|  |  |
| --- | --- |
| **Полномочная конференция (ПК-18)** **Дубай, 29 октября – 16 ноября 2018 г.** | logo_R_ |
|  |  |
|  |  |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | **Документ 67-R** |
|  | **12 октября 2018 года** |
|  | **Оригинал: английский** |
|  | |
| Бразилия (Федеративная Республика) | |
| Предложения для работы конференции | |
|  | |
|  | |

MOD B/67/1

РЕЗОЛЮЦИЯ 14 (Пересм. ДУБАЙ, 2018 Г.)

Признание прав и обязанностей   
всех Членов Секторов Союза

Полномочная конференция Международного союза электросвязи (Дубай, 2018 г.),

учитывая,

*а)* что права и обязанности Государств-Членов и Членов Секторов Союза изложены в Статье 3 Устава МСЭ;

*b)* что в Статье 19 Конвенции МСЭ перечислены типы объединений и организаций, которые могут быть уполномочены участвовать в деятельности Секторов как Члены Сектора;

*с)* что, за исключением положений пп. 239 и 340С Конвенции, только Государства-Члены имеют право голоса, в частности для утверждения Рекомендаций и Вопросов, в соответствии со Статьей 3 Устава,

признавая,

что Члены Секторов, упомянутые в списках, составленных Генеральным секретарем в соответствии с п. 237 Конвенции, могут участвовать во всех видах деятельности данного Сектора, за исключением официального голосования и некоторых конференций по разработке договоров, в связи с этим каждому Члену Сектора разрешается:

а) получать от Бюро данного Сектора любую запрошенную ими документацию, относящуюся к исследовательским комиссиям, ассамблеям или конференциям Сектора, в которых они могут участвовать в соответствии с надлежащими положениями Конвенции и на основе рабочих методов и процедур соответствующего Сектора;

b) направлять вклады исследовательским комиссиям, в частности тем, в которых они, в положенные сроки, высказали пожелание участвовать, в соответствии с рабочими методами и процедурами данного Сектора;

с) направлять представителей на такие собрания, сообщив их имена Бюро в положенные сроки, в соответствии с рабочими методами и процедурами данного Сектора;

d) вносить предложения о включении вопросов в повестку дня таких собраний, за исключением вопросов, относящихся к структуре и функционированию Союза;

e) принимать участие в любых дискуссиях и исполнять функции, такие как функции председателя или заместителя председателя исследовательской комиссии, рабочей группы, группы экспертов, группы докладчика или любой другой специальной группы, в зависимости от компетенции и наличия экспертов;

f) принимать участие в редакционной и издательской работе, необходимой перед принятием рекомендаций,

признавая далее,

что, как было установлено, координация между Государствами-Членами и Членами Секторов на национальном уровне позволила повысить эффективность работы,

решает

разрешить Членам Секторов принимать участие в любой процедуре поиска решений, направленной на достижение консенсуса в исследовательских комиссиях, региональных группах, рабочих группах, консультативных группах, региональных семинарах и собраниях и в рамках других мероприятий, в частности в области стандартизации,

предлагает Всемирной конференции по развитию электросвязи, Ассамблее радиосвязи и Всемирной ассамблее по стандартизации электросвязи

принять соответствующие положения, касающиеся рабочих методов и процедур в своих Секторах,

предлагает администрациям Государств-Членов

обеспечить на национальном уровне широкую координацию между всеми Членами Секторов в своих странах.

**Основания**: Бразилия предлагает внести изменения в Резолюцию 14 (Пересм. Анталия, 2006 г.) с главной целью поощрения и облегчения участия различных членов МСЭ в многочисленных форумах для обсуждений.

MOD B/67/2

РЕЗОЛЮЦИЯ 71 (Пересм. ДУБАЙ, 2018 Г.)

Стратегический план Союза на 2020–2023 годы

Полномочная конференция Международного союза электросвязи (Дубай, 2018 г.),

учитывая

положения Устава МСЭ и Конвенции МСЭ, относящиеся к стратегическим политическим принципам и планам,

отмечая

*а)* сложные задачи, стоящие перед Союзом при достижении им своих целей в постоянно изменяющейся среде электросвязи/информационно-коммуникационных технологий (ИКТ), а также условия разработки и выполнения стратегического плана, изложенные в Приложении 1 к настоящей Резолюции;

*b)* глоссарий терминов, представленный в Приложении 3 к настоящей Резолюции,

признавая

*a)* опыт, полученный в ходе выполнения Стратегического плана Союза на 2016–2019 годы;

*b)* что следует обеспечить учет роли регионального присутствия при реализации концепции "Единого МСЭ" в Стратегическом плане Союза и что Совету следует обеспечить, чтобы эта роль была соответствующим образом отражена в оперативном плане каждого Сектора;

*c)* что эффективной увязки между стратегическим планом и финансовым планом, представленными в Приложении 1 к Решению 5 (Пересм. Дубай, 2018 г.) настоящей Конференции, можно добиться путем перераспределения ресурсов Финансового плана на различные Секторы, а затем на цели и задачи стратегического плана, представленные в Дополнении к Приложению 1 к настоящей Резолюции,

решает

принять содержащийся в Приложении 1 к настоящей Резолюции Стратегический план Союза на 2020–2023 годы,

поручает Генеральному секретарю и Координационному комитету

1 дополнительно проработать и внедрить структуру результатов деятельности МСЭ для выполнения Стратегического плана Союза на 2020–2023 годы (Приложение 1) в соответствии с принципами управления, ориентированного на результаты (УОР), и составления бюджета, ориентированного на результаты (БОР);

2 координировать выполнение Стратегического плана, обеспечивая согласованность между Стратегическим планом, Финансовым планом, оперативными планами и двухгодичными бюджетами;

3 ежегодно представлять отчеты Совету МСЭ о ходе выполнения Стратегического плана на 2020–2023 годы, а также о показателях деятельности Союза, направленной на достижение его целей и задач;

4 рекомендовать Совету МСЭ возможные коррективы к этому плану ввиду изменений в среде электросвязи/ИКТ и/или в результате оценки показателей деятельности и структуры управления рисками:

i) внесения всех необходимых изменений для обеспечения того, чтобы стратегический план содействовал выполнению МСЭ своих целей и задач, принимая во внимание предложения со стороны консультативных групп Секторов, решения, принимаемые на конференциях и ассамблеях Секторов, и изменения стратегической направленности деятельности Союза в рамках финансовых ограничений, установленных полномочной конференцией;

ii) увязки стратегических, финансовых и оперативных планов МСЭ и разработки соответствующего стратегического плана в области людских ресурсов,

поручает Совету

1 осуществлять надзор за дальнейшей разработкой структуры результатов деятельности МСЭ, включая принятие соответствующих показателей, которые позволят лучше измерять эффективность и действенность выполнения Стратегического плана Союза (Приложение 1);

2 осуществлять мониторинг выполнения Стратегического плана Союза, содержащегося в Приложении 1 к настоящей Резолюции, и при необходимости корректировать стратегический план на основе отчетов Генерального секретаря;

3 представить следующей полномочной конференции оценку результатов выполнения Стратегического плана на 2020–2023 годы совместно с предлагаемым Стратегическим планом на 2024–2027 годы;

4 принять необходимые меры для того, чтобы скользящие оперативные планы Генерального секретариата и трех Секторов, ежегодно утверждаемые Советом, были полностью согласованы и соответствовали настоящей Резолюции и приложениям к ней, а также Финансовому плану Союза, утвержденному в Решении 5 настоящей Конференции,

предлагает Государствам-Членам

включать национальное и региональное видение вопросов политики, регулирования и эксплуатации в процесс стратегического планирования, осуществляемого Союзом, в период до следующей полномочной конференции, для того чтобы:

– повысить эффективность Союза при выполнении им своих целей, определенных в основных документах Союза, на основе сотрудничества в выполнении стратегического плана;

– помочь Союзу оправдывать изменяющиеся ожидания всех своих членов, по мере того как национальные структуры, обеспечивающие предоставление услуг электросвязи/ИКТ, продолжают развиваться,

предлагает Членам Секторов

сообщать о своих мнениях в отношении стратегического плана Союза через свои соответствующие Секторы и надлежащие консультативные группы.

**Основания**: Бразилия предлагает внести поправки в основной текст Резолюции 71 (не включая Приложения) в целях укрепления концепции "Единого МСЭ" путем усиления деятельности региональных отделений в области стандартизации и радиосвязи и путем укрепления механизмов мониторинга и контроля разработки и реализации оперативных планов Секторов.

SUP B/67/3

РЕЗОЛЮЦИЯ 128 (Пересм. Анталия, 2006 г.)

Поддержка Программы "Соединение в Северной и Южной Америке" и Плана действий Кито

Полномочная конференция Международного союза электросвязи (Анталия, 2006 г.),

**Основания**: Бразилия предлагает исключить Резолюцию 128 в связи с неактуальностью Программы "Соединение в Северной и Южной Америке" и Плана действий Кито в нынешней среде электросвязи/ИКТ, а также исключить Резолюцию 39 Всемирной конференции по развитию электросвязи 2017 года (ВКРЭ-17) по тому же вопросу.

MOD B/67/4

РЕЗОЛЮЦИЯ 130 (ПЕРЕСМ.ДУБАЙ, 2018 Г.)

Усиление роли МСЭ в обеспечении кибербезопасности

Полномочная конференция Международного союза электросвязи (Дубай, 2018 г.),

напоминая

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

*b)* резолюцию 68/167 ГА ООН о праве на неприкосновенность личной жизни в цифровой век;

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

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

*e)* резолюцию 70/125 ГА ООН, содержащую Итоговый документ совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений (ВВУИО);

*f)* Резолюцию 174 (Пересм. Пусан, 2014 г.) настоящей Конференции;

*g)* Резолюцию 181 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции;

*h)* Резолюцию 45 (Пересм. Дубай, 2014 г.) Всемирной конференции по развитию электросвязи (ВКРЭ) о механизмах совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним;

*i)* Резолюцию 140 (Пересм. Пусан, 2014 г.) настоящей Конференции;

*j)* Резолюцию 69 (Пересм. Буэнос-Айрес, 2017 г.) ВКРЭ о содействии созданию национальных групп реагирования на компьютерные инциденты, в частности в развивающихся странах[[1]](#footnote-1)1, и сотрудничеству между ними;

*k)* 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 в резолюции 70/125 ГА ООН, содержащей Итоговый документ совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений ВВУИО, подтверждается, что *"права, которыми люди пользуются в обычной жизни, должны защищаться и при пользовании интернетом. Мы особо отмечаем, что прогресс в достижении цели, поставленной на Всемирной встрече на высшем уровне по вопросам информационного общества, следует рассматривать не только как одну из функций экономического развития и распространения информационно-коммуникационных технологий, но и как одну из функций прогресса в осуществлении прав человека и основных свобод" и что "одним из приоритетов должно также стать укрепление доверия и безопасности в сфере использования информационно-коммуникационных технологий в интересах устойчивого развития, особенно с учетом растущих проблем в этой области, включая использование таких технологий для совершения противоправных действий, начиная от притеснений и домогательств и заканчивая преступлениями и террористическими актами"*;

*b)* 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 и сетям и их уязвимость продолжают создавать проблемы все большего масштаба, невзирая на национальные границы, в отношении безопасности для всех стран;

*c)* что МСЭ подписал соглашение о сотрудничестве с Форумом групп реагирования на инциденты и обеспечения безопасности (FIRST) в целях сотрудничества в рамках Глобальной программы кибербезопасности МСЭ и содействия процессу присоединения национальных CIRT Государств-Членов МСЭ к FIRST;

*d)* 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;

*e)* 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 с компьютерной безопасностью и на восстановление после него со стороны органов государственного управления на национальном (включая создание национальных групп реагирования на компьютерные инциденты (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;

*f)* необходимость постоянного развития новых технологий для обеспечения раннего обнаружения событий или инцидентов, ставящих под угрозу компьютерную безопасность, 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;

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

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

*i)* что некоторые МСП сталкиваются с дополнительными проблемами в обеспечении кибербезопасности при выполнении важных задач, таких как внесение исправлений в информационные системы, обновление операционных систем, реализация планов профилактики, реагирования и восстановления, соблюдение правительственных и отраслевых норм и положений и содействие непрерывному наращиванию потенциала;

*j)* что техническое сообщество и частный сектор являются ключевыми игроками в развитии и развертывании новых технологий и что их приложения должны включать целостные подходы, в рамках которых кибербезопасность рассматривается как непрерывный процесс;

*k)* что частные лица и организации должны внедрять передовой опыт, который позволил бы использовать гибкие подходы, основанные на оценке рисков и консенсусе, имеющиеся технические средства защиты в рамках осознанного и ответственного пользовательского поведения и что в связи с этим требуются дополнительные усилия по наращиванию потенциала и повышению осведомленности,

признавая,

*а)* что развитие ИКТ имело и продолжает иметь решающее значение для роста и развития глобальной экономики на основе безопасности и доверия;

*b)* что Всемирная встреча на высшем уровне по вопросам информационного общества (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 для информационного общества ведущей/содействующей организацией для этого направления деятельности и что Союз выполнял эту задачу в последние годы, например, в рамках ГПК;

*c)* что 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; и что ВКРЭ-17 приняла План действий Буэнос-Айреса, в Задаче 2 которого кибербезопасность определяется в качестве приоритета, и Резолюцию 69 (Пересм. Буэнос-Айрес, 2017 г.) о содействии созданию национальных групп CIRT, в частности в развивающихся странах, и сотрудничеству между ними;

*d)* 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, Всемирная ассамблея по стандартизации электросвязи (ВАСЭ) приняла Резолюцию 58 (Пересм. Хаммамет, 2016 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, сотрудничеству между ними и о важности координации между всеми соответствующими организациями;

*e)* 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*";

*f)* 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;

*g)* 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;

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

*i)* Резолюцию 50 (Пересм. Хаммамет, 2016 г.) о кибербезопасности, содержащую решение продолжать уделять кибербезопасности первостепенное значение в рамках МСЭ-Т в соответствии с его компетенцией и специальными знаниями и опытом, в том числе содействовать достижению общего понимания среди правительств и других заинтересованных сторон вопросов укрепления доверия и безопасности при использовании ИКТ на национальном, региональном и международном уровнях;

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

*k)* что Государства-Члены постоянно прилагают усилия для улучшения институциональной среды;

*l)* что оценка киберрисков или анализ издержек, связанных с киберрисками, а также расчет подверженности рискам обеспечивают лучшую оценку кибергигиены предприятия и его положения в области рисков,

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 личных данных и неприкосновенности частной жизни;

*b)* что несанкционированное слежение за сообщениями и/или их перехват, а также сбор данных, особенно в массовом масштабе, имеют негативные последствия для осуществления и реализации прав человека;

*с)* 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.) ВАСЭ и Резолюциями 45 (Пересм. Дубай, 2014 г.) и 69 (Пересм. Буэнос-Айрес, 2017 г.) ВКРЭ;

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

*e)* 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;

*f)* 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;

*g)* 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 Совета (2009 г.), такие как защита, безопасность, целостность, жизнеспособность и устойчивость интернета;

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

*j)* Статью 6 о безопасности и устойчивости сетей и Статью 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 уязвимости, 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,

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, 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 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-14 (Резолюция 45) и ВКРЭ-17, включая Задачу 2 и виды деятельности в рамках Вопроса 3/2;

4 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. Пусан, 2014 г.);

5 соблюдать и защищать аспекты защиты данных, связанные с электросвязью/ИКТ, в качестве одного из принципов дальнейшего укрепления кибербезопасности в рамках основного мандата и опыта МСЭ;

6 изучить конкретные проблемы кибербезопасности, с которыми сталкиваются МСП, особенно ограниченность их ресурсов, а также передовой опыт, инициативы и руководящие указания, направленные на их преодоление;

7 представить членам оценку положительных и отрицательных последствий внедрения появляющихся технологий в области кибербезопасности, включая необходимость принятия мер для прекращения нарушений этих прав и создания условий для предотвращения таких нарушений, в том числе путем обеспечения соответствия национального законодательства их обязательствам по международному праву в области прав человека;

8 содействовать изучению институциональных подходов, связанных с вопросами кибербезопасности, в сотрудничестве с Государствами-Членами и другими международными организациями,

поручает Генеральному секретарю и Директорам Бюро

1 продолжать анализировать:

i) работу, проделанную к настоящему времени тремя Секторами в рамках Глобальной программы кибербезопасности МСЭ и другими соответствующими организациями, и инициативы по противодействию существующим и будущим угрозам, 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;

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 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;

5 продолжать вести портал кибербезопасности в качестве средства обмена информацией о национальных, региональных и международных инициативах, связанных с кибербезопасностью во всем мире;

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

7 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, разрабатывая, в надлежащих случаях, отчеты и рекомендации, с тем чтобы выполнить резолюции ВАСЭ‑16, в частности Резолюции 50 и 52 (Пересм. Хаммамет, 2016 г.) и 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-12, в частности:

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

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

2 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-14 и во исполнение Резолюции 45 (Пересм. Дубай, 2014 г.), Резолюций 69 и 80 (Пересм. 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 поддерживать Государства – Члены МСЭ в разработке их национальных и/или региональных стратегий в области кибербезопасности для создания национальных средств борьбы с киберугрозами в соответствии с принципами международного сотрудничества согласно Задаче 3 Плана действий Буэнос-Айреса;

8 поддерживать Членов в повышении квалификации специалистов и наращивании потенциала в целях повышения уровня кибербезопасности;

9 поддерживать Членов в деятельности по оценке рисков, связанных с кибербезопасностью;

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

далее поручает Директору Бюро стандартизации электросвязи и Директору Бюро развития электросвязи

в рамках сферы ответственности каждого:

1 выполнять соответствующие Резолюции ВАСЭ-116 и ВКРЭ-17, в том числе программу, описанную в Задаче 2 Плана действий Буэнос-Айреса, касающиеся предоставления поддержки и помощи развивающимся странам в укреплении 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, в частности связанной с инфраструктурой ИКТ;

3 не допуская дублирования работы в рамках Вопроса 3/2 МСЭ-D, выявлять примеры передового опыта в области создания групп CIRT и подготовить справочное руководство 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 создания CIRT;

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

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

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

9 поощрять изучение угроз безопасности и уязвимостей совместно с экспертами и членами;

10 содействовать обсуждению концепции проектируемой безопасности и ее возможного применения в технических рекомендациях, а также в руководящих указаниях, касающихся регуляторных стратегий, в интересах Членов;

11 изучить влияние кибербезопасности на социально-экономическое развитие и разработать показатели для оценки результатов инвестиций в эту область;

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

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,

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 п. 12 Женевского плана действий, и содействовать подготовке исследований в этих областях;

3 содействовать разработке образовательных и учебных программ для повышения осведомленности пользователей о рисках в киберпространстве;

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

**Основания**: Предложение Бразилии нацелено на то, чтобы МСЭ обсудил конкретные проблемы в области кибербезопасности, с которыми сталкиваются малые и средние предприятия, и разработал примеры передового опыта; подчеркивает важность распространения и продвижения передового опыта и обучения в области кибербезопасности среди частных лиц и организаций; способствует анализу рисков и издержек и прибыли при оценке подверженности организаций угрозам кибербезопасности; указывает на необходимость предотвращения и устранения нарушений неприкосновенности частной жизни и прав человека в результате несанкционированного перехвата сообщений; акцентирует внимание на важности защиты данных как ключевого элемента кибербезопасности; и поручает МСЭ обсудить определение и использование концепции "проектируемой безопасности" в технических рекомендациях МСЭ.

ADD B/67/5

ПРОЕКТ НОВОЙ РЕЗОЛЮЦИИ [B-1]

Вопросы международной государственной политики, касающиеся аспектов приложений OTT, связанных с электросвязью

Полномочная конференция Международного союза электросвязи (Дубай, 2018 г.),

ссылаясь

*a)* на принципы разработки политики в области интернета, изложенные в

• итогах Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) и встреч высокого уровня ВВУИО+10;

• резолюции 70/125 Генеральной Ассамблеи Организации Объединенных Наций, содержащей Итоговый документ совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества;

*b)* на основные цели МСЭ, определенные в Уставе МСЭ;

*c)* на Резолюции 102 (Пересм. Дубай, 2018 г.) и 140 (Пересм. Дубай, 2018 г.) МСЭ, в частности положения, касающиеся роли МСЭ и правительств в разработке политики в области интернета на основе консультаций со всеми заинтересованными сторонами;

*d)* на решения Тунисской программы (пункты 35, 36, 67), такие как проведение политического диалога с участием многих заинтересованных сторон, и сложность экосистемы, состоящей из большого количества различных форумов, созданных для обсуждения политики в области интернета;

*e)* на важность Форума по вопросам управления использованием интернета для обсуждения политики в области интернета (Тунисская программа, пункты 72 и 73);

*f)* на дискуссии об ОТТ, проводимые в других соответствующих организациях, включая организации по разработке стандартов (ОРС) и организации по разработке политики,

учитывая,

*a)* что в пункте 15 Повестки дня в области устойчивого развития на период до 2030 года подчеркиваются огромные возможности ИКТ и глобального взаимного подключения сетей для ускорения человеческого прогресса, преодоления цифрового разрыва и формирования обществ, основанных на знаниях, способствующие достижению и ускорению достижения Целей в области устойчивого развития;

*b)* что приложения over-the-top (OTT) позволяют правительствам, предприятиям и частным лицам получать выгоду, участвовать в цифровой экономике и устойчивом социально-экономическом развитии и активно вносить в них вклад;

*c)* что изначально заложенный трансграничный характер OTT требует сотрудничества и координации между правительствами и всеми заинтересованными сторонами на международном уровне,

признавая,

*a)* принципиальные различия между услугами традиционной электросвязи и OTT, включая, в том числе, контроль инфраструктуры широкополосного доступа, уровень регуляторного воздействия, препятствия для выхода на рынок, конкурентную среду и присоединение к сетям общего пользования;

*b)* что операторы сетей и OTT являются частью одной и той же экосистемы, что подразумевает наличие важных взаимозависимостей между ними;

*c)* что связь между OTT и услугами традиционной электросвязи может быть использована для расширения возможностей установления соединений для не обслуживаемых и обслуживаемых в недостаточной степени групп населения;

*e)* что сотрудничество между OTT и операторами электросвязи может быть элементом содействия созданию инновационных, устойчивых и жизнеспособных бизнес-моделей, а также поощрения их положительной роли в стимулировании социально-экономических преимуществ;

*f)* что расширение OTT создает технические, экономические, социальные и политические проблемы и возможности для правительств и отрасли электросвязи/ИКТ,

признавая далее

*а)* исследования 3-й Исследовательской комиссии и 17-й Исследовательской комиссии МСЭ-Т, в частности утверждение определения OTT в рамках МСЭ в Рекомендации МСЭ-Т D.262 и технический отчет 3-й Исследовательской комиссии МСЭ-Т "Экономическое воздействие технологий ОТТ" (2017 г.);

*b)* исследования 1-й Исследовательской комиссии МСЭ-D и утверждение Всемирной конференцией по развитию электросвязи 2017 года исследуемого Вопроса 3/1 "Появляющиеся технологии, в том числе облачные вычисления, мобильные услуги и услуги OTT: проблемы и возможности, а также экономические и политические последствия для развивающихся стран";

*с)* вклады заинтересованных сторон, представленные на 5-й открытой консультации РГС-Интернет на тему "Соображения государственной политики в отношении OTT", и обсуждения, проведенные на очном открытом консультационном собрании 18 сентября 2017 года;

*d)* заключительный отчет 10-го собрания РГС-Интернет, в котором показаны самые разные точки зрения Государств-Членов относительно надлежащей роли МСЭ в отношении OTT,

решает

1 повысить в рамках МСЭ осведомленность и содействовать общему пониманию среди членов в отношении благоприятной среды для аспектов приложений OTT, связанных с электросвязью;

2 содействовать в рамках МСЭ техническим, экономическим и политическим исследованиям аспектов приложений OTT, связанных с электросвязью,

поручает консультативным группам Секторов

выявлять вопросы, касающиеся аспектов приложений OTT, связанных с электросвязью, и стимулировать их изучение в исследовательских комиссиях Секторов в соответствии с их опытом и целью,

поручает РГС-Интернет

представлять Совету ежегодный отчет о деятельности, осуществляемой в МСЭ в отношении аспектов приложений OTT, связанных с электросвязью, который согласуется с работой исследовательских комиссий и консультативных групп МСЭ, вкладами Государств-Членов и Членов Секторов и открытыми материалами для консультаций,

поручает Директорам Бюро

тесно сотрудничать с РГС-Интернет и с консультативными группами Секторов в целях предоставления информации по вопросам, касающимся настоящей резолюции,

предлагает Государствам-Членам и Членам Секторов

вносить свой вклад в вышеупомянутую деятельность и принимать активное участие в выполнении настоящей резолюции.

**Основания**: На протяжении последних 20 лет некоторые приложения over-the-top (OTT) (далее "OTT") развиваются и постепенно заменяют традиционную электросвязь/ИКТ. Корреляция и взаимозависимость между электросвязью/ИКТ и OTT приводят к тому, что МСЭ все чаще обсуждает вопросы, связанные с OTT.

В сентябре 2017 года Рабочая группа Совета МСЭ по вопросам международной государственной политики, касающимся интернета (РГС-Интернет) провела свою 5-ю очную открытую консультацию на тему "Соображения государственной политики в отношении OTT". Консультация прошла успешно: было представлено 70 вкладов от различных заинтересованных сторон и всех регионов, кроме того, как в ходе очной консультации, так и в РГС-Интернет прошли широкие дискуссии на эту тему.

Бразильские заинтересованные стороны представили в рамках открытых консультаций восемь вкладов. Бразильская администрация представила РГС-Интернет вклад, в котором объяснялась рамочная основа обсуждения вопросов OTT в Бразилии с участием многих заинтересованных сторон, перечислялись вопросы, касающиеся экосистемы OTT, и предлагалось, чтобы в обсуждениях OTT в МСЭ упор делался на OTT, связанные с электросвязью, а также содержалась просьба о соблюдении принципов управления интернетом с участием многих заинтересованных сторон, установленных Всемирной встречей на высшем уровне по вопросам информационного общества (ВВУИО)[[2]](#footnote-2)1.

ВКРЭ-17 утвердила создание в МСЭ-D Вопроса 3/1 по теме "Появляющиеся технологии, в том числе облачные вычисления, мобильные услуги и услуги OTT: проблемы и возможности, а также экономические и политические последствия для развивающихся стран". 3-я Исследовательская комиссия МСЭ-T утвердила в апреле 2018 г. проект Рекомендации МСЭ-Т D.262 "Рамочная основа для сотрудничества в сфере услуг OTT", в которой ОТТ определяется как

"Приложение, доступ и работа с которым осуществляются с помощью общедоступного интернета, при этом оно может быть прямой технической или функциональной заменой для традиционных услуг международной электросвязи. (ПРИМЕЧАНИЕ. – Определение ОТТ является вопросом национального суверенитета и может различаться в разных Государствах-Членах)."[[3]](#footnote-3)2

Таким образом, Бразилия с удовлетворением отмечает уровень внимания, уделяемого OTT Советом МСЭ, Всемирной конференцией по развитию электросвязи 2017 года (ВКРЭ-17) и 3‑й Исследовательской комиссией МСЭ-Т.

Как в МСЭ-Т, так и в МСЭ-D в обсуждениях будут участвовать Члены Секторов МСЭ, в том числе поставщики ОТТ, операторы электросвязи, представители гражданского общества, научные учреждения, представители технического сообщества и другие международные организации.

МСЭ многого достиг в вопросах, связанных с OTT. Проект новой резолюции в Приложении I направлен на признание и активизацию работы, проводимой в настоящее время в МСЭ, на содействие совершенствованию отслеживания и мониторинга связанных с электросвязью аспектов приложений OTT, которые могут быть прямой технической или функциональной заменой для традиционных услуг международной электросвязи, во всех органах МСЭ, а также на обеспечение соблюдения установленных ВВУИО принципов управления использованием интернета с участием многих заинтересованных сторон.

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

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)
2. 1 <https://www.itu.int/md/S17-RCLINTPOL10-C-0005/en> [↑](#footnote-ref-2)
3. 2 <https://www.itu.int/md/T17-SG03-R-0011/en> [↑](#footnote-ref-3)