимать во внимание проблемы, с которыми сталкиваются все заинтересованные стороны, в частности в развивающихся странах, в деятельности по укреплению доверия и безопасности при использовании ИКТ и определять меры, которые могут способствовать решению этих проблем;

8 содействовать доступности для Государств-Членов, Членов Секторов и соответствующих организаций информации о национальных удостоверяющих центрах, их сферах деятельности, используемых алгоритмах и идентификаторах;

9 определять и документально оформлять практические меры по укреплению безопасности при использовании ИКТ на международном уровне, в том числе концепцию, согласно которой безопасность рассматривается как непрерывный и итерационный процесс, основываясь на широко распространенных практике, руководящих указаниях и рекомендациях, которые Государства-Члены и другие заинтересованные стороны могут решить применять в целях расширения своих возможностей по борьбе с киберугрозами и атаками, включая динамичный, итерационный, основанный на оценке рисков подход, отражающий постоянно меняющийся характер угроз и уязвимостей, и усиления международного сотрудничества в деле укрепления доверия и безопасности при использовании ИКТ, и учитывая ГПК, а также в рамках имеющихся финансовых ресурсов;

10 оказывать поддержку в области стратегии, организации, информационно-пропагандистской деятельности, сотрудничества, оценки и развития профессиональных навыков;

11 предоставлять необходимую техническую и финансовую поддержку в пределах существующих бюджетных ресурсов в соответствии с Резолюцией 58 (Пересм. Дубай, 2012 г.);

12 поощрять привлечение экспертов к деятельности МСЭ в области укрепления доверия и безопасности при использовании ИКТ;

13 осуществлять мобилизацию необходимых внебюджетных ресурсов вне регулярного бюджета Союза для выполнения настоящей Резолюции в целях оказания помощи развивающимся странам;

14 оказывать развивающимся странам поддержку и помощь в популяризации Рекомендаций МСЭ-Т, касающихся безопасности, и содействии их осуществлению;

15 оказывать помощь Государствам-Членам в проведении оценки и адаптации законодательной и нормативно-правовой базы на основе более эффективного использования отчета по Глобальному индексу кибербезопасности (GCI) МСЭ;

16 установить ежегодную "обратную связь" с уполномоченными администрациями Государств-Членов для анализа и совершенствования процесса расчета GCI,

поручает Генеральному секретарю

в соответствии с его инициативой по данному вопросу:

1 представлять отчеты Совету о выполнении и эффективности плана действий по усилению роли МСЭ в укреплении доверия и безопасности при использовании ИКТ, принимая во внимание деятельность трех Секторов;

2 сотрудничать в этом отношении с соответствующими международными организациями, в том числе путем принятия меморандумов о взаимопонимании, при условии утверждения Советом согласно Резолюции 100 (Миннеаполис, 1998 г.) Полномочной конференции,

просит Совет

включить отчет Генерального секретаря в документы, рассылаемые Государствам-Членам в соответствии с п. 81 Конвенции,

предлагает Государствам-Членам

1 рассмотреть возможность присоединения к соответствующим надлежащим международным и региональным инициативам по совершенствованию национальных нормативно-правовых баз, имеющих отношение к безопасности информационных сетей и сетей связи;

2 тесно взаимодействовать в рамках усиления регионального и международного сотрудничества, учитывая Резолюцию 45 (Пересм. Дубай, 2014 г.), с тем чтобы укреплять доверие и безопасность при использовании ИКТ в целях снижения рисков и угроз;

3 поддерживать инициативы МСЭ в области кибербезопасности, включая введение Глобального индекса кибербезопасности (GCI), с тем чтобы содействовать осуществлению государственных стратегий и обмену информацией о деятельности, проводимой в отраслях и секторах;

4 информировать Генерального секретаря о соответствующей деятельности, касающейся настоящей Резолюции и связанной с доверием и безопасностью при использовании ИКТ;

5 пользоваться ресурсами, поддержкой и передовым опытом, сформировавшимися в рамках национальных, региональных и международных инициатив в области кибербезопасности во всем мире, которые доступны на веб-странице МСЭ, посвященной вопросам кибербезопасности;

6 сотрудничать с соответствующими организациями путем обмена передовым опытом в области укрепления доверия и безопасности при использовании ИКТ, включая разработку и создание национальных групп CIRT;

7 продолжать повышать осведомленность путем распространения информации о передовом опыте и стратегиях, которые были реализованы в целях расширения возможностей разработки надлежащей политики для решения проблемы защиты пользователей, с тем чтобы укреплять доверие при использовании электросвязи/ИКТ,

предлагает Государствам-Членам, Членам Секторов и Ассоциированным членам

1 представлять вклады по этой теме соответствующим исследовательским комиссиям МСЭ и в отношении любой другой деятельности, за которую Союз несет ответственность;

2 вносить вклад в укрепление доверия и безопасности при использовании ИКТ на национальном, региональном и международном уровнях путем осуществления деятельности, определенной в итоговых документах ВВУИО, в Заявлении ВВУИО+10 о выполнении решений ВВУИО и в разработанной ВВУИО+10 Концепции ВВУИО на период после 2015 года, в итоговом документе совещания высокого уровня ГА ООН, посвященного общему обзору хода осуществления решений ВВУИО, и вносить вклад в подготовку и реализацию этих видов деятельности;

3 повышать осведомленность всех заинтересованных сторон, в том числе организаций и отдельных пользователей, о важности укрепления кибербезопасности, в том числе применения базовых средств защиты;

4 содействовать разработке образовательных и учебных программ для повышения осведомленности пользователей о рисках в киберпространстве и шагах, которые пользователи могут предпринимать для своей защиты;

5 предусмотреть применение в своих усилиях по укреплению доверия и безопасности при использовании ИКТ итерационного, основанного на оценке рисков подхода к борьбе с изменяющимися угрозами и уязвимостями и поощрять формирование культуры, в которой обеспечение безопасности рассматривается как непрерывный и итерационный процесс, который должен быть включен в разработку и развертывание технологий и их приложений с самого начала и не прекращаться на протяжении всего их жизненного цикла;

6 взаимодействовать, в надлежащих случаях, для устранения и предупреждения проблем, подрывающих доверие и безопасность при использовании электросвязи/ИКТ.

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

1. 1 К ним относятся наименее развитые страны, малые островные развивающиеся государства, развивающиеся страны, не имеющие выхода к морю, и страны с переходной экономикой. [↑](#footnote-ref-1)