|  |  |  |  |
| --- | --- | --- | --- |
|  | Всемирная ассамблея по стандартизации  электросвязи (ВАСЭ-24) Нью-Дели, 15−24 октября 2024 года | |  |
|  | | | |
|  | |  | |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | | Дополнительный документ 15 к Документу 39-R | |
|  | | 13 сентября 2024 года | |
|  | | Оригинал: английский | |
|  | | | |
| Государства – члены Межамериканской комиссии по электросвязи (СИТЕЛ) | | | |
| ПРЕДЛАГАЕМЫЕ ИЗМЕНЕНИЯ К РЕЗОЛЮЦИИ 50 | | | |
|  | | | |
|  | | | |

|  |  |  |
| --- | --- | --- |
| **Резюме**: | СИТЕЛ предлагает внести изменения в Резолюцию 50 ВАСЭ, чтобы обеспечить ее совместимость с изменениями, внесенными в Резолюцию 130 ПК-22 и Резолюцию 45 ВКРЭ-22. Эти усилия по согласованию и гармонизации резолюций направлены на продвижение подхода, ориентированного на безопасность, при котором безопасность органично интегрируется в продукты с момента их создания и постоянно поддерживается на протяжении всего срока их существования. Кроме того, для повышения общей ясности предлагается внести ряд редакционных уточнений. | |
| **Для контактов**: | Мария Селесте Фуэнмайор  (Maria Celeste Fuenmayor)  Межамериканская комиссия по коммуникациям | Эл. почта: [mfuenmayor@oas.org](mailto:mfuenmayor@oas.org) |

MOD IAP/39A15/1

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. Бухарест, 2022 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 защите важнейших информационных инфраструктур;

*h)* о резолюциях 77/211 и 68/167 ГА ООН о праве на неприкосновенность личной жизни в цифрой век;

*i*) о резолюции 76/19 ГА ООН о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности;

*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. 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 и безопасности при использовании ИКТ, и решение этих вопросов;

*f)* что рост киберугроз и кибератак приводит к существенным и увеличивающимся потерям для пользователей систем электросвязи/ИКТ, что вызывает тревогу во всех без исключения странах 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, и других появляющихся услуг и технологий электросвязи/ИКТ;

*j*) что снижение рисков, вызываемых человеческим фактором, является ключевым элементом кибербезопасности;

*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-T и 2-й Исследовательской комиссии МСЭ-D, и по Кигалийскому плану действий, принятому на последней 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 *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, 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, Рекомендация МСЭ-Т X.509 обеспечивает структуру сертификатов открытых ключей и атрибутов;

*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 Ассоциация по стандартам Института инженеров по электротехнике и радиоэлектронике (IEEE-SA), среди прочих, уже имеют значительный объем опубликованных материалов и ими проводится работа, непосредственно связанная с этой темой, что необходимо учитывать;

*d)* значение развития культуры, в которой безопасность рассматривается как непрерывный и итерационный процесс, изначально встраиваемый в продукты и сохраняющийся на протяжении всего срока их службы,

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 уделяет основное 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, которая 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 возник целый спектр разнообразных кибератак, таких как фишинг, фарминг, скан/вторжение, распределенная атака типа отказ в обслуживании, искажение внешнего вида веб-сайта и несанкционированный доступ, 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;

*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;

*g)* что появление новых приложений и технологий, основанных на ИИ, может существенно повлиять на кибербезопасность, создавая новые угрозы и новые стратегии защиты,

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 и IoT, которые базируются на сетях электросвязи/ИКТ), в соответствии с их мандатами, установленными в Резолюции 2 (Пересм. Женева, 2022 г.) настоящей ассамблеи;

3 что МСЭ-Т в рамках своего мандата и своей компетенции следует продолжать пропагандировать важность укрепления и защиты информационных систем и систем электросвязи от киберугроз и злонамеренной кибердеятельности 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 глобальную осведомленность в отношении безопасности в сфере ИКТ путем разработки Рекомендаций и Технических отчетов, обеспечивающих основу процедур, технической политики и стандартов кибербезопасности;

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 услуг и технологий электросвязи/ИКТ согласно своим мандатам для разработки Рекомендаций, Добавлений и Технических отчетов, которые помогают преодолевать проблемы, связанные с безопасностью;

7 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";

8 что следует содействовать согласованным и совместимым процессам обмена информацией, касающейся реагирования на инциденты на национальном, региональном и международном уровнях;

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 и безопасности при использовании ИКТ;

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

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

12 что киберустойчивость сетей и систем ИКТ следует рассматривать в качестве приоритета в области развития сетей и инфраструктуры,

поручает 17-й Исследовательской комиссии

1 содействовать исследованиям в области кибербезопасности, включая безопасность новых и появляющихся услуг и технологий электросвязи/ИКТ, которые будут поддерживаться глобальной инфраструктурой электросвязи/ИКТ;

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, и предоставлять эту информацию соответствующим группам Сектора радиосвязи МСЭ (МСЭ-R) и МСЭ-D, выполняя миссию ведущей исследовательской комиссии МСЭ-T по вопросам безопасности;

3 содействовать совместной координационной деятельности в области безопасности среди всех соответствующих исследовательских комиссий и оперативных групп в МСЭ и других организации по разработке стандартов;

4 тесно сотрудничать со всеми другими исследовательскими комиссиями МСЭ-Т, разработать план действий для оценки существующих, дорабатываемых и новых Рекомендаций МСЭ-T по преодолению уязвимостей безопасности и продолжать представлять на регулярной основе отчеты по вопросам безопасности электросвязи/ИКТ для Консультативной группы по стандартизации электросвязи;

5 определить общий/единый комплекс средств безопасности на всех этапах цикла разработки (требования, проектирование, реализация, проверка, выпуск и обслуживание) информационных систем/сетей/приложений/услуг, для того чтобы с самого начала средства и функции безопасности могли быть интегрированы на всех этапах жизненного цикла продуктов;

6 разработать одну или несколько эталонных структур архитектуры безопасности с функциональными компонентами безопасности, которые возможно рассматривать в качестве основы проектирования архитектуры безопасности для разных систем/сетей/приложений/данных, с тем чтобы повысить качество Рекомендаций по вопросам безопасности;

7 разработать совместные механизмы анализа безопасности и управления инцидентами;

8 продолжать учитывать риски, связанные с человеческим фактором, в области кибербезопасности,

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 Сборнику по безопасности, 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 ИКТ, как указано в Резолюции 130 (Пересм. Бухарест, 2022 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 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 и безопасности при использовании ИКТ;

9 распространять информацию среди всех заинтересованных сторон, связанных с вопросами кибербезопасности, путем организации учебных программ, форумов, семинаров-практикумов, семинаров и т. д. 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 продолжать поддерживать инициативы по поощрению активного участия женщин в деятельности МСЭ-Т в области кибербезопасности и на руководящих должностях, включая "Сеть женщин" (NoW) в МСЭ-Т,

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 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;

5 продолжать вносить свой вклад в работу 17-й Исследовательской комиссии по кибербезопасности, включая подходы к управлению рисками;

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