|  |  |  |  |
| --- | --- | --- | --- |
|  | Всемирная ассамблея по стандартизации  электросвязи (ВАСЭ-24) Нью-Дели, 15−24 октября 2024 года | |  |
|  | | | |
|  | |  | |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | | Дополнительный документ 10 к Документу 37-R | |
|  | | 22 сентября 2024 года | |
|  | | Оригинал: английский | |
|  | | | |
| Администрации стран – членов Азиатско-Тихоокеанского сообщества электросвязи | | | |
| ПРЕДЛАГАЕМЫЕ ИЗМЕНЕНИЯ К РЕЗОЛЮЦИИ 50 | | | |
|  | | | |
|  | | | |

|  |  |  |
| --- | --- | --- |
| **Резюме**: | В настоящем документе содержится предложение по изменению Резолюции 50 ВАСЭ "Кибербезопасность". | |
| **Для контактов**: | Масанори Кондо  (Masanori Kondo)  Генеральный секретарь Азиатско-Тихоокеанское сообщество электросвязи | Эл. почта: [aptwtsa@apt.int](mailto:aptwtsa@apt.int) |

Введение

Безопасность приобретает все большее значение для современной инфраструктуры электросвязи/ИКТ. МСЭ-Т должен играть определенную роль в разработке ключевых технических Рекомендаций, способствующих укреплению доверия, уверенности и безопасности при использовании ИКТ. Основные области исследований составляют обеспечение безопасности с помощью ИКТ и обеспечение безопасности ИКТ.

Безопасность должна рассматриваться на протяжении всего жизненного цикла системы/сети/приложения, в противном случае система/сеть/приложение будет полна уязвимостей безопасности, требующих большого количества исправлений.

Учитывая, что деятельность по стандартизации безопасности способствует предотвращению ущерба от вредоносной кибердеятельности, работу в области безопасности необходимо продолжать. Кроме того, исследовательские комиссии МСЭ-Т, особенно ИК17, должны рассматривать новые определяемые технологии безопасности, такие как безопасность ИИ, безопасность метавселенной, защита при нулевом доверии, безопасность цепочки поставок программного обеспечения и т. д.

Основная цель внесения этих изменений заключается в том, чтобы уточнить и усилить роль ИК17 как ведущей исследовательской комиссии по безопасности.

Предложение

Исходя из вышеизложенного, администрации стран – членов АТСЭ предлагают ВАСЭ-24 рассмотреть возможность пересмотра Резолюции 50 ВАСЭ "Кибербезопасность".

MOD APT/37A10/1

РЕЗОЛЮЦИЯ 50 (Пересм. Нью-Дели, 2024 г.)

Кибербезопасность

(Флорианополис, 2004 г.; Йоханнесбург, 2008 г.; Дубай, 2012 г.; Хаммамет, 2016 г.; Женева, 2022 г.; Нью-Дели, 2024 г.)

Всемирная ассамблея по стандартизации электросвязи (Нью-Дели, 2024 г.),

напоминая

*a)* о Резолюции 130 (Пересм. Бухарест, 2022 г.) Полномочной конференции о роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ);

*b)* о Резолюции 174 (Пересм. Дубай, 2018 г.) Полномочной конференции о роли МСЭ в связи с вопросами международной государственной политики, касающимися риска незаконного использования ИКТ;

*c)* о Резолюции 179 (Пересм. Бухарест, 2022 г.) Полномочной конференции о роли МСЭ в защите ребенка в онлайновой среде;

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

*e)* о резолюциях 55/63 и 56/121 Генеральной Ассамблеи Организации Объединенных Наций (ГА ООН), устанавливающих нормативно-правовые рамки для борьбы с неправомерным использованием информационных технологий в преступных целях;

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

*g)* о резолюции 58/199 ГА ООН о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур;

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

*i)* о резолюции 41/65 ГА ООН о принципах, касающихся дистанционного зондирования Земли из космоса;

*j)* о резолюции 70/125 ГА ООН об итоговом документе совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества;

*k)* 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;

*l)* о Резолюции 52 (Пересм. Хаммамет, 2016 г.) Всемирной ассамблеи по стандартизации электросвязи о противодействии распространению спама и борьбе со спамом;

*m)* о Резолюции 58 (Пересм. Женева, 2022 г.) настоящей ассамблеи о поощрении создания национальных групп реагирования на компьютерные инциденты, в частности для развивающихся стран[[1]](#footnote-1)1;

*n)* что МСЭ является ведущей содействующей организацией по Направлению деятельности C5 ВВУИО в Тунисской программе для информационного общества (Укрепление доверия и безопасности при использовании ИКТ);

*o)* о касающихся кибербезопасности положениях итоговых документов ВВУИО,

учитывая

*a)* решающее значение инфраструктуры электросвязи/ИКТ и ее применения практически для всех видов социально-экономической деятельности;

*b)* что традиционная коммутируемая телефонная сеть общего пользования обладает определенным уровнем присущих ей защитных свойств в силу ее иерархической структуры и встроенных систем управления;

*c)* что сети на базе протокола Интернет (IP) обеспечивают более низкий уровень разделения между пользовательскими и сетевыми компонентами, если не принимать надлежащие меры при проектировании защиты и сферы управления;

*d)* что, таким образом, претерпевающие конвергенцию традиционные сети и IP-сети в большей степени уязвимы в отношении вторжений, если не принимать надлежащие меры при проектировании защиты и сферы управления такими сетями;

*e)* что кибербезопасность является сквозной темой, а среда кибербезопасности является сложной и разноплановой при наличии на национальном, региональном и глобальном уровнях многих различных заинтересованных сторон, которые несут ответственность за определение, рассмотрение вопросов, связанных с укреплением доверия, уверенности и безопасности при использовании ИКТ, и решение этих вопросов;

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

*g)* что тот факт, среди прочих, что важнейшие инфраструктуры электросвязи/ИКТ взаимосвязаны между собой на глобальном уровне, означает, что низкий уровень безопасности инфраструктуры в одной стране может привести к большей степени уязвимости и риска в других странах, и что ввиду этого важно сотрудничество;

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

*i)* что стандарты способны поддерживать аспекты безопасности интернета вещей (IoT) и "умных" городов и сообществ, включая аспекты безопасности для новых и появляющихся технологий;

*j)* что для того, чтобы защитить глобальные инфраструктуры электросвязи/ИКТ от угроз и проблем, связанных с меняющейся средой кибербезопасности, требуются согласованные действия на национальном, региональном и международном уровнях для предотвращения инцидентов в сфере кибербезопасности, готовности к ним и реагирования на них, а также восстановления после них;

*k)* работу, предпринимаемую и проводимую в МСЭ, в том числе в 17‑й Исследовательской комиссии МСЭ-T и 2-й Исследовательской комиссии МСЭ-D, включая заключительный отчет по Вопросу 22/1-1 1-й Исследовательской комиссии МСЭ-D, и по Дубайскому плану действий, принятому ВКРЭ (Дубай, 2014 г.);

*l)* что Сектор стандартизации электросвязи МСЭ (МСЭ-Т) должен играть определенную роль в рамках своего мандата и своей компетенции с учетом пункта *j)* раздела *учитывая*,

учитывая далее,

*а)* что Рекомендация МСЭ-Т Х.1205 содержит определение, описание технологий и принципы защиты сетей в области кибербезопасности;

*b)* что Рекомендация МСЭ-Т Х.805 обеспечивает систематизированную основу для выявления уязвимых мест, Рекомендация МСЭ-T X.509 обеспечивает структуры сертификатов открытых ключей и атрибутов, а в Рекомендации МСЭ-T X.1500 представлена модель обмена информацией о кибербезопасности (CYBEX) и рассматриваются методы, которые можно было бы использовать для содействия обмену информацией о кибербезопасности;

*с)* что в Рекомендации МСЭ-Т X.1060 организациям предлагается основа для создания центра по защите от киберугроз (CDC) и управления таким центром, который обеспечивает безопасность организации, оценку ее эффективности в реализации услуг защиты и устраняет ее риски кибербезопасности;

*d)* что МСЭ-Т и Объединенный технический комитет по информационным технологиям (ОТК1) Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК), а также ряд консорциумов и объединений по разработке стандартов, таких как Консорциум World Wide Web (W3C), Организация по развитию стандартов структурированной информации (OASIS), Альянс Fast IDentity Online (FIDO), Целевая группа по инженерным проблемам интернета (IETF) и Институт инженеров по электротехнике и радиоэлектронике (IEEE), среди прочих, уже имеют значительный объем опубликованных материалов и ими проводится работа, непосредственно связанная с этой темой, что необходимо учитывать;

*e)* значение текущей работы в области эталонной архитектуры безопасности для управления жизненным циклом данных по электронной коммерции,

признавая,

*a)* что в пункте постановляющей части Резолюции 130 (Пересм. Бухарест, 2022 г) Директору Бюро стандартизации электросвязи (БСЭ) поручается повысить интенсивность ведущейся в рамках существующих исследовательских комиссий МСЭ-Т работы;

*b)* что в Резолюции 71 (Пересм. Бухарест, 2022 г.) Полномочной конференции принят Стратегический план на 2024−2027 годы, включая Стратегическую цель 1 ("Универсальная возможность установления соединений: сделать возможным универсальный доступ к приемлемым в ценовом отношении, высококачественным и защищенным электросвязи/ИКТ и содействовать такому доступу"), в соответствии с которой Союз должен достичь универсально доступных, приемлемых в ценовом отношении, высококачественных, функционально совместимых и защищенных инфраструктуры, услуг и приложений электросвязи/информационно-коммуникационных технологий (ИКТ);

*c)* что Глобальная программа кибербезопасности (ГПК) МСЭ содействует международному сотрудничеству, целью которого является предложение стратегий для поиска решений по укреплению доверия и безопасности при использовании ИКТ, принимая во внимание аспекты безопасности на протяжении всего жизненного цикла в ходе процесса разработки стандартов;

*d)* вызовы, с которыми сталкиваются государства, особенно развивающиеся страны, в связи с укреплением доверия и безопасности при использовании ИКТ, и Резолюцию 44 (Пересм. Женева, 2022 г.) ВАСЭ о сокращении разрыва в стандартизации между развивающимися и развитыми странами;

*e)* проблемы, с которыми сталкиваются Государства-Члены, особенно в развивающихся странах, при создании надежной и безопасной инфраструктуры и приложений электросвязи/ИКТ для технических и операционных аспектов защиты данных и информации, позволяющей установить личность (PII),

признавая далее,

*а)* что возникают кибератаки, такие как фишинг, спам, фарминг, скан/вторжение, распределенная атака типа отказ в обслуживании, целенаправленные устойчивые угрозы, искажение внешнего вида веб-сайта, несанкционированный доступ, вредоносное ПО, отравление данных, спуфинг и т. д., которые имеют серьезные последствия;

*b)* что ботнеты используются для распределения вредоносных бот-программ и осуществления кибератак;

*c)* что источники атак иногда трудно определить;

*d)* отмечая, что для борьбы с важнейшими угрозами кибербезопасности применительно к программному и аппаратному обеспечению может требоваться своевременное управление уязвимостями и своевременное обновление аппаратного и программного обеспечения и назначение соответствующих прав доступа для предотвращения атак на оконечные устройства;

*e)* что количество атак программ-вымогателей продолжает расти;

*f)* что применение новых технологий наряду с постоянно развивающейся глобальной инфраструктурой электросвязи/ИКТ ставит новые задачи и предъявляет повышенные требования к безопасности технологий электросвязи/ИКТ и техническим и операционным аспектам защиты данных и PII, что может повлиять на архитектуру сетевой безопасности;

*g)* развитие технологий в области управления угрозами кибербезопасности и защиты электросвязи/ИКТ;

*h)* удовлетворение потребностей в развитии потенциала в области безопасности, включая развитие потенциала персонала в области управления рисками и технологиями безопасности;

*i)* что обеспечение безопасности данных и инфраструктура больших данных являются одними из ключевых компонентов в сфере кибербезопасности, поскольку данные зачастую являются мишенью кибератак, при этом широкое применение технологии больших данных делает эту цель повсеместно распространенной в современном поведении сети;

*j)* что кибербезопасность является ключевым элементом укрепления доверия и безопасности при использовании электросвязи/ИКТ;

*k)* что безопасность занимает важное место на протяжении всего жизненного цикла систем, сетей, приложений и данных;

*l)* что архитектура и структура безопасности имеют важное значение и могут рассматриваться как основа для разработки архитектуры безопасности для различных систем, сетей, приложений и данных,

отмечая

*а)* энергичные действия и заинтересованность в разработке стандартов и Рекомендаций в области безопасности электросвязи/ИКТ в 17-й Исследовательской комиссии, ведущей исследовательской комиссии МСЭ-Т по вопросам безопасности и управления определением идентичности, и в других органах по стандартизации, включая Группу "Глобальное сотрудничество по стандартам" (ГСС);

*b)* что следует оценивать аспекты функциональной совместимости и безопасности развивающейся сетевой инфраструктуры и стремительных инноваций в развитии открытой сетевой инфраструктуры;

*c)* что в дополнение к другим киберугрозам, серьезной проблемой для Государств-Членов стали технические и операционные аспекты защиты данных и PII;

*d)* что нужно обеспечить, по мере возможности, согласование национальных, региональных и международных стратегий и инициатив, чтобы избежать дублирования и использовать ресурсы оптимальным образом;

*e)* значительные совместные усилия со стороны правительств, частного сектора, гражданского общества, технического сообщества и академических организаций в рамках их соответствующих функций и обязанностей, а также между ними, по укреплению доверия, уверенности и безопасности при использовании ИКТ,

решает

1 продолжать уделять этой работе в рамках МСЭ-Т первостепенное значение 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;

2 что всем исследовательским комиссиям МСЭ-Т следует продолжать оценивать существующие и появляющиеся новые Рекомендации в соответствии со своими мандатами, изложенными в Резолюции 2 (Пересм. Женева, 2022 г.) настоящей ассамблеи, с учетом вопросов безопасности на протяжении всего процесса разработки стандартов МСЭ-Т с точки зрения надежности их структуры и функционирования, а также возможности использования злоумышленниками, и принимать во внимание новые и появляющиеся услуги и технологии электросвязи/ИКТ, которые должны поддерживаться глобальной инфраструктурой электросвязи/ИКТ (в том числе, например, облачными вычислениями и IoT, которые базируются на сетях электросвязи/ИКТ);

3 что МСЭ-Т в рамках своего мандата и своей компетенции следует продолжать на глобальном уровне пропагандировать необходимость укреплять и защищать информационные системы и системы электросвязи от киберугроз и злонамеренной кибердеятельности в области безопасности ИКТ путем разработки Рекомендаций и Технических отчетов, поддерживающих процедуры, техническую политику и рамки кибербезопасности, наращивать развитие кадрового потенциала для обеспечения безопасности, а также продолжать содействовать сотрудничеству между соответствующими международными и региональными организациями с целью расширения обмена технической информацией в области безопасности информационных сетей и сетей электросвязи;

4 что МСЭ-Т должен повышать глобальную осведомленность в отношении безопасности в сфере ИКТ путем разработки Рекомендаций и Технических отчетов, обеспечивающих процедуры, техническую политику и основы кибербезопасности с целью более эффективного управления рисками кибербезопасности и защиты своих информационных сетей и сетей электросвязи;

5 что МСЭ-Т должен взаимодействовать с МСЭ-D, в частности в контексте Вопроса 3/2 (Защищенность сетей информации и связи: Передовой опыт по созданию культуры кибербезопасности) МСЭ-D;

6 что соответствующие исследовательские комиссии МСЭ-Т должны следовать за развитием новых и появляющихся технологий согласно своим мандатам, с тем чтобы обратить внимание ИК17 на области, в которых могут потребоваться новые Рекомендации, Добавления и Технические отчеты для решения проблем, связанных с безопасностью, и учета технических и операционных аспектов для защиты данных и PII;

7 что МСЭ-Т должен продолжить работу по разработке и совершенствованию терминов и определений в области укрепления безопасности, уверенности (в том числе посредством защиты данных и информации, позволяющей установить личность) и доверия при использовании электросвязи/ИКТ, включая кибербезопасность;

8 что следует содействовать глобальным согласованным и совместимым процессам обмена информацией, касающейся реагирования на инциденты;

9 что исследовательские комиссии МСЭ-Т должны продолжать поддерживать связи с организациями по разработке стандартов и другими органами, действующими в этой области, и поощрять привлечение экспертов к деятельности МСЭ в области укрепления доверия, уверенности и безопасности при использовании ИКТ;

10 что следует разрабатывать и поддерживать безопасные, надежные и устойчивые сети и услуги электросвязи/ИКТ с целью укрепления доверия и уверенности при использовании электросвязи/ИКТ;

11 что 17-й Исследовательской комиссии необходимо разработать механизмы совместного анализа кибербезопасности и управления инцидентами;

12 что устойчивость сетей и систем ИКТ следует рассматривать в качестве приоритета в области развития сетей, инфраструктуры и приложений электросвязи/ИКТ,

поручает 17-й Исследовательской комиссии

1 содействовать исследованиям в области кибербезопасности, включая безопасность, а также технические и операционные аспекты данных и PII для новых и появляющихся услуг и технологий для преодоления уязвимостей при использовании глобальной инфраструктурой электросвязи/ИКТ путем разработки Рекомендаций, Добавлений и Технических отчетов в зависимости от ситуации;

2 оказывать помощь Директору БСЭ в поддержке "Дорожной карты по стандартам в области безопасности ИКТ", что должно включать направления работы по осуществлению стандартизации, связанной с безопасностью, техническими и операционными аспектами защиты данных и PII, а также сборник по безопасности, в который следует включить перечень Рекомендаций и терминов и их определение, и предоставлять эту информацию соответствующим группам Сектора радиосвязи МСЭ (МСЭ-R) и МСЭ-D, выполняя миссию ведущей исследовательской комиссии по вопросам безопасности;

3 содействовать совместной координационной деятельности в области уверенности, доверия и безопасности среди всех соответствующих исследовательских комиссий и оперативных групп в МСЭ и других организации по разработке стандартов, включая Группу по совместной координационной деятельности по защите ребенка в онлайновой среде и ее анализ разрывов;

4 тесно сотрудничать со всеми другими исследовательскими комиссиями МСЭ-Т, разработать план действий для оценки существующих, дорабатываемых и новых Рекомендаций МСЭ-T по устранению постоянно меняющихся угроз и уязвимостей в области безопасности, чтобы обеспечить устойчивость сетей ИКТ к кибератакам, и продолжать представлять на регулярной основе отчеты по вопросам безопасности электросвязи/ИКТ для Консультативной группы по стандартизации электросвязи;

5 продолжать определять общий/единый комплекс средств безопасности для каждого этапа жизненных циклов информационных систем/сетей/приложений/данных, включая развитие кадрового потенциала для обеспечения безопасности, для того чтобы в результате с самого начала стало возможным обеспечение безопасности на этапе проектного решения (средства и функции безопасности, предусмотренные проектным решением) для систем/сетей/приложений/данных;

6 продолжать разрабатывать одну или несколько структур или эталонных архитектур безопасности с функциональными компонентами безопасности, в том числе с учетом взаимодействия по вопросам безопасности между системами различных типов, которые возможно рассматривать в качестве основы проектирования архитектуры безопасности для разных систем/сетей/приложений/данных, с тем чтобы повысить качество Рекомендаций по вопросам безопасности, и предоставлять справочные документы по проектированию систем безопасности для потенциальных приложений новых технологий в глобальной инфраструктуре электросвязи/ИКТ;

7 учитывать постоянные изменения в технологиях и бизнесе ИКТ, регулярно анализировать Рекомендации по безопасности сетей и пересматривать существующие Рекомендации с целью адаптации к новым требованиям безопасности и реагирования на новые угрозы безопасности сетей;

8 предоставить примеры передового опыта для оценки и улучшения безопасности, технических и операционных аспектов защиты данных и PII в развивающейся инфраструктуре электросвязи/ИКТ,

поручает Директору Бюро стандартизации электросвязи

1 продолжать поддерживать и вести перечень национальных, региональных и международных инициатив и деятельности на основе информационной базы, относящейся к Дорожной карте по стандартам безопасности электросвязи/ИКТ, и на основе деятельности МСЭ-D в области кибербезопасности, а также с помощью других соответствующих организаций, чтобы содействовать в максимально возможной степени всемирному согласованию стратегий и подходов в этой чрезвычайно важной области, включая разработку общих подходов в области кибербезопасности;

2 вносить вклад в ежегодные отчеты Совету МСЭ по укреплению доверия и безопасности при использовании электросвязи/ИКТ, как указано в Резолюции 130 (Пересм. Бухарест, 2022 г.);

3 представлять отчет Совету МСЭ о ходе работы по Дорожной карте по стандартам безопасности электросвязи/ИКТ;

4 продолжать и далее признавать ту роль, которую играют другие организации, обладающие опытом и техническими знаниями в области стандартов безопасности, защиты данных, PII и координировать свою деятельность с этими организациями, в соответствующих случаях;

5 продолжать осуществление и последующие меры в отношении соответствующих видов деятельности, связанной с ВВУИО, в области укрепления доверия и безопасности при использовании электросвязи/ИКТ в сотрудничестве с другими Секторами МСЭ и в сотрудничестве с соответствующими заинтересованными сторонами, что является одним из способов обмена информацией и передовым опытом по национальным, региональным и международным инициативам по вопросам кибербезопасности, носящим недискриминационный характер на глобальном уровне;

6 сотрудничать с ГПК Генерального секретаря и с другими глобальными или региональными проектами в области кибербезопасности, в зависимости от случая, в вопросах содействия созданию потенциала и развитию отношений и партнерских связей с различными региональными и международными организациями и инициативами, занимающимися вопросами кибербезопасности, в зависимости от случая, и предложить всем Государствам-Членам, особенно развивающимся странам, принимать участие в этой деятельности и обеспечивать координацию между этими различными видами деятельности;

7 оказывать поддержку Директору Бюро развития электросвязи (БРЭ) в помощи Государствам-Членам в создании между развивающимися странами соответствующей структуры, которая позволяла бы оперативно реагировать на значительные инциденты, и предложить план действий, направленный на усиление их защиты с учетом механизмов и партнерств, в соответствующих случаях;

8 оказывать поддержку соответствующим видам деятельности исследовательских комиссий МСЭ-Т, связанным с укреплением и созданием доверия, уверенности и безопасности при использовании ИКТ;

9 распространять информацию среди всех заинтересованных сторон и улучшить понимание заинтересованных сторон по вопросам кибербезопасности, путем организации учебных программ, форумов, семинаров-практикумов, семинаров и т. д., в зависимости от ситуации, по Рекомендациям МСЭ-T и руководящим указаниям по реализации для директивных и регуляторных органов, операторов и других заинтересованных сторон, особенно из развивающихся стран;

10 рассматривать, когда это возможно, вопрос о повышения осведомленности путем проведения семинаров-практикумов одновременно с собраниями соответствующих региональных групп исследовательских комиссий МСЭ-Т или мероприятий в координации и сотрудничестве с Директором БРЭ и региональными отделениями МСЭ параллельно с этими собраниями,

предлагает Государствам-Членам, Членам Сектора, Ассоциированным членам и Академическим организациям, в зависимости от обстоятельств,

1 тесно взаимодействовать в рамках усиления регионального и международного сотрудничества, принимая во внимание Резолюцию 130 (Пересм. Бухарест, 2022 г.) Полномочной конференции, с целью укрепления доверия и безопасности при использовании электросвязи/ИКТ для уменьшения рисков и управления угрозами;

2 сотрудничать и активно участвовать в выполнении настоящей Резолюции и в связанной с ней деятельности;

3 участвовать в соответствующих видах деятельности исследовательских комиссий МСЭ-Т по разработке стандартов и руководящих указаний по кибербезопасности в целях укрепления доверия, уверенности и безопасности при использовании ИКТ;

4 применять соответствующие Рекомендации, Технические отчеты и Добавления МСЭ-Т;

5 продолжать вносить свой вклад в работу 17-й Исследовательской комиссии по изучению подходов к управлению рисками кибербезопасности и киберзащитой.

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

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