# РЕЗОЛЮЦИЯ 45 (Пересм. Кигали, 2022 г.)

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

Всемирная конференция по развитию электросвязи (Кигали, 2022 г.),

*напоминая*

*a)* о Резолюции 130 (Пересм. Дубай, 2018 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. Дубай, 2018 г.) Полномочной конференции о роли МСЭ в защите ребенка в онлайновой 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 45 (Пересм. Дубай, 2014 г.) Всемирной конференции по развитию электросвязи (ВКРЭ);

*f)* о Резолюции 50 (Пересм. Женева, 2022 г.) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) о кибербезопасности;

*g)* о Резолюции 52 (Пересм. Хаммамет, 2016 г.) ВАСЭ о противодействии распространению спама и борьбе со спамом;

*h)* о Резолюции 58 (Пересм. Женева, 2022 г.) ВАСЭ о поощрении создания национальных групп реагирования на компьютерные инциденты (CIRT), в частности для развивающихся стран[1];

*i)* о Резолюции 69 (Пересм. Кигали, 2022 г.) настоящей Конференции о содействии созданию CIRT, в частности в развивающихся странах, и сотрудничестве между ними;

---

[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 67 (Пересм. Кигали, 2022 г.) настоящей Конференции о роли Сектора развития электросвязи МСЭ (МСЭ-D) в защите ребенка в онлайновой среде;

*k)* о соответствующих Мнениях шестого Всемирного форума по политике в области электросвязи (ВФПЭ-21), 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 целях действующего Стратегического плана Союза;

*p)* об исследуемом Вопросе МСЭ-D "Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности", в работе по которому в течение прошлого исследовательского периода участвовали многие члены для составления отчетов, в том числе учебных материалов, предназначенных для использования в развивающихся странах, таких как сборник по национальному опыту, образцы передового опыта для государственно-частных партнерств (ГЧП), образцы передового опыта по созданию CIRT с сопроводительными учебными материалами и образцы передового опыта для основ управления CIRT;

*q)* об отчете председателя Группы экспертов высокого уровня (HLEG) о Глобальной программе кибербезопасности (ГПК), созданной Генеральным директором МСЭ в соответствии с требованиями Направления деятельности С5 об укреплении доверия и безопасности при использовании ИКТ, и согласно Резолюции 140 (Пересм. Дубай, 2018 г.) Полномочной конференции о роли МСЭ в качестве единственной содействующей организации по Направлению деятельности С5 ВВУИО и Резолюции 58 (Пересм. Женева, 2022 г.) о поощрении создания национальных групп CIRT, в частности для развивающихся стран;

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

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

*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 в резолюции 64/211 Генеральной Ассамблеи Организации Объединенных Наций (ГА ООН) государствам-членам предлагается использовать, если и когда они сочтут это целесообразным, прилагаемый к этой Резолюции инструмент добровольной самооценки национальных усилий;

*d)* необходимость разработки Государствами-Членами национальных программ кибербезопасности, опирающихся на национальный план, ГЧП, прочную правовую основу, возможности управления, наблюдения за инцидентами, оповещения, реагирования и восстановления после них, а также на культуру информирования, используя в качестве ориентира отчеты о передовом опыте для разработки национального подхода к вопросам обеспечения кибербезопасности: основы управления для организации национальных мероприятий по обеспечению кибербезопасности;

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

*f)* причины, предопределившие принятие Резолюции 37 (Пересм. Кигали, 2022 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;

*g)* результаты некоторых видов деятельности МСЭ, относящихся к кибербезопасности, особенно, среди прочего, виды деятельности, которые координирует Бюро развития электросвязи, в целях выполнения мандата МСЭ как содействующей организации в осуществлении Направления деятельности С5 (Укрепление доверия и безопасности при использовании ИКТ);

*h)* что различные организации из всех секторов общества совместно работают для обеспечения кибербезопасности электросвязи/ИКТ;

*i)* 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;

*j)* 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;

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

*l)* что кибербезопасность стала крайне важным вопросом на международном уровне для обеспечения устойчивого 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)* 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;

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

*c)* необходимость в проведении соответствующих действий и принятии превентивных мер, определяемых законодательством и направленных на борьбу со злоупотреблениями электросвязью/ИКТ, в соответствии с этическими аспектами информационного общества, предусмотренными 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 сетей электросвязи/ИКТ, а также необходимость защищать сети электросвязи/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);

*d)* необходимость эффективного противодействия вызовам и угрозам, возникающим в результате использования электросвязи/ИКТ, например в целях, которые несовместимы с задачами по поддержанию международной стабильности и безопасности и могут оказать негативное воздействие на целостность инфраструктуры в рамках отдельных государств в ущерб их безопасности, и совместной работы с целью предотвращения злоупотребления информационными ресурсами и технологиями в преступных и террористических целях, соблюдая при этом права человека;

*e)* 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;

*f)* 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 полной 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;

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

*h)* 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 Встречи на высшем уровне;

*i)* 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;

*j)* необходимость принять эффективные меры для решения существенной проблемы, связанной со спамом, о чем говорится в пункте 41 Тунисской программы, а также, в том числе, со спамом, киберпреступностью, вирусами, червями и сетевыми атаками с целью отказа в обслуживании;

*k)* необходимость эффективной координации деятельности в рамках МСЭ-D,

*отмечая*

*a)* продолжающуюся работу 17-й Исследовательской комиссии (Безопасность) МСЭ-Т и других организаций по разработке стандартов по различным аспектам безопасности электросвязи/ИКТ;

*b)* 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;

*c)* что сотрудничество и совместная деятельность Государств-Членов, Членов Сектора и соответствующих заинтересованных сторон способствуют созданию и поддержанию культуры кибербезопасности,

*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, выявления передового опыта, предоставления помощи в реализации технических мер и разработки соответствующих инструментов и учебных материалов в целях содействия созданию культуры кибербезопасности;

2 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,

*поручает 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;

3 продолжать в сотрудничестве с соответствующими организациями и заинтересованными сторонами проводить исследования по укреплению кибербезопасности 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, а также защиту в онлайновой среде детей, молодежи и любого уязвимого лица;

4 учитывать результаты Глобального индекса кибербезопасности (GCI) для ориентирования инициатив БРЭ, связанных с кибербезопасностью, уделяя особое внимание разрывам, выявленным в процессе определения GCI;

5 изменить 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 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;

9 оказывать помощь Государствам-Членам, в особенности развивающимся странам, путем предоставления руководящих указаний и передового опыта для преодоления проблем кибербезопасности и спама, возникающих в связи с новыми и появляющимися технологиями;

10 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;

11 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;

12 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;

13 в сотрудничестве с различными заинтересованными сторонами содействовать рассмотрению соответствующими исследовательскими комиссиями МСЭ-D исследований, связанных с кибербезопасностью;

14 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;

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

16 в сотрудничестве с Директором БСЭ помогать развивающимся странам в совершенствовании процесса развития своего потенциала, проводя семинары-практикумы, семинары или мероприятия в рамках основных направлений ГПК по организационным и техническим мерам;

17 представить отчет о результатах выполнения настоящей Резолюции следующей ВКРЭ;

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

*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 меморандумах 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*

1 довести настоящую Резолюцию до сведения следующей Полномочной конференции в целях рассмотрения и принятия необходимых мер, в соответствующих случаях;

2 представить отчет о результатах этой деятельности на следующих собраниях Совета и Полномочной конференции в зависимости от обстоятельств,

*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 признать кибербезопасность, 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;

3 стимулировать поставщиков услуг защищаться от выявленных рисков, стремиться обеспечивать непрерывность предоставляемых услуг и уведомлять о нарушениях безопасности;

4 сотрудничать на национальном уровне в целях совершенствования процесса выработки решений по поддержанию кибербезопасности и устойчивости сетей;

5 информировать МСЭ о существующих механизмах сотрудничества между членами и с другими региональными или международными организациями и учреждениями на двустороннем уровне,

*предлагает Государствам-Членам*

1 тесно взаимодействовать в целях укрепления регионального и международного сотрудничества, направленного на решение текущих и будущих вопросов, связанных с кибербезопасностью и спамом;

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

3 разработать на национальном уровне стратегии и средства для обеспечения защиты национальной критической инфраструктуры, в том числе усиления способности к восстановлению инфраструктуры электросвязи/ИКТ;

4 содействовать обмену информацией по вопросам кибербезопасности на национальном, региональном и международном уровнях.