|  |  |  |
| --- | --- | --- |
| **Полномочная конференция (ПК-22)** **Бухарест, 26 сентября – 14 октября 2022 г.** | |  |
|  | |  |
|  |  | |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | **Дополнительный документ 35 к Документу 76-R** | |
|  | **1 сентября 2022 года** | |
|  | **Оригинал: английский** | |
|  | | |
| Государства – члены Межамериканской комиссии по электросвязи (СИТЕЛ) | | |
| IAP 35 − предложение о внесении изменений в РЕЗОЛЮЦИЮ 130 | | |
| об УсилениИ роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий | | |
|  | | |

MOD IAP/76A35/1

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 76/189 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 76/19 ГА ООН о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также поощрении ответственного поведения государств при использовании информационно-коммуникационных технологий;

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

*g)* о Резолюции 70 (Пересм. Дубай, 2018 г.) Полномочной конференции об учете гендерных аспектов в деятельности МСЭ и содействии обеспечению гендерного равенства и расширению прав и возможностей женщин посредством электросвязи/информационно-коммуникационных технологий;

*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. Бухарест, 2022 г.) настоящей Конференции о защите пользователей/потребителей услуг электросвязи;

*l)* о Резолюции 45 (Пересм. Кигали, 2022 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. Бухарест, 2022 г.) настоящей Конференции о роли МСЭ в выполнении решений ВВУИО и в общем обзоре их выполнения, проводимом ГА ООН;

*n)* о Резолюции 50 (Пересм. Женева, 2022 г.) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) о кибербезопасности;

*o)* о Резолюции 58 (Пересм. Женева, 2022 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;

*p)* о Резолюции 67 (Пересм. Кигали, 2022 г.) ВКРЭ о роли Сектора развития электросвязи МСЭ (МСЭ-D) в защите ребенка в онлайновой среде;

*q)* о Резолюции 69 (Пересм. Кигали, 2022 г.) ВКРЭ о содействии созданию национальных групп реагирования на компьютерные инциденты, в частности в развивающихся странах, и сотрудничестве между ними;

*r)* 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)* что угрозы инфраструктуре, технологиям и связанным с ними приложениям, сетям и устройствам и их уязвимость продолжают создавать проблемы все большего масштаба, невзирая на национальные границы, в отношении безопасности для всех стран;

*d)* что Совет на своей сессии 2022 года утвердил Руководящие указания по использованию МСЭ в своей работе Глобальной программы кибербезопасности (ГПК);

*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 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)* 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;

*g)* 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 вероятность и воздействие таких инцидентов и снизят растущие риски и угрозы, которым подвергаются такие платформы;

*h)* что в резолюции 70/125 ГА ООН об итоговом документе совещания высокого уровня Генеральной Ассамблеи, 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;

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

*j)* что характер среды стандартов кибербезопасности отражает многосторонний характер кибербезопасности и требует учета управляемых экспертами процессов со стороны МСЭ и других национальных, региональных, глобальных и отраслевых организаций;

*j bis)* что эта среда может быть комплексной, и МСЭ может играть важную роль в повышении осведомленности Членов о соответствующей работе в других организациях, процессах и инициативах, содействующих укреплению доверия и безопасности при использовании ИКТ;

*j ter)* что МСЭ может играть важную роль в повышении осведомленности других соответствующих организаций, процессов и инициатив об особых проблемах, с которыми сталкиваются развивающиеся страны в вопросах укрепления доверия и безопасности при использовании ИКТ;

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

*k bis)* что существует необходимость в том, чтобы специалисты по кибербезопасности обеспечивали доступность и эффективность программ подготовки, позволяющих нанимать людей с необходимыми навыками и опытом;

*k ter)* что, несмотря на прогресс, достигнутый в некоторых областях, многие страны сталкиваются с проблемами в развитии полезных компетенций и возможностей профессионального роста, и это является значительным препятствием для укрепления доверия и безопасности в сфере ИКТ;

*l)* 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;

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

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

*n bis)* необходимость повышать осведомленность и пропагандировать среди населения основные шаги, отражающие передовые практические методы защиты себя от рисков в сфере кибербезопасности, в том числе в отдаленных, сельских и недостаточно обслуживаемых сообществах и уязвимых группах,

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;

*b bis)* что электросвязь/ИКТ содействуют развитию гражданского общества и способствуют повышению уровня социальных благ и открытости для всех, предоставляя гражданам, бизнесу и правительственным органам новые каналы совместного использования знаний и увеличения их объема, а также участия в принятии решений, влияющих на их жизнь и профессиональную деятельность;

*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-22 приняла Кигалийский план действий и отраженные в нем приоритеты МСЭ-D, в частности приоритет обеспечения инклюзивной и защищенной электросвязи/ИКТ для устойчивого развития в целях оказания поддержки Государствам-Членам в обеспечении защищенной электросвязи/ИКТ для устойчивого развития в интересах всех; ВКРЭ-22 приняла Резолюцию 45 (Пересм. Кигали, 2022 г.) о механизмах совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним; ВКРЭ‑22 также приняла Резолюцию 69 (Пересм. Кигали, 2022 г.) о содействии созданию национальных групп CIRT, в частности в развивающихся странах, и сотрудничестве между ними;

*e)* что в Кигалийской декларации , принятой ВКРЭ-22, указано, что "В цифровую эпоху незаменимой является возможность установления универсальных, безопасных и приемлемых в ценовом отношении широкополосных соединений, что открывает перспективы повышения производительности и эффективности, ликвидации нищеты, повышения качества жизни и гарантии превращения устойчивого развития в реальность для всех, укрепление доверия и безопасности при использовании электросвязи/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-22 приняла Резолюцию 58 (Пересм. Женева, 2022 г.) о поощрении создания национальных групп CIRT, в частности в развивающихся странах, а ВКРЭ-22 приняла Резолюцию 69 (Пересм. Кигали, 2022 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, 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 мер;

*j)* соответствующие результаты работы ВАСЭ-22, а именно:

i) Резолюцию 50 (Пересм. Женева, 2022 г.) о кибербезопасности;

ii) Резолюцию 52 (Пересм. Женева, 2022 г.) о противодействии распространению спама и борьбе со спамом;

*k)* что защищенные и надежные сети будут укреплять доверие и поощрять обмен информацией и ее использование;

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

*l bis)* что многие Государства-Члены сталкиваются со значительной нехваткой квалифицированных кадров в сфере кибербезопасности и что нехватка подготовленных специалистов по кибербезопасности является одним из основных препятствий для укрепления доверия и безопасности при использовании ИКТ;

*l ter)* что во многих Государствах-Членах наблюдается значительное нарушение гендерного баланса в сфере кибербезопасности, что затрудняет решение проблемы нехватки квалифицированных кадров;

*l quart)* что важно поощрять большее число людей, особенно женщин и девушек, избирать карьеру в области кибербезопасности, с тем чтобы решить проблему нехватки квалифицированных кадров;

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

*n)* 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;

*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 (Пересм. Женева, 2022 г.) и 52 (Пересм. Хаммамет, 2016 г.) и Резолюциями 45 (Пересм. Кигали, 2022 г.) и 69 (Пересм. Кигали, 2022 г.);

*с)* что МСЭ должен играть основополагающую роль и, когда того требуют его Государства-Члены, выступать одним из имеющихся в распоряжении возможных средств укрепления доверия и безопасности при использовании ИКТ;

*d)* что МСЭ также помогает развивающимся странам в укреплении доверия и безопасности при использовании ИКТ и поддерживает создание CIRT в координации со всеми соответствующими организациями;

*e)* 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;

*f)* 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;

*g)* 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;

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

решает

1 продолжать придавать этой работе в рамках МСЭ высокий приоритет, принимая во внимание новые и появляющиеся услуги и технологии электросвязи/ИКТ, и 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 продолжать работу, придавая ей высокий приоритет, в соответствии со сферами компетенции и опытом МСЭ, 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-22;

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

4 *bis* способствовать укреплению доверия и безопасности при использовании ИКТ таким образом, чтобы это содействовало развитию гражданского общества и поддерживало более высокие уровни социальных благ и открытости для всех;

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;

5 *bis* вести активную работу с развивающимися странами по решению конкретных проблем, стоящих перед ними в области укрепления доверия и безопасности при использовании ИКТ и в случае наличия многих предприятий координировать и объединять свои усилия;

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 готовить статистические отчеты и демонстрировать последствия внедрения появляющихся в области кибербезопасности технологий и учитывать результаты в деятельности МСЭ в сфере укрепления доверия и безопасности при использовании ИКТ;

11 поощрять 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 поощрять и направлять деятельность по формированию среды ИКТ на основе принципов доверия и безопасности на благо развивающихся стран;

13 использовать структуру ГПК для того, чтобы далее направлять работу Союза по укреплению доверия и безопасности при использовании ИКТ, принимая во внимание утвержденные Советом Руководящие указания по использованию МСЭ в своей работе ГПК,

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. Кигали, 2022 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. Кигали, 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;

9 учитывать результаты Глобального индекса кибербезопасности (GCI) для ориентирования инициатив МСЭ, связанных с кибербезопасностью, уделяя особое внимание разрывам, выявленным в процессе определения GCI,

поручает Директору Бюро стандартизации электросвязи

1 вести 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 (Пересм. Женева, 2022 г.) и 52 (Пересм. Хаммамет, 2016 г.) и Резолюцию 58 (Пересм. Женева, 2022 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, на основе:

• Резолюции 50 (Пересм. Женева, 2022 г.) о кибербезопасности;

• Резолюции 52 (Пересм. Женева, 2022 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, задействуя опыт осуществляемых под руководством экспертов многосторонних процессов разработки стандартов и их результаты;

4 содействовать работе над исследуемым Вопросом 3/2 МСЭ-D;

5 сотрудничать с Директором Бюро развития электросвязи в деле распространения в развивающихся странах информации о руководящих указаниях, рекомендациях, технических отчетах и передовой практике по вопросам укрепления доверия и безопасности при использовании информационно-коммуникационных технологий, которые были разработаны исследовательскими комиссиями Сектора стандартизации электросвязи МСЭ (МСЭ-T),

поручает Директору Бюро развития электросвязи

1 в соответствии с результатами ВКРЭ-22 и во исполнение Резолюций 45 (Пересм. Кигали, 2022 г.) и 69 (Пересм. Буэнос-Айрес, 2017 г.), Резолюции 80 (Буэнос-Айрес, 2017 г.) 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 и содействие Государствам – Членам МСЭ, в их усилиях по укреплению потенциала в соответствии с их национальным законодательством в целях защиты от киберугроз;

2 *bis* продолжать реализацию успешных программ развития МСЭ в области введения технических и процедурных мер по обеспечению безопасности электросвязи/ИКТ, таких как разработка национальных стратегий кибербезопасности и создание CIRT, для предотвращения и выявления киберугроз, управления ими и восстановления после них;

2 *ter* направлять Государства-Члены МСЭ по их просьбе для задействования ресурсов, созданных другими международными организациями по борьбе с киберпреступностью, а именно УНП ООН и ИНТЕРПОЛ;

3 оказывать необходимую финансовую и административную поддержку этим проектам в пределах имеющихся ресурсов, в том числе предназначенных для обеспечения непрерывности процесса GCI, 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 актуальной информацией об угрозах кибербезопасности, 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 членов в деятельности по повышению квалификации специалистов и созданию потенциала в целях укрепления кибербезопасности;

8 *bis* поддерживать членов в решении проблемы нехватки специалистов по кибербезопасности путем привлечения людей к работе в области кибербезопасности и содействия трудоустройству женщин в сфере 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,

поручает далее Директору Бюро стандартизации электросвязи и Директору Бюро развития электросвязи, каждому в рамках своей сферы ответственности

1 выполнять соответствующие Резолюции ВАСЭ-22 и ВКРЭ-22, в отношении приоритета МСЭ-D в Кигалийском плане действий, 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 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;

4 определять, 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, и поощрять их внедрение;

4 *bis* учитывать особые трудности и потребности в сфере кибербезопасности, с которыми сталкиваются малые и средние предприятия (МСП), внедряя эти конкретные аспекты в деятельность МСЭ по укреплению доверия, уверенности и безопасности при использовании ИКТ;

5 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;

5 *bis* оказывать поддержку Государствам-Членам в определении основных шагов, которые должны быть предприняты всеми для своей защиты от рисков в сфере кибербезопасности, а также поощрять и поддерживать Членов МСЭ и другие заинтересованные стороны в пропагандировании этих шагов среди населения;

6 определять, документально оформлять и пропагандировать 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;

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;

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

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

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

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 продолжать мобилизацию опыта Международного союза электросвязи в области развития в целях укрепления национальной, региональной и международной кибербезопасности для содействия достижению Целей в области устойчивого развития, при взаимодействии с другими соответствующими органами/учреждениями системы Организации Объединенных Наций и другими соответствующими международными органами, принимая во внимание конкретные мандаты и сферы компетенции различных учреждений, учитывая при этом необходимость не допускать дублирования работы между организациями, а также между Бюро или Генеральным секретариатом;

3 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. Кигали, 2022 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 национальных 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;

7 *bis* определить основные шаги, которые должно предпринимать население для того, чтобы защитить себя от рисков кибербезопасности, и поощрять и поддерживать Членов МСЭ и другие заинтересованные стороны к тому, чтобы пропагандировать их,

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, в особенности для уязвимых групп и сообществ, и шагах, которые они могут предпринимать для своей защиты;

5 доводить до сведения общественности итоги обмена информацией между Государствами-Членами, компетентными организациями и специалистами в целях поощрения и расширения знаний населения о кибербезопасности;

6 предусмотреть применение в своих усилиях по укреплению доверия и безопасности при использовании электросвязи/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 *bis* пропагандировать инициативы по привлечению большего числа людей к работе в области кибербезопасности и предоставлять им возможности для прохождения профессиональной подготовки;

6 *ter* оказывать поддержку, с тем чтобы женщины и девушки могли получить доступ к обучению и карьере в области кибербезопасности;

7 взаимодействовать, в надлежащих случаях, для устранения и предупреждения проблем, подрывающих доверие и безопасность при использовании электросвязи/ИКТ, а также совершенствовать решения в области обеспечения защиты кибербезопасности и устойчивости сетей;

8 способствовать усовершенствованию процесса GCI, включая обсуждение методологии, структуры, весовых коэффициентов и вопросов.

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

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)