|  |  |
| --- | --- |
| **Всемирная ассамблея по стандартизации  электросвязи (ВАСЭ-20) Женева, 1–9 марта 2022 года** |  |
|  |  |
| **ПЛЕНАРНОЕ ЗАСЕДАНИЕ** | Дополнительный документ 30 к Документу 39-R |
|  | **19 октября 2021 года** |
|  | **Оригинал: английский** |
|  | |
| Государства – члены Межамериканской комиссии по электросвязи (СИТЕЛ) | |
| Предлагаемое изменение Резолюции 50 | |
|  | |
|  | |

|  |  |
| --- | --- |
| **Резюме**: | СИТЕЛ предлагает внести изменения в Резолюцию 50 ВАСЭ. |

Введение

В настоящем вкладе представлено предложение по изменению Резолюции 50 ВАСЭ. Предлагаемый измененный текст включает новое положение в разделе *учитывая* и предполагает перенос в раздел *решает* положения, касающегося необходимости согласования регуляторных стратегий и подходов в отношении безопасности в ИКТ с целью повышения осведомленности на глобальном уровне и содействия координации.

Предложение

Внести указанные изменения в Резолюцию 50.

MOD IAP/39A30/1

РЕЗОЛЮЦИЯ 50 (Пересм. Женева, 2022 г.)

Кибербезопасность

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

Всемирная ассамблея по стандартизации электросвязи (Женева, 2022 г.),

напоминая

*a)* Резолюцию 130 (Пересм. Дубай, 2018 г.) Полномочной конференции о роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ);

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

*c)* Резолюцию 179 (Пересм. Дубай, 2018 г.) Полномочной конференции о роли МСЭ в защите ребенка в онлайновой среде;

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

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

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

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

*h)* резолюцию 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;

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

*j)* Резолюцию 52 (Пересм. Женева, 2022 г.) настоящей Ассамблеи о противодействии распространению спама и борьбе со спамом;

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

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

*m)* касающиеся кибербезопасности положения итоговых документов ВВУИО,

учитывая

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

*b)* 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 ИКТ, и решение этих вопросов;

*c)* что существенный ущерб, который может быть нанесен вследствие недостаточного уровня безопасности ИКТ, является предметом тревоги для всех без исключения развитых и развивающихся стран мира;

*d)* 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;

*e)* 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;

*f)* что стандарты способны поддерживать аспекты безопасности всей электросвязи/ИКТ;

*g)* 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;

*h)* что для защиты глобальной среды электросвязи/ИКТ Членам МСЭ следует рассмотреть набор минимальных требований на национальном уровне для обеспечения сосуществования на международном уровне, а также процедуры, разработанные в рамках Рекомендаций и исследований МСЭ-Т, а также других признанных организаций по стандартизации;

*i)* работу, предпринимаемую и проводимую в МСЭ, в том числе в 17‑й Исследовательской комиссии МСЭ-T, 2-й Исследовательской комиссии МСЭ-D, и по Плану действий Буэнос-Айреса, принятому ВКРЭ (Буэнос-Айрес, 2017 г.);

*j)* 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;

*b)* что Рекомендация МСЭ-Т Х.805 обеспечивает систематизированную основу для выявления уязвимых мест, в Рекомендации МСЭ-T X.509 приведены 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 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), 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;

*d)* значение рассмотрения безопасности при использовании ИКТ как непрерывного и итерационного процесса, изначально встраиваемого в цифровые продукты и услуги и сохраняющегося на протяжении всего срока их службы, а также надлежащего учета рисков, связанных с нарушениями безопасности, в том числе текущей работы в области эталонной архитектуры безопасности для управления жизненным циклом электронного правительства, электронного предпринимательства, электронной коммерции и других услуг электронного общества,

признавая,

*a)* что в пункте постановляющей части Резолюции 130 (Пересм. Пусан, 2014 г.) Директору Бюро стандартизации электросвязи (БСЭ) поручается повысить интенсивность ведущейся в рамках существующих исследовательских комиссий МСЭ-Т работы;

*b)* что что в Резолюции 71 (Пересм. Дубай, 2018 г.) принят Стратегический план на 2020−2023 годы, включая Стратегическую цель 3 *Устойчивость*: *управлять рисками, проблемами и возможностями, возникающими в результате стремительного роста электросвязи/ИКТ*, в соответствии с которой Союз уделяет основное внимание повышению качества, надежности, устойчивости, способности к восстановлению сетей и систем, а также укреплению *доверия и безопасности при использовании 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,

признавая далее,

*а)* что растет спектр и разнообразие кибератак, таких как фишинг, фарминг, скан/вторжение, распределенная атака типа отказ в обслуживании, искажение внешнего вида веб-сайта, несанкционированный доступ и пр., которые имеют серьезные последствия;

*b)* что могут быть использованы различные векторы 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;

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

*f)* что кибербезопасность является одним из элементов укрепления доверия и безопасности при использовании электросвязи/ИКТ,

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

*c)* 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 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 с точки зрения надежности их структуры и возможности использования злоумышленниками, и принимать во внимание новые услуги и появляющиеся приложения, которые должны поддерживаться глобальной инфраструктурой электросвязи/ИКТ (в том числе, например, облачными вычислениями, безопасности на основе квантовых технологий, а также IoT, которые основаны на сетях электросвязи/ИКТ), в соответствии с их мандатами, установленными в Резолюции 2;

3 что МСЭ-Т в рамках своего мандата и своей компетенции следует продолжать пропагандировать необходимость укреплять и защищать информационные системы и системы электросвязи от киберугроз и кибератак и 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 осведомленность на глобальном уровне и освещать национальные стратегии и подходы в отношении безопасности в сфере ИКТ путем разработки Рекомендаций и технических отчетов;

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

6 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";

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

8 что 17-й Исследовательской комиссии, в тесном сотрудничестве со всеми другими исследовательскими комиссиями МСЭ‑Т, следует разработать план действий для оценки существующих, изменяемых и новых Рекомендаций МСЭ-T по противодействию уязвимостям в сфере безопасности и продолжать представлять отчеты по вопросам безопасности электросвязи/ИКТ для Консультативной группы по стандартизации электросвязи (КГСЭ);

9 что исследовательские комиссии МСЭ-Т должны продолжать поддерживать связи с организациями по разработке стандартов и другими органами, действующими в этой области;

10 что аспекты безопасности должны учитываться на протяжении всего процесса разработки стандартов МСЭ-Т,

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 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;

2 вносить вклад в ежегодные отчеты Совету МСЭ по укреплению доверия и безопасности при использовании ИКТ, как указано в Резолюции 130 (Пересм. Дубай, 2018 г.);

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

4 продолжать и далее признавать ту роль, которую играют другие организации, обладающие опытом и техническими знаниями в области стандартов безопасности, 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 ИКТ в сотрудничестве с другими Секторами МСЭ и в сотрудничестве с соответствующими заинтересованными сторонами, что является одним из способов обмена информацией 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, развивать отношения и партнерские связи 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 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 и безопасности при использовании ИКТ,

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. Дубай, 2018 г.) Полномочной конференции, с целью укрепления доверия и безопасности при использовании ИКТ для уменьшения рисков и угроз;

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 ИКТ;

4 применять соответствующие Рекомендации и Добавления МСЭ-Т.

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

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)