ITUПубликации
Резолюции

Международный союз электросвязи
Сектор стандартизации

ВСЕМИРНАЯ АССАМБЛЕЯ ПО СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ
Нью-Дели, 15–24 октября 2024 года

Резолюция 50 – Кибербезопасность

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

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. Пусан, 2014 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 64/211 ГА ООН о создании глобальной культуры кибербезопасности и оценке национальных усилий по защите важнейших информационных инфраструктур;

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

i) 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;

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. Кигали, 2022 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. Нью-Дели, 2024 г.) настоящей Ассамблеи о противодействии распространению спама и борьбе со спамом;

m) о Резолюции 58 (Пересм. Нью-Дели, 2024 г.) настоящей Ассамблеи о поощрении создания и совершенствования национальных групп реагирования на компьютерные инциденты (CIRT), в частности для развивающихся стран[1];

n) что МСЭ является ведущей содействующей организацией по Направлению деятельности С5 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 и безопасности при использовании электросвязи/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 всех видов электросвязи/ИКТ;

j) что обеспечение защищенности и безопасности появляющихся технологий электросвязи/ИКТ имеет жизненно важное значение для безопасности киберпространства, что обусловливает решающую роль разработки стандартов безопасности для этих технологий;

---

[1] К таковым относятся наименее развитые страны, малые островные развивающиеся государства, развивающиеся страны, не имеющие выхода к морю, а также страны с переходной экономикой.

k) 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;

l) работу, предпринимаемую и проводимую в МСЭ, в том числе в 17-й Исследовательской комиссии МСЭ-Т и 2-й Исследовательской комиссии МСЭ-D, и по Кигалийскому плану действий, принятому ВКРЭ (Кигали, 2022 г.);

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

учитывая далее,

a) что Рекомендация МСЭ-Т X.1205 содержит определение, описание технологий и принципы защиты сетей;

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

c) 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 уже имеют значительный объем опубликованных материалов и ими проводится работа, непосредственно связанная с этой темой, что необходимо учитывать;

d) значение учета фактора безопасности при использовании технологий электросвязи/ИКТ в качестве непрерывного и итерационного процесса, встроенного в продукты с самого начала и продолжающегося в течение всего их жизненного цикла;

e) что итерационный подход, основанный на оценке рисков и включающий сочетание факторов, ориентированных на технологии, процессы и людей, является ключом к укреплению безопасности и устойчивости при использовании технологий электросвязи/ИКТ, позволяя разрабатывать и применять при необходимости практические методы обеспечения кибербезопасности для борьбы с постоянно меняющимися угрозами и уязвимостями одновременно с поддержкой инноваций и появляющихся технологий электросвязи/ИКТ,

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 Союза 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 будет уделять пристальное внимание достижению универсально доступных, приемлемых в ценовом отношении, высококачественных, функционально совместимых и защищенных инфраструктуры, услуг и приложений электросвязи/ИКТ;

c) что стандарты являются ключевым компонентом Направления 2 (технические и процедурные меры) Глобальной программы кибербезопасности (ГПК) МСЭ, призванной содействовать международному сотрудничеству, целью которого является предложение стратегий для поиска решений по укреплению доверия и безопасности при использовании электросвязи/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 электросвязи/ИКТ,

признавая далее,

a) что растет число и многообразие появляющихся кибератак, таких как фишинг, фарминг, скан/вторжение, распределенная атака типа отказ в обслуживании, искажение внешнего вида веб-сайта и несанкционированный доступ, которые эволюционируют и имеют значительные последствия;

b) что для распределения вредоносных бот-программ и осуществления кибератак может использоваться широкий диапазон векторов;

c) что источники атак иногда трудно определить;

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

e) что обеспечение безопасности данных является одним из ключевых компонентов кибербезопасности, поскольку данные зачастую являются мишенью кибератак;

f) что кибербезопасность является основополагающим элементом укрепления доверия и безопасности при использовании электросвязи/ИКТ;

g) расширение масштабов доступа к электросвязи/ИКТ во всем мире, в частности к интернету, а также их использования несовершеннолетними,

отмечая

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

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

c) что в дополнение к другим киберугрозам, серьезной проблемой для Государств-Членов становятся аспекты кибербезопасности в области защиты данных и информации, позволяющей установить личность (PII);

d) 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 и безопасности при использовании электросвязи/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 электросвязи/ИКТ на национальном, региональном и международном уровнях;

2 что исследовательским комиссиям МСЭ-Т следует, в соответствии со своими мандатами, изложенными в Резолюции 2 (Пересм. Нью-Дели, 2024 г.) настоящей Ассамблеи, продолжать оценивать существующие и появляющиеся Рекомендации МСЭ-Т с точки зрения надежности их структуры и функционирования, а также возможности использования злоумышленниками, передавая соответствующие вопросы безопасности на рассмотрение 17-й Исследовательской комиссии МСЭ-Т, и принимать во внимание новые и появляющиеся услуги и технологии электросвязи/ИКТ, которые должны поддерживаться глобальной инфраструктурой электросвязи/ИКТ;

3 что МСЭ-Т в рамках своего мандата и своей компетенции следует продолжать повышать глобальный уровень осведомленности по вопросам безопасности в области электросвязи/ИКТ путем разработки Рекомендаций и Технических отчетов МСЭ-Т, обеспечивающих основу процедур, технической политики и стандартов кибербезопасности и пропагандирующих важность защиты электросвязи/ИКТ от киберугроз и злонамеренной кибердеятельности, наращивать усилия по развитию кадрового потенциала организаций для обеспечения безопасности, а также продолжать содействовать сотрудничеству между соответствующими международными и региональными организациями с целью расширения обмена технической информацией в области безопасности электросвязи/ИКТ в интересах управления рисками кибербезопасности и защиты электросвязи/ИКТ;

4 что МСЭ-Т следует учитывать потребности пользователей и разработчиков при подготовке итоговых документов, которые могли бы использоваться для содействия обеспечению кибербезопасности появляющихся технологий, относящихся к электросвязи/ИКТ;

5 что МСЭ-Т следует учитывать значение создания потенциала для содействия принятию стандартов в целях поддержки кибербезопасности, в особенности для развивающихся стран, но и не только для них;

6 что МСЭ-Т в этом отношении следует координировать свои действия и сотрудничать с МСЭ-D, как в контексте исследуемого Вопроса 3/2 (Защищенность сетей информации и связи: Передовой опыт по созданию культуры кибербезопасности) МСЭ-D, так и в контексте усилий Бюро развития электросвязи (БРЭ) по созданию потенциала;

7 что соответствующим исследовательским комиссиям МСЭ-Т следует отслеживать развитие новых и появляющихся технологий и услуг электросвязи/ИКТ согласно своим мандатам для того, чтобы сообщать 17-й Исследовательской комиссии МСЭ-Т об областях, которые могут потребовать разработки новых Рекомендаций, Добавлений и Технических отчетов МСЭ-Т в целях решения проблем, связанных с кибербезопасностью и ее аспектами в области защиты данных и PII;

8 что МСЭ-Т должен продолжить работу по разработке и совершенствованию терминов и определений в области укрепления безопасности и доверия при использовании электросвязи/ИКТ, включая термин "кибербезопасность";

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

10 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 и безопасности при использовании электросвязи/ИКТ;

11 что аспекты безопасности следует учитывать на протяжении всего процесса разработки стандартов МСЭ-Т;

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

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

поручает 17-й Исследовательской комиссии Сектора стандартизации электросвязи МСЭ

1 содействовать исследованиям в области кибербезопасности, включая аспекты защиты данных и PII новых и появляющихся услуг и технологий электросвязи/ИКТ, для преодоления уязвимостей при использовании глобальной инфраструктуры электросвязи/ИКТ путем разработки Рекомендаций, Добавлений и Технических отчетов МСЭ-Т, в соответствующих случаях;

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 кибербезопасностью, и ее аспектами защиты данных и PII, а также сборник по безопасности, в который следует включить перечень Рекомендаций МСЭ-Т, терминов и определений, и предоставлять эту информацию соответствующим группам Сектора радиосвязи МСЭ и МСЭ-D, выполняя миссию ведущей исследовательской комиссии МСЭ-Т по вопросам безопасности;

3 руководить совместной координационной деятельностью в области доверия и безопасности среди всех соответствующих исследовательских комиссий МСЭ и других организации по разработке стандартов, в зависимости от случая;

4 тесно сотрудничать со всеми другими исследовательскими комиссиями МСЭ-Т, разработать план действий для оценки существующих, дорабатываемых и новых Рекомендаций МСЭ-Т по реагированию на постоянно меняющиеся угрозы и уязвимости в области безопасности, чтобы стимулировать устойчивость сетей электросвязи/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 на всех этапах жизненного цикла разработки информационных систем/сетей/приложений/услуг, таких как требования, проектирование, реализация, проверка, выпуск и обслуживание, включая развитие кадрового потенциала организаций 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;

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

7 продолжать разрабатывать механизмы совместного анализа кибербезопасности и инструменты управления инцидентами в целях поддержки работы CIRT, в особенности в развивающихся странах;

8 рассматривать возможность выполнения требований, по мере их установления, по разработке технических стандартов в поддержку усилий по повышению уровня онлайновой безопасности для несовершеннолетних;

9 учитывать постоянные изменения в сфере электросвязи/ИКТ, регулярно анализировать и пересматривать существующие Рекомендации МСЭ-Т по безопасности сетей с целью адаптации к новым требованиям безопасности и реагирования на новые угрозы в области безопасности сетей;

10 представлять примеры передового опыта для оценки и совершенствования кибербезопасности, включая аспекты защиты данных и PII, в развивающейся инфраструктуре электросвязи/ИКТ;

11 проводить оценку воздействия новых и появляющихся технологий электросвязи/ИКТ в части кибербезопасности, выявляя разрывы и вырабатывая рекомендации по стратегиям безопасного внедрения и использования,

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 кибербезопасности, включая, в том числе, аспекты кибербезопасности, связанные, среди прочего, со стандартами защиты данных и PI, 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 другими организациями и всеми 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 БРЭ в руководстве разработкой Рекомендаций МСЭ-Т и, возможно, других инструментов, которые Государства-Члены, в частности развивающиеся страны, могут использовать для планирования оперативного реагирования в случае значительных инцидентов, и в содействии этим органам в составлении планов действий с использованием соответствующей структуры, при необходимости и по запросу, направленных на усиление их защиты с учетом механизмов и партнерств;

8 оказывать поддержку соответствующим видам деятельности 17-й исследовательской комиссии МСЭ-Т, связанным с укреплением и созданием доверия и безопасности при использовании электросвязи/ИКТ, и координировать эту работу с работой исследовательских комиссий МСЭ-D, а также с деятельностью в рамках соответствующих программ;

9 распространять информацию среди всех заинтересованных сторон и повышать осведомленность заинтересованных сторон по вопросам кибербезопасности путем организации учебных программ, форумов, семинаров-практикумов, семинаров и т. д., в зависимости от ситуации, по Рекомендациям МСЭ-Т и руководящим указаниям по реализации для директивных и регуляторных органов, операторов и других заинтересованных сторон, особенно из развивающихся стран, с целью повышения уровня осведомленности и определения потребностей в сотрудничестве с Директором БРЭ;

10 работать с региональными организациями электросвязи в целях повышения эффективности предоставления информации и специальных знаний более широкой аудитории;

11 рассматривать, когда это возможно, вопрос о повышении осведомленности путем приурочивания проведения семинаров-практикумов к собраниям соответствующих региональных групп исследовательских комиссий МСЭ-Т или мероприятий в координации и сотрудничестве с Директором БРЭ и региональными отделениями МСЭ параллельно с этими собраниями, когда это целесообразно,

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

1 тесно взаимодействовать в рамках усиления регионального и международного сотрудничества и поддержки, 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 реагирования на угрозы;

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 и безопасности при использовании электросвязи/ИКТ;

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

5 продолжать вносить свой вклад в работу 17-й Исследовательской комиссии МСЭ-Т по изучению подходов к управлению рисками кибербезопасности и киберзащитой, действуя в рамках сферы компетенций МСЭ;

6 продолжать участвовать в инициативах, направленных на поощрение активного участия женщин в мероприятиях и на руководящих постах, связанных с вопросами кибербезопасности, в МСЭ-Т;

7 принять и поддерживать реализацию мер кибербезопасности для новых и появляющихся технологий электросвязи/ИКТ в рамках своих юрисдикций, содействуя тем самым формированию безопасной и устойчивой среды для всех пользователей.