

РЕЗОЛЮЦИЯ 45 (Пересм. Баку, 2025 г.)

Механизмы совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним

Всемирная конференция по развитию электросвязи (Баку, 2025 г.),

напоминая

- a)* о Резолюции 130 (Пересм. Бухарест, 2022 г.) Полномочной конференции об усилении 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 онлайн-среде;
- d)* о Резолюции 181 (Гвадалахара, 2010 г.) Полномочной конференции об определении и терминологии, связанных с укреплением доверия и безопасности при использовании информационно-коммуникационных технологий;
- e)* о Резолюции 50 (Пересм. Нью-Дели, 2024 г.) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ о кибербезопасности);
- f)* о Резолюции 52 (Пересм. Нью-Дели, 2024 г.) ВАСЭ о противодействии распространению спама и борьбе со спамом;
- g)* о Резолюции 58 (Пересм. Нью-Дели, 2024 г.) ВАСЭ о поощрении создания и укрепления национальных групп реагирования на компьютерные инциденты (CIRT), в частности для развивающихся стран¹;
- h)* о Резолюции 69 (Пересм. Баку, 2025 г.) настоящей Конференции о содействии созданию CIRT, в частности в развивающихся странах, и сотрудничестве между ними;
- i)* о Резолюции 67 (Пересм. Баку, 2025 г.) настоящей Конференции о роли Сектора развития электросвязи МСЭ (МСЭ-D) в защите ребенка в онлайн-среде;

¹ К ним относятся наименее развитые страны, малые островные развивающиеся государства, развивающиеся страны, не имеющие выхода к морю, и страны с переходной экономикой.

- j)* о Резолюции 214 (Бухарест, 2022 г.) Полномочной конференции о технологиях искусственного интеллекта (ИИ) и электросвязи/ИКТ, в которой определяется сфера охвата деятельности Директора Бюро развития электросвязи (БРЭ) по поддержке работы МСЭ-D по решению проблем и использованию возможностей, возникающих в связи с ИИ как новой и появляющейся технологией, применяемой в области кибербезопасности и борьбы со спамом;
- k)* о соответствующих Мнениях шестого Всемирного форума по политике в области электросвязи, которые подпадают под мандат МСЭ-D;
- l)* о благородных принципах, целях и задачах, воплощенных в Уставе Организации Объединенных Наций и во Всеобщей декларации прав человека;
- m)* что МСЭ играет ведущую содействующую роль по Направлению деятельности С5 Тунисской программы для информационного общества (Укрепление доверия и безопасности при использовании ИКТ) Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО);
- n)* об относящихся к кибербезопасности положениях Тунисского обязательства и Тунисской программы ВВУИО;
- o)* о тематических приоритетах действующего Стратегического плана Союза;
- p)* о Женевской декларации принципов ВВУИО, в пункте 37 которой говорится, что "спам представляет для пользователей, сетей и в целом для интернета серьезную проблему, масштабы которой возрастают. Вопросы, касающиеся спама и кибербезопасности, следует рассматривать на соответствующих национальном и международном уровнях";
- q)* об исследуемом Вопросе 3/2 МСЭ-D "Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности";
- r)* об отчете председателя Группы экспертов высокого уровня (HLEG) о Глобальной программе кибербезопасности (ГПК), созданной Генеральным директором МСЭ в соответствии с требованиями Направления деятельности С5 ВВУИО об укреплении доверия и безопасности при использовании ИКТ, и согласно Резолюции 140 (Пересм. Бухарест, 2022 г.) Полномочной конференции о роли МСЭ в качестве ведущей содействующей организации по Направлению деятельности С5 и Резолюции 58 (Пересм. Нью-Дели, 2024 г.) о поощрении создания и совершенствования национальных групп CIRT, в частности для развивающихся стран;

s) что Совет МСЭ на своей сессии 2022 года утвердил Руководящие указания по использованию МСЭ в своей работе ГПК;

t) что МСЭ и Управление Организации Объединенных Наций по наркотикам и преступности (ЮНОДК) подписали Меморандум о взаимопонимании (MoU), направленный на укрепление доверия и безопасности при использовании ИКТ;

u) о Глобальном цифровом договоре, принятом в качестве приложения к резолюции 79/1 Генеральной Ассамблеи Организации Объединенных Наций (ГА ООН), в котором устанавливаются задачи, принципы, обязательства и действия, связанные с цифровой трансформацией²,

учитывая

a) роль электросвязи/ИКТ как эффективных инструментов содействия делу мира, безопасности и стабильности экономического развития, укрепления демократии, социальной сплоченности, надлежащего управления и верховенства права, а также необходимость противодействовать нарастающим проблемам и угрозам, возникающим в результате злоупотребления этими технологиями, в том числе в преступных и террористических целях, обеспечивая при этом соблюдение прав человека (см. также пункт 15 Тунисского обязательства);

b) необходимость обеспечения доверия и безопасности при использовании электросвязи/ИКТ путем укрепления основы для доверия (пункт 39 Тунисской программы) и необходимость того, чтобы правительства в сотрудничестве с другими заинтересованными сторонами в рамках своих соответствующих функций разработали необходимое законодательство, предусматривающее проведение расследования и уголовное преследование киберпреступности, на национальном уровне, и сотрудничали на региональном и международном уровнях с учетом существующих баз;

c) что существование криптографически значимого квантового компьютера будет представлять угрозу для некоторых развернутых средств криптографии, используемых в сетях электросвязи/ИКТ;

d) что в резолюции 64/211 ГА ООН государствам-членам предлагается использовать, если и когда они сочтут это целесообразным, прилагаемый к этой Резолюции инструмент добровольной самооценки национальных усилий;

² Следует отметить, что некоторые Государства-Члены не поддержали Глобальный цифровой договор.

- e)* необходимость разработки Государствами-Членами национальных программ кибербезопасности, опирающихся на национальный план, государственно-частные партнерства, прочную правовую основу, возможности управления инцидентами, наблюдения за инцидентами, оповещения об инцидентах, реагирования на инциденты и восстановления после них, а также на культуру информирования, с использованием, когда это желательно или применимо, в качестве ориентира ряда ресурсов, разработанных и/или предоставленных МСЭ, а также его членами и партнерами;
- 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 кибербезопасности 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)* что существенные и возрастающие потери, которые несут пользователи систем электросвязи/ИКТ в связи с возрастающей во всем мире проблемой инцидентов кибербезопасности, включая те, которые связаны с неправомерным использованием электросвязи/ИКТ в злонамеренных целях, являются предметом тревоги для всех без исключения развитых и развивающихся стран мира;
- h)* причины, предопределившие принятие Резолюции 37 (Пересм. Баку, 2025 г.) настоящей Конференции о преодолении цифрового разрыва, принимая во внимание важность осуществления с участием многих заинтересованных сторон на международном уровне и направления деятельности, указанные в пункте 108 Тунисской программы, в том числе укрепление доверия и безопасности при использовании ИКТ;
- i)* результаты некоторых видов деятельности МСЭ, относящихся к кибербезопасности, особенно, среди прочего, виды деятельности, которые координирует БРЭ, в целях выполнения мандата МСЭ как содействующей организации в осуществлении Направления деятельности C5;
- j)* что различные организации из всех секторов общества совместно работают для обеспечения кибербезопасности услуг и технологий электросвязи/ИКТ и укрепления доверия к ним;
- k)* что все соответствующие заинтересованные стороны могут играть важную роль в повышении осведомленности о вопросах кибербезопасности, в особенности среди женщин, детей, лиц с ограниченными возможностями, лиц с особыми потребностями и лиц с ограниченными возможностями в связи с возрастом возможностями;

l) что тот факт, среди прочих, что критические 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;

m) что многие Государства-Члены сталкиваются со значительной нехваткой квалифицированных кадров в сфере кибербезопасности, что нехватка подготовленных специалистов по кибербезопасности является одним из основных препятствий для кибербезопасности и что важно поощрять большее число людей избирать профессиональную деятельность в области кибербезопасности;

n) что повышение квалификации специалистов и создание потенциала играют ключевую роль в укреплении кибербезопасности, в том числе в необходимом повышении уровня осведомленности и содействия использованию базовых мер безопасности для обеспечения кибергигиены, которые каждый должен принимать для своей защиты от рисков кибербезопасности, включая женщин, детей, лиц с ограниченными возможностями, лиц с особыми потребностями, а также лиц с ограниченными в связи с возрастом возможностями;

o) различная информация, материалы, передовой опыт и финансовые ресурсы, в зависимости от случая, доступны Государствам-Членам через национальные, региональные и другие соответствующие международные организации в соответствии с их конкретным функциями;

p) что в ГПК поощряется международное сотрудничество с целью предложения стратегий для решений по укреплению доверия и безопасности при использовании электросвязи/ИКТ;

q) что кибербезопасность и киберустойчивость стали основополагающими вопросами на национальном, региональном и международном уровнях для обеспечения устойчивого цифрового развития, и что МСЭ-D в рамках своего мандата может продолжать вносить вклад в эту деятельность по укреплению доверия и безопасности при использовании ИКТ,

признавая

a) вызовы, с которыми сталкиваются государства, особенно развивающиеся страны, в связи с укреплением доверия и безопасности при использовании электросвязи/ИКТ;

b) что меры, принимаемые для обеспечения стабильности и безопасности сетей электросвязи/ИКТ, для защиты от киберугроз/киберпреступности и противодействия спаму, должны обеспечивать защиту и соблюдение положений о неприкосновенности частной жизни и о свободе слова, которые содержатся в соответствующих частях Всеобщей декларации прав человека (см. также пункт 42 Тунисской программы) и Международного пакта о гражданских и политических правах;

c) что в резолюции 75/176 ГА ООН о праве на неприкосновенность личной жизни в цифровой век подтверждается, что "права, которыми люди пользуются в обычной жизни, включая право на неприкосновенность частной жизни, должны защищаться и при использовании Интернетом, при этом особое внимание должно уделяться защите детей";

d) необходимость в проведении соответствующих действий и принятии превентивных мер, определяемых законодательством и направленных на борьбу со злоупотреблениями электросвязью/ИКТ, в рамках этических аспектов информационного общества, предусмотренных в Женевских декларации принципов и плане действий ВВУИО (пункт 43 Тунисской программы), необходимость противодействия терроризму во всех его формах и проявлениях в сетях электросвязи/ИКТ при соблюдении прав человека и в соответствии с другими обязательствами по международному праву, которые упоминаются в п. 81 постановляющей части резолюции 60/1 Генеральной Ассамблеи ООН по итогам Всемирного саммита 2005 года, и важность безопасности, последовательности и стабильности интернета, а также необходимость защищать интернет и другие сети ИКТ от угроз и уязвимости (пункт 45 Тунисской программы), при обеспечении неприкосновенности частной жизни и защиты личной информации и личных сведений, будь то посредством принятия законодательства, реализации совместных рамочных программ, использования передового опыта и применения саморегулируемых и технических мер торгово-промышленным сектором и пользователями (пункт 46 Тунисской программы);

e) необходимость принятия эффективных мер в связи с вызовами и угрозами, возникающими в результате использования электросвязи/ИКТ, например в целях, которые несовместимы с задачами по поддержанию международной стабильности и безопасности и могут оказать воздействие на целостность инфраструктуры в рамках отдельных государств, и совместной работы с целью предотвращения неправомерного использования информационных ресурсов и технологий, соблюдая при этом права человека;

f) роль электросвязи/ИКТ в деле защиты детей и содействия их развитию и что следует активизировать деятельность по защите детей и молодежи от растления и защищать их права в контексте электросвязи/ИКТ, подчеркивая, что наилучшее обеспечение интересов ребенка имеет первостепенное значение;

g) стремление и решимость всех заинтересованных сторон построить ориентированное на интересы людей, открытое для всех и защищенное информационное общество, направленное на развитие на основе целей и принципов Устава Организации Объединенных Наций, международного права и принципа многосторонних отношений, соблюдая в полном объеме и поддерживая Всеобщую декларацию прав человека, с тем чтобы люди во всем мире могли создавать информацию и знания, иметь к ним доступ, пользоваться и обмениваться ими в безопасности, для того чтобы в полной мере раскрыть свой потенциал и реализовать согласованные на международном уровне цели и задачи в области развития, включая Цели в области устойчивого развития (ЦУР) на период до 2030 года;

h) положения пунктов 4, 5 и 55 Женевской декларации принципов и что свобода слова и свободный поток информации, идей и знаний благоприятствуют развитию;

i) что Тунисский этап ВВУИО явился уникальной возможностью для повышения уровня информированности о преимуществах, которые электросвязь/ИКТ могут дать человечеству, и о том, как они могут изменить деятельность, взаимоотношения и жизнь людей и, таким образом, укрепить уверенность в будущем при условии безопасного использования электросвязи/ИКТ, как показала реализация решений ВВУИО;

j) что спам является глобальной проблемой, имеющей свои особенности в различных регионах, и что для борьбы с ним необходим подход, основанный на сотрудничестве с участием многих заинтересованных сторон;

k) что манипуляции с представлением информации вызывающей стороны при ее получении пользователем является важным вопросом, касающимся голосового спама, который может возникать из-за уязвимостей в области кибербезопасности, что может потребовать применения надлежащих мер и продолжения международного сотрудничества между всеми заинтересованными сторонами;

l) необходимость принять эффективные меры для решения существенной проблемы, связанной со спамом, о чем говорится в пункте 41 Тунисской программы, а также, в том числе, с кибератаками и инцидентами кибербезопасности;

m) что для защиты пользователей электросвязи/ИКТ, особенно в развивающихся странах, необходимы всеобъемлющие механизмы противодействия спаму,

отмечая

a) необходимость эффективной координации деятельности в рамках МСЭ-D;

- b)* продолжающуюся работу 17-й Исследовательской комиссии (Безопасность) Сектора стандартизации электросвязи МСЭ (МСЭ-Т) и других организаций по разработке стандартов по различным аспектам безопасности электросвязи/ИКТ;
- c)* что спам представляет собой важную проблему и по-прежнему содержит угрозу для пользователей, сетей и интернета в целом и что вопрос кибербезопасности следует решать на соответствующем национальном, региональном и международном уровнях;
- d)* что сотрудничество и совместная деятельность Государств-Членов, Членов Сектора и соответствующих заинтересованных сторон способствуют созданию и поддержанию культуры кибербезопасности;
- e)* продолжающуюся работу частного сектора, академических организаций, технического сообщества и всех остальных соответствующих заинтересованных сторон по содействию обеспечению кибербезопасности в секторе электросвязи/ИКТ;
- f)* что в связи с продолжающимся развитием новых и появляющихся услуг и технологий электросвязи/ИКТ перед странами могут стоять серьезные новые проблемы и открываться новые возможности в области кибербезопасности и противодействия спаму;
- g)* что важным вопросом являются аспекты кибербезопасности, связанные с защитой данных и информации, позволяющей установить личность (PII);
- h)* что необходимо содействовать росту числа и развитию разнообразных и квалифицированных кадров в области кибербезопасности, способных устранять и смягчать риски кибербезопасности, а также способствовать осознанию важности востребованных видов профессиональной квалификации и возможностей профессионального роста,

решает

1 по-прежнему признавать кибербезопасность одним из приоритетных видов деятельности МСЭ, принимая во внимание новые и появляющиеся услуги и технологии электросвязи/ИКТ, и продолжать рассматривать в сфере своей основной компетенции вопрос укрепления безопасности и доверия при использовании электросвязи/ИКТ путем повышения осведомленности, обмена передовым опытом, предоставления помощи в реализации технических мер и разработки соответствующих инструментов и учебных материалов в целях содействия созданию культуры кибербезопасности;

2 продолжать укреплять взаимодействие и сотрудничество, а также обмениваться информацией со всеми соответствующими международными и региональными организациями по вопросам, касающимся кибербезопасности, включая инициативы, связанные с киберустойчивостью, в сферах компетенции МСЭ, учитывая необходимость в оказании помощи развивающимся странам;

3 предложить национальным и международным финансовым организациям уделять больше внимания предоставлению значительной финансовой поддержки, в том числе посредством льготных механизмов кредитования, национальным программам подготовки и обучения практическим навыкам в области кибербезопасности для тех развивающихся стран, которые не располагают соответствующими возможностями в этой сфере, уделяя приоритетное внимание молодежи, женщинам и лицам с ограниченными возможностями;

4 продолжать содействовать развитию партнерских отношений для создания потенциала в области кибербезопасности, с тем чтобы МСЭ-D мог работать с другими соответствующими заинтересованными сторонами и организациями, обладающими специальными знаниями и опытом в этой области;

5 продолжать учитывать аспекты кибербезопасности во всех инициативах и проектах МСЭ-D в области цифрового развития,

порукает Директору Бюро развития электросвязи

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

2 продолжать организовывать в сотрудничестве с соответствующими организациями, в соответствующих случаях, с учетом вкладов членов и во взаимодействии с Директором Бюро стандартизации электросвязи (БСЭ), собрания Государств-Членов, Членов Сектора и других заинтересованных сторон для обсуждения путей и средств повышения кибербезопасности, включая противодействие распространению спама и борьбу с ним;

3 продолжать в сотрудничестве с соответствующими организациями и заинтересованными сторонами проводить исследования по укреплению кибербезопасности и киберустойчивости в развивающихся странах на региональном и международном уровнях на основании четкого определения их потребностей, в первую очередь относящихся к использованию электросвязи/ИКТ, включая противодействие спаму и борьбу с ним, новые и появляющиеся услуги и технологии в области электросвязи/ИКТ, защиту в онлайн-среде детей, молодежи и любого уязвимого лица, а также аспекты кибербезопасности, связанные с защитой данных и информации, PII;

- 4 учитывать результаты Глобального индекса кибербезопасности (GCI) для ориентирования инициатив БРЭ, связанных с кибербезопасностью, уделяя особое внимание разрывам, выявленным в процессе определения GCI;
- 5 поддерживать действующий способ представления результатов GCI, таким образом, чтобы страны были представлены по уровням, а не по индивидуальному рейтингу, для более точного отображения уровня развития кибербезопасности в Государствах-Членах;
- 6 определять и документально оформлять практические меры по поддержке развивающихся стран в создании потенциала и развитии навыков кибербезопасности, принимая во внимание конкретные проблемы, с которыми они сталкиваются;
- 7 поддерживать инициативы Государств-Членов, особенно в развивающихся странах, касающиеся механизмов совершенствования сотрудничества в области кибербезопасности, в том числе по вопросам противодействия спаму и борьбы с ним;
- 8 оказывать поддержку Государствам-Членам в определении основных мер кибербезопасности для обеспечения кибергигиены, которые каждый должен принимать для своей защиты от рисков кибербезопасности и спама, а также поощрять и поддерживать членов МСЭ и другие заинтересованные стороны в популяризации таких мер среди населения;
- 9 оказывать помощь Государствам-Членам, в особенности развивающимся странам, путем предоставления руководящих указаний и передового опыта в отношении проблем и возможностей в области кибербезопасности и противодействия спаму, связанных с новыми и появляющимися услугами и технологиями электросвязи/ИКТ;
- 10 содействовать повышению осведомленности и понимания необходимости подготовки стран к переходу к постквантовой криптографии в сетях электросвязи/ИКТ в рамках сферы компетенции и специальных знаний МСЭ и поощрять членов обмениваться примерами передового опыта и национальным опытом в этой области;
- 11 в сотрудничестве с Директором БСЭ распространять среди развивающихся стран информацию о руководящих указаниях, рекомендациях, технических отчетах и примерах передового опыта, касающихся кибербезопасности, которые были разработаны исследовательскими комиссиями МСЭ-Т, в частности 17-й Исследовательской комиссией как ведущей исследовательской комиссией по вопросам безопасности;

12 способствовать распространению технических Рекомендаций МСЭ-Т и соответствующих информационных ресурсов, разработанных другими организациями, которые могут помочь развивающимся странам в определении и осуществлении мер по предупреждению, обнаружению и смягчению последствий голосового спама, возникающего вследствие уязвимостей в области кибербезопасности, а также содействовать международному сотрудничеству между всеми заинтересованными сторонами;

13 в сотрудничестве с Директором БСЭ помогать развивающимся странам в повышении их степени подготовленности, с тем чтобы обеспечить высокий уровень и эффективность кибербезопасности, включая киберустойчивость, их критических инфраструктур электросвязи/ИКТ, в том числе путем проведения семинаров-практикумов и курсов подготовки, направленных на содействие развитию кибергигиены, и других мероприятий в рамках основных направлений ГПК по организационным, техническим и связанным с созданием потенциала мерам, в соответствующих случаях;

14 помогать Государствам-Членам в создании соответствующей структуры между развивающимися странами, позволяющей быстро обнаруживать и реагировать на значительные инциденты, в том числе оказывая содействие добровольному обмену информацией между заинтересованными администрациями, и предложить план действий, направленный на усиление их защиты и укрепление киберустойчивости с учетом механизмов и партнерств, в соответствующих случаях;

15 параллельно с работой 2-й Исследовательской комиссии МСЭ-D по Вопросу 3/2 осуществлять сбор информации от Государств-Членов и обмен информацией, касающейся правил, политики и других мер, разработанных и/или реализуемых национальными регуляторными органами в сфере электросвязи и другими заинтересованными организациями в целях укрепления доверия и безопасности при использовании электросвязи/ИКТ;

16 поощрять все соответствующие заинтересованные стороны к участию в деятельности центров профессиональной подготовки Академии МСЭ по обучению, образованию и просвещению по вопросам кибербезопасности в рамках ГПК и/или внесению вклада в эту деятельность;

17 оказывать помощь Государствам-Членам путем расширения обмена актуальной информацией по вопросам кибербезопасности и передовым опытом для рассмотрения Государствами-Членами;

18 представить отчет о результатах выполнения настоящей Резолюции следующей всемирной конференции по развитию электросвязи;

19 продолжать консультации с членами по совершенствованию процесса GCI, включая обсуждение методологии, показателей структуры, весовых коэффициентов и вопросов, с привлечением, в надлежащих случаях, Группы экспертов и с учетом финансовых последствий;

20 продолжать оказывать поддержку Сети женщин (NoW) МСЭ-D и другим инициативам в целях поощрения активного участия женщин в деятельности МСЭ-D, связанной с кибербезопасностью, и выполнения ими руководящих функций;

21 развивать, поддерживать и популяризировать хранилище примеров передового опыта по мерам, которые способствуют тому, чтобы люди, особенно женщины и девушки, избирали профессии в области кибербезопасности, и которые поощряют их к этому,

предлагает Генеральному секретарю в координации с Директорами Бюро радиосвязи, Бюро стандартизации электросвязи и Бюро развития электросвязи

1 представить отчет о МоВ между странами, а также о существующих формах сотрудничества, обеспечивая анализ их статуса и сферы применения, а также использования этих механизмов сотрудничества, с целью укрепления кибербезопасности и борьбы с киберугрозами, с тем чтобы обеспечить Государствам-Членам возможность определения необходимости в дополнительных МоВ и механизмах;

2 оказывать содействие региональным и глобальным инициативам в области кибербезопасности и предложить всем странам, в особенности развивающимся странам, принять участие в данной деятельности;

3 продолжать мобилизацию опыта МСЭ в области развития в целях укрепления национальной, региональной и международной кибербезопасности для содействия достижению ЦУР, 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,

просит Генерального секретаря

представлять отчеты о результатах этой деятельности на следующих собраниях Совета и полномочных конференциях, в зависимости от случая,

предлагает Государствам-Членам, Членам Сектора, Ассоциированным членам и Академическим организациям

- 1 обеспечить необходимую поддержку осуществлению настоящей Резолюции и принимать активное участие в ее осуществлении;
- 2 продолжать поддерживать партнерские отношения с МСЭ-D в целях обеспечения необходимых ресурсов для реализации инициатив, таких как проект "Кибертехнологии во благо", направленных на оказание поддержки развивающимся странам, уделяя особое внимание наименее развитым странам, развивающимся странам, не имеющим выхода к морю, и малым островным развивающимся государствам, в развитии их потенциала в области кибербезопасности;
- 3 признать кибербезопасность, в том числе ее аспекты, связанные с воздействием новых и появляющихся услуг и технологий электросвязи/ИКТ, противодействие спаму и борьбу со спамом одной из высокоприоритетных задач и принять соответствующие меры, а также содействовать укреплению доверия и безопасности при использовании электросвязи/ИКТ на национальном, региональном и международном уровнях;
- 4 стимулировать поставщиков услуг защищаться от выявленных рисков кибербезопасности, сводить к минимуму подверженность таким рискам, стремиться обеспечивать непрерывность предоставляемых услуг и уведомлять о нарушениях кибербезопасности в соответствии со своим национальным законодательством;
- 5 содействовать инициативам, которые способствуют тому, чтобы больше людей, особенно женщин и девушек, избирали профессию в области кибербезопасности, в том числе путем разработки соответствующих программ образования и профессиональной подготовки;
- 6 предоставлять информацию об инновационных решениях, направленных на противодействие угрозам кибербезопасности и спаму, и обмениваться этой информацией;
- 7 тесно сотрудничать, с тем чтобы способствовать решению проблем и использованию возможностей, связанных с новыми и появляющимися технологиями, для обеспечения кибербезопасности услуг и технологий электросвязи/ИКТ, а также противодействия спаму, в том числе посредством национальных, региональных и международных усилий, в зависимости от случая;
- 8 сотрудничать на национальном уровне в целях совершенствования процесса выработки решений по поддержанию кибербезопасности и устойчивости сетей;
- 9 информировать МСЭ о существующих механизмах сотрудничества между членами и с другими региональными или международными организациями и учреждениями на двустороннем уровне;

10 представлять вклады для работы в рамках соответствующего исследуемого Вопроса МСЭ-D по кибербезопасности и в рамках других смежных инициатив МСЭ-D по кибербезопасности;

11 содействовать разработке образовательных и учебных программ для повышения осведомленности пользователей о рисках кибербезопасности, особенно для женщин, детей, лиц с ограниченными возможностями и лиц с особыми потребностями, а также лиц с ограниченными в связи с возрастом возможностями, и шагах, которые они могут предпринимать для своей защиты от этих рисков;

12 содействовать разработке инструментов и материалов для повышения уровня кибербезопасности и киберустойчивости среди малых и средних предприятий;

13 принимать участие в совершенствовании процесса GCI, включая обсуждение методологии, показателей, структуры, весовых коэффициентов и вопросов, с привлечением Группы экспертов по GCI;

14 содействовать обсуждениям, обмену информацией, созданию потенциала и исследованиям по проблемам и возможностям в области кибербезопасности и противодействия спаму по мере развития технологий ИИ и их использования в электросвязи/ИКТ, с тем чтобы сделать их более эффективными и функциональными;

15 использовать Академию МСЭ для создания потенциала и профессиональной подготовки в области новых и появляющихся услуг и технологий электросвязи/ИКТ и соответствующих тем, связанных с кибербезопасностью,

предлагает Государствам-Членам

1 собирать и анализировать опыт, связанный с применением новых и появляющихся технологий электросвязи/ИКТ в борьбе со спамом;

2 настоятельно рекомендовать всем соответствующим заинтересованным сторонам содействовать повышению осведомленности населения о рисках кибербезопасности, в особенности среди женщин, детей, лиц с ограниченными возможностями, лиц с особыми потребностями и лиц с ограниченными в связи с возрастом возможностями;

3 активно участвовать в работе МСЭ-D в области кибербезопасности и противодействия распространению спама и борьбы со спамом, организуя технические учебные занятия, а также мероприятия в рамках семинаров-практикумов для регуляторных органов и операторов электросвязи;

4 создать соответствующую структуру, позволяющую быстро реагировать на серьезные инциденты кибербезопасности, и предложить план действий, направленный на предупреждение таких инцидентов, смягчение их последствий и восстановление после них;

- 5 разработать на национальном уровне стратегии и средства для обеспечения защиты национальной критической инфраструктуры, в том числе усиления способности к восстановлению инфраструктуры электросвязи/ИКТ;
- 6 принять меры к развитию своего национального потенциала в области кибербезопасности с учетом основных направлений GCI, если это применимо;
- 7 содействовать обмену информацией по вопросам кибербезопасности на национальном, региональном и международном уровнях;
- 8 вносить вклад в развитие хранилища примеров передового опыта МСЭ по мерам, которые способствуют тому, что больше людей, особенно женщин и девушек, избирают профессии в области кибербезопасности, и которые поощряют их к этому.