|  |  |
| --- | --- |
| **Полномочная конференция (ПК-14)****Пусан, 20 октября – 7 ноября 2014 г.** | logo_R_ |
|  |  |
|  |  |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | **Документ 70-R** |
|  | **10 сентября 2014 года** |
|  | **Оригинал: испанский** |
|  |
| Куба |
| ПРЕДЛОЖЕНИЯ ДЛЯ РАБОТЫ КОНФЕРЕНЦИИ |
|  |
|  |

# I Пересмотр Резолюции 64 (Пересм. Гвадалахара, 2010 г.)

Недискриминационный доступ к современным средствам, услугам и приложениям электросвязи/информационно-коммуникационных технологий,
включая прикладные исследования и передачу технологий,
на взаимно согласованных условиях

# II Пересмотр Резолюции 130 (Пересм. Гвадалахара, 2010 г.)

Усиление роли МСЭ в укреплении доверия и безопасности
при использовании информационно-коммуникационных технологий

# III Пересмотр Резолюции 174 (Гвадалахара, 2010 г.)

Роль МСЭ в связи с вопросами международной государственной
политики, касающимися риска незаконного использования
информационно-коммуникационных технологий

# I Пересмотр Резолюции 64 (Пересм. Гвадалахара, 2010 г.)

Недискриминационный доступ к современным средствам, услугам и приложениям электросвязи/информационно-коммуникационных технологий,
включая прикладные исследования и передачу технологий,
на взаимно согласованных условиях

# 1 Резюме

В настоящем вкладе предлагается обновить Резолюцию 64 (Пересм. Гвадалахара, 2010 г.) с учетом того, что после ее утверждения отмечен рост применения государствами дискриминационного доступа к ресурсам электросвязи/ИКТ, включая:

1.1 отказ в доступе к открытым сайтам и к ресурсам интернета;

1.2 ограничения на доступ к современным технологиям, услугам и приложениям электросвязи/ИКТ и на их передачу.

# 2 Базовая информация и текущая ситуация

На прошедших недавно всемирных конференциях по стандартизации и по развитию электросвязи были утверждены резолюции, касающиеся недискриминационного доступа к средствам и услугам электросвязи/ИКТ, в том числе:

2.1 Всемирная ассамблея по стандартизации электросвязи (Дубай, 2012 г.) приняла Резолюцию 69, в которой Государствам-Членам предлагается воздерживаться от осуществления действий, которые могут помешать другому Государству-Члену осуществлять доступ к открытым интернет-сайтам и использовать ресурсы.

2.2 Всемирная конференция по развитию электросвязи (Дубай, 2014 г.) приняла Резолюцию 37 (Пересм. Дубай, 2014 г.) "Преодоление цифрового разрыва" и признала важность Резолюции 15 (Пересм. Хайдарабад, 2010 г.) "Прикладные исследования и передача технологий" и Резолюции 20 (Пересм. Хайдарабад, 2010 г.) "Недискриминационный доступ к современным средствам, услугам и соответствующим приложениям электросвязи/информационно-коммуникационных технологий".

2.3 Настоящее предложение основано также на:

i) решениях Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), в частности пунктах 15, 18 и 19 Тунисского обязательства и пунктах 90 и 107 Тунисской программы;

ii) роли МСЭ в глобальном развитии электросвязи/ИКТ в соответствии с его мандатом в рамках Направлений деятельности С2, С5 и С6 Тунисской программы и его участии в реализации других направлений деятельности этой Программы, в частности Направлений деятельности С7 и С8;

iii) задачах, установленных в пункте 3 раздела *решает* Резолюции 64, где признается, что МСЭ "следует максимально поощрять сотрудничество Членов Союза по вопросу о недискриминационном доступе к средствам, услугам и приложениям электросвязи и информационных технологий, созданным на базе Рекомендаций МСЭ‑Т и МСЭ‑R, в целях содействия удовлетворению потребностей пользователей в современных услугах и приложениях электросвязи/ИКТ".

В связи с отмеченным выше, администрация Кубы предлагает пересмотр Резолюции 64 (Пересм. Гвадалахара, 2010 г.) для учета предложений, кратко изложенных ниже.

# 3 Краткое содержание изменений к Резолюции 64 (Пересм. Гвадалахара, 2010 г.)

Прилагаем, в установленном для Полномочной конференции 2014 года формате, предложение о внесении изменений в Резолюцию 64 (Пересм. Гвадалахара, 2010 г.), основными направлениями которых являются следующие.

В раздел *напоминая* Резолюции вносятся поправки для учета недавно принятых резолюций, направленных на то, чтобы не допускать дискриминационного доступа к ресурсам электросвязи, путем добавления следующего текста:

ADD: Резолюцию 69 (Пересм. Дубай, 2012 г.) Всемирной ассамблеи по стандартизации электросвязи, в которой всем Государствам-Членам предлагается воздерживаться от осуществления действий, которые могут помешать другому Государству-Члену осуществлять доступ к открытым интернет-сайтам и использовать ресурсы.

В раздел *предлагает правительствам Государств – Членов Союза* вносятся поправки путем добавления следующего положения:

ADD: воздерживаться от осуществления любых односторонних и/или дискриминационных действий, которые могут помешать другому Государству-Члену осуществлять доступ к открытым интернет-сайтам и ресурсам электросвязи или приобретать новые технологии электросвязи, а также современные средства и услуги электросвязи/ИКТ и соответствующие приложения, в духе Статьи 1 Устава МСЭ и принципов ВВУИО.

В связи с вышеизложенным, администрация Кубы предлагает Конференции утвердить изменения к Резолюции 64, содержащиеся в предложении CUB/70/1.

MOD CUB/70/1

РЕЗОЛЮЦИЯ 64 (Пересм. ПУСАН, 2014 Г.)

Недискриминационный доступ к современным средствам, услугам и приложениям электросвязи/информационно-коммуникационных технологий,
включая прикладные исследования и передачу технологий,
на взаимно согласованных условиях

Полномочная конференция Международного союза электросвязи (Пусан, 2014 г.),

напоминая

*а)* результаты Женевского (2003 г.) и Тунисского (2005 г.) этапов Всемирной встречи на высшем уровне по вопросам информационного общества, в частности пункты 15, 18 и 19 Тунисского обязательства и пункты 90 и 107 Тунисской программы для информационного общества;

*b)* Резолюцию 64 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции;

*с)* результаты Всемирной конференции по развитию электросвязи и, в частности, Резолюцию 15 (Пересм. Хайдарабад, 2010 г.) о прикладных исследованиях и передаче технологий, Резолюцию 20 (Пересм. Хайдарабад, 2010 г.) о недискриминационном доступе к современным средствам, услугам и соответствующим приложениям электросвязи/ИКТ и Резолюцию 37 (Пересм. Дубай, 2010 г.) о преодолении цифрового разрыва;

*d)* Резолюцию 69 (Пересм. Дубай, 2012 г.) Всемирной ассамблеи по стандартизации электросвязи, в которой Государствам-Членам предлагается воздерживаться от осуществления действий, которые могут помешать другому Государству-Члену осуществлять доступ к открытым интернет-сайтам и использовать ресурсы,

принимая во внимание

значение электросвязи/информационно-коммуникационных технологий (ИКТ) для политического, экономического, социального и культурного прогресса,

принимая во внимание также,

*а)* что МСЭ играет значительную роль в деле содействия глобальному развитию электросвязи/ИКТ и приложений ИКТ в рамках мандата МСЭ, в частности в реализации Направлений деятельности С2, С5 и С6 Тунисской программы, а также участвует в реализации других направлений деятельности, в частности Направлений деятельности С7 и С8 Тунисской программы;

*b)* что с этой целью Союз координирует усилия, направленные на обеспечение гармоничного развития средств электросвязи/ИКТ, позволяя осуществлять недискриминационный доступ к этим средствам и к современным услугам и приложениям электросвязи;

*с)* что этот доступ поможет преодолеть цифровой разрыв,

принимая во внимание, кроме того,

необходимость подготовки предложений по вопросам, определяющим стратегию развития электросвязи/ИКТ и приложений ИКТ во всемирном масштабе в рамках мандата МСЭ, а также содействия мобилизации ресурсов, требуемых для этой цели,

отмечая,

*а)* что современные средства, услуги и приложения электросвязи/ИКТ создаются, в основном, на базе Рекомендаций Сектора стандартизации электросвязи МСЭ (МСЭ‑Т) и Сектора радиосвязи МСЭ (МСЭ‑R);

*b)* что Рекомендации МСЭ‑Т и МСЭ‑R являются результатом коллективных усилий всех сторон, участвующих в процессе стандартизации в рамках МСЭ, и принимаются Членами Союза на основе консенсуса;

*с)* что ограничения в доступе к средствам, услугам и приложениям электросвязи/ИКТ, от которых зависит развитие национальной электросвязи и которые создаются на базе Рекомендаций МСЭ‑Т и МСЭ‑R, являются препятствием гармоничному развитию и совместимости электросвязи во всемирном масштабе;

*d)* Резолюцию 15 (Пересм. Хайдарабад, 2010 г.) о прикладных исследованиях и передаче технологии;

*e)* Резолюцию 20 (Пересм. Хайдарабад, 2010 г.) о недискриминационном доступе к современным средствам, услугам и соответствующим приложениям электросвязи/ИКТ;

*f)* Стратегический план Союза, изложенный в Резолюции 71 (Пересм. Пусан, 2014 г.) настоящей конференции,

признавая,

что достижение полной согласованности сетей электросвязи невозможно без обеспечения недискриминационного доступа всех без исключения стран, участвующих в работе Союза, к новым технологиям электросвязи, современным средствам, услугам и соответствующим приложениям электросвязи/ИКТ, включая прикладные исследования и передачу технологий, на взаимно согласованных условиях, без нанесения ущерба национальным нормам и международным обязательствам, относящимся к компетенции других международных организаций,

решает

1 продолжать в рамках мандата МСЭ удовлетворять потребность в обеспечении недискриминационного доступа к созданным на базе Рекомендаций МСЭ‑Т и МСЭ‑R технологиям, средствам, услугам и соответствующим приложениям электросвязи и информационных технологий, включая прикладные исследования и передачу технологии на взаимно согласованных условиях;

2 что МСЭ следует способствовать недискриминационному доступу к средствам, услугам и приложениям электросвязи и информационных технологий, созданным на базе Рекомендаций МСЭ‑Т и МСЭ‑R;

3 что МСЭ следует максимально поощрять сотрудничество Членов Союза по вопросу о недискриминационном доступе к средствам, услугам и приложениям электросвязи и информационных технологий, созданным на базе Рекомендаций МСЭ‑Т и МСЭ‑R, в целях содействия удовлетворению потребностей пользователей в современных услугах и приложениях электросвязи/ИКТ,

поручает Директорам трех Бюро

в рамках соответствующих сфер их компетенции выполнить настоящую Резолюцию и достичь ее целей,

предлагает правительствам Государств − Членов Союза

1 содействовать производителям оборудования электросвязи/ИКТ и поставщикам услуг и приложений в обеспечении того, чтобы средства, услуги и приложения электросвязи/ИКТ, созданные на базе Рекомендаций МСЭ‑Т и МСЭ‑R, могли быть доступными населению без какой-либо дискриминации, а также в содействии прикладным исследованиям и передаче технологий;

2 сотрудничать между собой в целях осуществления настоящей Резолюции;

3 воздерживаться от осуществления любых односторонних и/или дискриминационных действий, которые могут помешать другому Государству-Члену осуществлять доступ к открытым интернет-сайтам и ресурсам электросвязи или приобретать новые технологии электросвязи, а также современные средства и услуги электросвязи/ИКТ и соответствующие приложения, в духе Статьи 1 Устава МСЭ и принципов ВВУИО,

поручает Генеральному секретарю

передать текст настоящей Резолюции Генеральному секретарю Организации Объединенных Наций в целях доведения до мирового сообщества позиции МСЭ как специализированного учреждения Организации Объединенных Наций по вопросу недискриминационного доступа к новым технологиям электросвязи и информационным технологиям и современным средствам, услугам и соответствующим приложениям электросвязи/ИКТ в рамках мандата МСЭ как важного фактора мирового технологического прогресса, а также прикладных исследований и передачи технологий Государствам-Членам на взаимно согласованных условиях, который может способствовать преодолению цифрового разрыва.

# II Пересмотр Резолюции 130 (Пересм. Гвадалахара, 2010 г.)

Усиление роли МСЭ в укреплении доверия и безопасности
при использовании информационно-коммуникационных технологий

# 1 Резюме

В настоящем вкладе предлагается обновить Резолюцию 130 (Пересм. Гвадалахара, 2010 г.) в интересах обеспечения доверия и безопасности при использовании ИКТ с учетом того, что в последние годы они все более широко используются при совершении преступных действий, угрожающих функционированию инфраструктур электросвязи, сохранению мира и социально-экономическому развитию Государств-Членов, включая:

• нарушение конфиденциальности связи и защиты личных данных пользователей;

• рассылку спама по электронной почте или через подвижные системы обмена сообщениями (SMS или MMS) с политическими и маркетинговыми целями;

• изменение маршрутизации трафика и ухудшение качества услуг электросвязи.

# 2 Базовая информация

В Резолюции 130 (Пересм. Гвадалахара, 2010 г.) признается необходимость мониторинга воздействия таких угроз и указывается:

"*b)* что при применении и развитии информационно-коммуникационных технологий (ИКТ) возникают новые угрозы из различных источников, которые оказывали воздействие на степень доверия и безопасности при использовании ИКТ всеми Государствами-Членами, Членами Секторов и другими заинтересованными сторонами, включая всех пользователей ИКТ, а также воздействие на сохранение мира и социально-экономическое развитие всех Государств-Членов";

"*e)* что для защиты таких инфраструктур, решения этих проблем и противодействия этим угрозам требуются скоординированные действия на национальном, региональном и международном уровнях, направленные на предотвращение, подготовку, а также реагирование на тот или иной инцидент с компьютерной безопасностью".

Кроме того, следует принимать во внимание резолюции, принятые Всемирной ассамблеей по стандартизации электросвязи (Дубай, 2012 г.) и Всемирной конференцией по развитию электросвязи (Дубай, 2014 г.), в частности:

i) Резолюцию 50 "Кибербезопасность" и Резолюцию 52 "Противодействие распространению спама и борьба со спамом", утвержденные ВАСЭ;

ii) Резолюцию 45 "Механизмы совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним" и Резолюцию 69 "Содействие созданию национальных групп реагирования на компьютерные инциденты, в частности в развивающихся странах, и сотрудничеству между ними", принятые ВКРЭ.

В связи с вышеизложенным, администрация Кубы предлагает пересмотр Резолюции 130 (Пересм. Гвадалахара, 2010 г.) для учета предложений, кратко изложенных ниже.

# 3 Предлагаемые изменения к Резолюции 130 (Пересм. Гвадалахара, 2010 г.)

Прилагаем, в установленном для Полномочной конференции 2014 года формате, предлагаемые изменения, при этом основные исправления являются следующими:

3.1 Внесение изменений в пункт *b)* раздела *учитывая* для определения новых форм кибератак путем добавления следующей формулировки:

MOD: "… возникают новые угрозы из различных источников, такие как фишинг, бот-сети, распределенные атаки типа отказа в обслуживании и др., серьезные последствия которых включают возможное скрытое и незаконное использование отдельными лицами, организациями и государствами компьютерных систем других стран для атак на третьи страны…".

3.2 Внесение изменений в пункт 2 раздела *поручает Генеральному секретарю и Директорам Бюро* путем добавления следующего положения:

MOD: в соответствии с Резолюцией 45 (Пересм. Дубай, 2014 г.) представлять Совету ежегодный отчет, включающий анализ данных об инцидентах, предоставленных Государствами-Членами, а также оценку эффективности плана действий по усилению роли МСЭ в укреплении доверия и безопасности при использовании ИКТ.

3.3 Внесение изменений в раздел *поручает Генеральному секретарю* путем включения следующего пункта:

MOD: 1 изучить в рамках Совета вопрос, связанный с выполнением эффективного плана действий по укреплению роли МСЭ в создании доверия и безопасности при использовании ИКТ, принимая во внимание деятельность трех Секторов в этом отношении.

3.4 Внесение изменений в раздел *предлагает Государствам-Членам* путем добавления следующих положений:

ADD: 2 укреплять региональное и международное сотрудничество, принимая во внимание Резолюцию 45 (Пересм. Дубай, 2014 г.), с помощью заключения соглашений и внедрения мер, направленных на содействие уменьшению рисков и угроз доверию и безопасности при использовании ИКТ;

ADD: 3 воздерживаться от использования ИКТ для деятельности:

i) связанной с экстерриториальным перехватом и мониторингом сообщений таким образом, который нарушает конфиденциальность связи и защиту личных данных пользователей;

ii) угрожающей доверию и безопасности при использовании ИКТ, сохранению мира и социально-экономическому развитию других Государств-Членов; и

iii) отрицательно воздействующей на маршрутизацию трафика и качество услуг электросвязи,

ADD: информировать Генерального секретаря о любых инцидентах такого рода, которые упоминаются выше.

**4** В связи с вышеизложенным, администрация Кубы предлагает Конференции утвердить изменения к Резолюции 130, содержащиеся в предложении CUB/70/2.

MOD CUB/70/2

РЕЗОЛЮЦИЯ 130 (ПЕРЕСМ. ПУСАН, 2014 Г.)

Усиление роли МСЭ в укреплении доверия и безопасности
при использовании информационно-коммуникационных технологий

Полномочная конференция Международного союза электросвязи (Пусан, 2014 г.),

напоминая

*а)* Резолюцию 130 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции;

*b)* Резолюцию 69 (Пересм. Дубай, 2014 г.) Всемирной конференции по развитию электросвязи (ВКРЭ) о создании национальных групп реагирования на компьютерные инциденты (CIRT), в частности в развивающихся странах, и сотрудничестве между ними;

*с)* что в Резолюции 1305 Совета МСЭ, принятой на его сессии 2009 года, защита, безопасность, целостность, жизнеспособность и устойчивость интернета определены как вопросы государственной политики, относящиеся к сфере компетенции МСЭ,

учитывая

*а)* решающее значение информационно-коммуникационных инфраструктур и их применений для практически всех видов социально-экономической деятельности;

*b)* что при применении и развитии информационно-коммуникационных технологий (ИКТ) возникают новые угрозы из различных источников, такие как фишинг, бот-сети, распределенные атаки типа отказа в обслуживании и др., серьезные последствия которых включают возможное скрытое и незаконное использование отдельными лицами, организациями и государствами компьютерных систем других стран для атак на третьи страны, которые оказывали воздействие на степень доверия и безопасности при использовании ИКТ всеми Государствами-Членами, Членами Секторов и другими заинтересованными сторонами, включая всех пользователей ИКТ, а также воздействие на сохранение мира и социально-экономическое развитие всех Государств-Членов; и что угрозы сетям и их уязвимость продолжают создавать проблемы все большего масштаба, невзирая на национальные границы, в отношении безопасности для всех стран, в частности для развивающихся стран, включая наименее развитые страны, малые островные развивающиеся государства, развивающиеся страны, не имеющие выхода к морю, и страны с переходной экономикой, при этом отмечая в данном контексте усиление роли МСЭ в укреплении доверия и безопасности при использовании ИКТ и необходимость дальнейшего укрепления международного сотрудничества, а также развития надлежащих существующих национальных, региональных и международных механизмов (например, соглашений, примеров передового опыта, меморандумов о взаимопонимании и т. п.);

*с)* что Генеральному секретарю МСЭ было предложено поддержать Международное многостороннее партнерство против киберугроз (ИМПАКТ), Форум групп реагирования на инциденты и обеспечения безопасности (FIRST) и другие глобальные и региональные проекты в области кибербезопасности, в зависимости от случая, и что всем странам, в частности развивающимся странам, предложено принять участие в их деятельности;

*d)* Глобальную программу кибербезопасности (ГПК) МСЭ;

*e)* что для защиты таких инфраструктур, решения этих проблем и противодействия этим угрозам требуются скоординированные действия на национальном, региональном и международном уровнях, направленные на предотвращение, подготовку, а также реагирование на тот или иной инцидент с компьютерной безопасностью и восстановление после него со стороны органов государственного управления на национальном (включая создание национальных групп CIRT) и субнациональном уровнях со стороны частного сектора, граждан и пользователей в дополнение к международному и региональному сотрудничеству и координации и что МСЭ должен играть ведущую роль в этой области в соответствии со своими мандатом и компетенцией;

*f)* необходимость постоянного развития новых технологий для обеспечения раннего обнаружения событий или инцидентов, ставящих под угрозу компьютерную безопасность, а также скоординированного и своевременного реагирования на них, или инцидентов с безопасностью компьютерных сетей, которые могут поставить под угрозу доступность, целостность и конфиденциальность важнейших инфраструктур в Государствах − Членах МСЭ, и разработки стратегий, которые сведут к минимуму воздействие таких инцидентов и снизят растущие риски и угрозы, которым подвергаются такие платформы,

признавая,

*а)* что развитие ИКТ имело и продолжает иметь решающее значение для роста и развития глобальной экономики на основе безопасности и доверия;

*b)* что Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО) подтвердила большое значение укрепления доверия и безопасности при использовании ИКТ, чрезвычайную важность осуществления решений при участии многих заинтересованных сторон на международном уровне и разработала Направление деятельности С5 (Укрепление доверия и безопасности при использовании ИКТ), по которому МСЭ назван в Тунисской программе для информационного общества ведущей/содействующей организацией для этого направления деятельности и что Союз выполнял эту задачу в последние годы, например, в рамках ГПК;

*c)* что ВКРЭ-14 приняла Дубайский план действий и его Программу по кибербезопасности, в которой кибербезопасность определяется в качестве приоритетного направления деятельности Бюро развития электросвязи (БРЭ) и устанавливаются направления деятельности, которые должно осуществлять БРЭ; а также приняла Резолюцию 45 (Пересм. Дубай, 2014 г.), касающуюся механизмов совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним, в которой Генеральному секретарю предлагается довести Резолюцию до сведения следующей полномочной конференции с целью ее рассмотрения и принятия необходимых мер, в соответствующих случаях; и Резолюцию 69 (Пересм. Дубай, 2014 г.) о создании национальных групп CIRT, в частности в развивающихся странах, и сотрудничестве между ними; и что, кроме того, 17-й Исследовательской комиссией Сектора стандартизации электросвязи МСЭ (МСЭ-Т) изучается вопрос о создании национального центра безопасности сетей общего пользования на базе IP для развивающихся стран;

*d)* что в целях поддержки создания национальных групп CIRT в Государствах-Членах, в которых существует необходимость в наличии групп CIRT и в которых такие группы в настоящее время отсутствуют, Всемирная ассамблея по стандартизации электросвязи (ВАСЭ) приняла Резолюцию 58 (Пересм. Дубай, 2012 г.), касающуюся поощрения создания национальных групп CIRT, в частности в развивающихся странах, а ВКРЭ-14 приняла Резолюцию 69 (Пересм. Дубай, 2014 г.) о создании национальных групп CIRT, в частности в развивающихся странах, и сотрудничестве между ними;

*e)* п. 15 Тунисского обязательства, где говорится: "Признавая принципы универсального и недискриминационного доступа всех стран к ИКТ, необходимость принятия во внимание уровня социально-экономического развития каждой страны и уважая ориентированные на развитие аспекты информационного общества, мы подчеркиваем, что ИКТ являются эффективным инструментом содействия делу мира, безопасности и стабильности, усиления демократии, социальной сплоченности, надлежащего управления и верховенства права на национальном, региональном и международном уровнях. ИКТ могут использоваться для содействия экономическому росту и развитию предприятий. Для достижения этих целей ключевое значение имеет развитие инфраструктуры, создание человеческого потенциала, информационная безопасность и безопасность сетей. Мы далее признаем необходимость эффективного противодействия проблемам и угрозам, возникающим в результате использования ИКТ 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. Необходимо предотвращать злоупотребление информационными ресурсами и технологиями в преступных и террористических целях и соблюдать права человека", и что после ВВУИО проблемы, возникающие в результате этого ненадлежащего использования ресурсов ИКТ, только продолжают возрастать;

*f)* что Государствам-Членам, в особенности развивающимся странам, при разработке соответствующих осуществимых правовых мер, касающихся защиты от киберугроз на национальном, региональном и международном уровнях, может потребоваться помощь МСЭ, в том что касается разработки технических и процедурных мер, направленных на защиту элементов национальной инфраструктуры ИКТ, которая предоставляется по просьбе этих Государств-Членов, отмечая при этом, что существует ряд региональных и международных инициатив, в рамках которых этим странам может оказываться поддержка в разработке таких правовых мер;

*g)* Мнение 4 (Лиссабон, 2009 г.) Всемирного форума по политике в области электросвязи о совместных стратегиях по укреплению доверия и безопасности при использовании ИКТ;

*h)* соответствующие результаты работы ВАСЭ-12, а именно:

i) Резолюцию 50 (Пересм. Дубай, 2012 г.) о кибербезопасности;

ii) Резолюцию 52 (Пересм. Дубай, 2012 г.) о противодействии распространению спама и борьбе со спамом;

*i)* что Резолюция 69 (Пересм. Дубай, 2014 г.) предусматривает создание групп CIRT,

отдавая себе отчет в том,

*a)* что МСЭ и другие международные организации в рамках различных видов деятельности анализируют вопросы, относящиеся к укреплению доверия и безопасности при использовании ИКТ, включая стабильность и меры по противодействию спаму, вредоносным программным средствам и т. п. и по защите личных данных и неприкосновенности частной жизни;

*b)* что 17-я Исследовательская комиссия МСЭ-Т, 1-я и 2‑я Исследовательские комиссии Сектора развития электросвязи (МСЭ-D) и другие соответствующие исследовательские комиссии МСЭ продолжают работать над техническими средствами обеспечения безопасности информационных сетей и сетей связи в соответствии с Резолюциями 50 и 52 (Пересм. Дубай, 2012 г.) и Резолюциями 45 (Пересм. Дубай, 2014 г.) и 69 (Пересм. Дубай, 2014 г.);

*с)* что МСЭ должен играть основополагающую роль в укреплении доверия и безопасности при использовании ИКТ;

*d)* что в Мнении 4 (Лиссабон, 2009 г.) о совместных стратегиях по укреплению доверия и безопасности при использовании ИКТпредлагается МСЭ продолжать – главным образом на основе вкладов и рекомендаций Членов Союза – осуществлять дальнейшие инициативы и виды деятельности в тесном партнерстве с другими соответствующими национальными, региональными и международными объединениями и организациями в соответствии с Резолюцией 71 (Пересм. Пусан, 2014 г.) настоящей конференции, касающейся Стратегического плана Союза на 2012−2015 годы, и всеми соответствующими резолюциями МСЭ;

*e)* что 1-я Исследовательская комиссия МСЭ-D продолжает проводить исследования, предусмотренные в Вопросе 22-1/1 МСЭ-D "Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности", которые отражены в резолюции 64/211 Генеральной Ассамблеи Организации Объединенных Наций,

отмечая,

*а)* что в качестве межправительственной организации, участие в работе которой принимает частный сектор, МСЭ занимает надлежащее положение, для того чтобы играть важную роль совместно с другими соответствующими международными органами и организациями в противодействии угрозам и уязвимости, которые влияют на усилия по укреплению доверия и безопасности при использовании ИКТ;

*b)* пп. 35 и 36 Женевской декларации принципов и п. 39 Тунисской программы, касающиеся укрепления доверия и безопасности при использовании ИКТ;

*с)* что хотя отсутствуют общепринятые определения спама и других терминов в этой области, спам был охарактеризован 2-й Исследовательской комиссией МСЭ-Т на ее собрании в июне 2006 года как термин, обычно используемый для обозначения незапрашиваемой массовой рассылки электронных сообщений по электронной почте или на мобильные телефоны (SMS, MMS), как правило, с целью продвижения товаров и услуг коммерческого характера;

*d)* инициативы Союза, касающиеся ИМПАКТ и FIRST;

*е)* что Программа 2 БРЭ Дубайского плана действий была принята при том понимании со стороны делегаций ВКРЭ-14, что БРЭ не занимается разработкой законопроектов,

памятуя

о работе МСЭ, закрепленной в Резолюциях 50 и 52 (Пересм. Дубай, 2012 г.) и 58 (Пересм. Дубай, 2012 г.), Резолюциях 45 (Пересм. Дубай, 2014 г.) и 69 (Пересм. Дубай, 2014 г.), Программе БРЭ по кибербезопасности Дубайского плана действий; соответствующих Вопросах МСЭ-Т, касающихся технических аспектов безопасности информационных сетей и сетей связи; и Вопросе 22‑1/1 МСЭ-D,

решает

1 продолжать уделять этой работе в рамках МСЭ высокий приоритет в соответствии с его компетенцией и техническими знаниями и опытом;

2 придать высокий приоритет работе МСЭ, описанной в разделе памятуя, выше, в соответствии с его сферами компетенции и опытом, принимая во внимание при этом необходимость избегать дублирования работы в рамках трех Бюро и Генерального секретариата либо работы, которая в большей степени соответствует мандатам других межправительственных и соответствующих международных органов;

3 что МСЭ должен сосредоточить ресурсы и программы на тех областях кибербезопасности, которые соответствуют его основному мандату и опыту, в особенности в технической сфере и сфере развития, и не включать области, относящиеся к применению Государствами-Членами правовых или политических принципов, связанных с национальной обороной, национальной безопасностью, контентом и киберпреступностью, которые относятся к их суверенным правам; при том что это, однако, не препятствует выполнению МСЭ своего мандата по разработке технических рекомендаций, предназначенных для уменьшения уязвимости инфраструктуры ИКТ, и не препятствует предоставлению МСЭ всей той помощи, которая была согласована на ВКРЭ-14, включая виды деятельности в рамках Программы по кибербезопасности, например "*содействие Государствам-Членам, в частности развивающимся странам, в разработке надлежащих и действенных законодательных мер, касающихся защиты от киберугроз"*, и виды деятельности в рамках Вопроса 22-1/1,

поручает Генеральному секретарю и Директорам Бюро

1 продолжать анализировать:

i) работу, проделанную к настоящему времени тремя Секторами в рамках инициативы МСЭ по Глобальной программе кибербезопасности и другими соответствующими организациями, и инициативы по противодействию существующим и будущим угрозам, таким как вопросы противодействия спаму, масштабы которого растут и расширяются, для того чтобы укрепить доверие и безопасность при использовании ИКТ;

ii) ход работы по выполнению настоящей Резолюции, при том что МСЭ продолжает играть руководящую роль в качестве ведущей/содействующей организации по Направлению деятельности С5 при помощи консультативных групп в соответствии с Уставом МСЭ и Конвенцией МСЭ;

2в соответствии с Резолюцией 45 (Пересм. Дубай, 2014 г.) представлять Совету ежегодный отчет, включающий анализ данных об инцидентах, предоставленных Государствами-Членами, а также оценку эффективности плана действий по усилению роли МСЭ в укреплении доверия и безопасности при использовании ИКТ;

3 способствовать доступу к средствам и ресурсам в пределах имеющегося бюджета, необходимым для укрепления доверия и безопасности при использовании ИКТ, для всех Государств-Членов в соответствии с разработанными ВВУИО положениями об универсальном и недискриминационном доступе к ИКТ для всех стран;

4 продолжать поддерживать портал кибербезопасности как средство совместного использования информации о национальных, региональных и международных инициативах, связанных с кибербезопасностью во всем мире;

5 ежегодно представлять Совету отчет об этой деятельности и в надлежащих случаях вносить предложения;

6 далее укреплять координацию между соответствующими исследовательскими комиссиями и программами,

поручает Директору Бюро стандартизации электросвязи

1 активизировать работу в существующих исследовательских комиссиях МСЭ-Т, с тем чтобы:

i) противодействовать существующим и будущим угрозам и уязвимости, которые влияют на усилия по укреплению доверия и безопасности при использовании ИКТ, разрабатывая, в надлежащих случаях, отчеты и рекомендации, с тем чтобы выполнить резолюции ВАСЭ-12, в частности Резолюции 50 и 52 (Пересм. Дубай, 2012 г.) и 58 (Пересм. Дубай, 2012 г.), допуская начало работы до утверждения Вопроса;

ii) изыскивать способы расширения обмена технической информацией в этих областях, содействовать принятию протоколов и стандартов, укрепляющих безопасность, и способствовать международному сотрудничеству между соответствующими объединениями;

iii) содействовать осуществлению проектов, разработанных во исполнение решений ВАСЭ-12, в частности:

a) Резолюции 50 (Пересм. Дубай, 2012 г.) о кибербезопасности;

b) Резолюции 52 (Пересм. Дубай, 2012 г.) о противодействии распространению спама и борьбе со спамом;

2 продолжать сотрудничать с соответствующими организациями с целью обмена передовым опытом и распространения информации, например путем проведения совместных семинаров‑практикумов и курсов профессиональной подготовки, в рамках групп по совместной координационной деятельности и посредством письменных вкладов, представляемых соответствующими организациями на основе сделанного им предложения,

поручает Директору Бюро развития электросвязи

1 в тесном сотрудничестве с соответствующими партнерами разрабатывать в соответствии с результатами ВКРЭ-10 и во исполнение Резолюции 45 (Пересм. Дубай, 2014 г.), Резолюции 69 (Пересм. Дубай, 2014 г.) и Программы 2 Хайдарабадского плана действий проекты расширения сотрудничества в области кибербезопасности и противодействия спаму, направленные на удовлетворение потребностей развивающихся стран;

2 в ответ на поступающие просьбы оказывать поддержку усилиям Государств – Членов МСЭ по созданию потенциала путем: упрощения доступа Государств-Членов к ресурсам, созданным другими соответствующими международными организациями, которые занимаются разработкой национального законодательства для борьбы с киберпреступностью; поддержки усилий, предпринимаемых Государствами – Членами МСЭ на национальном и региональном уровнях, по созданию потенциала для защиты от киберугроз/киберпреступности при сотрудничестве между ними; в соответствии с национальным законодательством Государств-Членов, упомянутым выше, путем оказания помощи Государствам-Членам, в частности развивающимся странам, в разработке надлежащих и осуществимых правовых мер, связанных с защитой от киберугроз на национальном, региональном и международном уровнях; введения технических и процедурных мер, направленных на защиту национальной инфраструктуры ИКТ, с учетом работы соответствующих исследовательских комиссий МСЭ-Т и, в надлежащих случаях, других соответствующих организаций; создания организационных структур, таких как CIRT, для выявления киберугроз, их учета и реагирования на них, а также механизмов сотрудничества на региональном и международном уровнях;

3 оказывать необходимую финансовую и административную поддержку для этого проекта в пределах имеющихся ресурсов и изыскивать дополнительные ресурсы (в денежной и натуральной формах) для осуществления этого проекта в рамках соглашений о партнерстве;

4 обеспечивать координацию работы по этому проекту в контексте общей деятельности МСЭ в роли ведущей/содействующей организации по Направлению деятельности С5 ВВУИО, и исключить любое дублирование деятельности по этой важной проблематике с Генеральным секретариатом и МСЭ‑Т;

5 координировать работу по этому проекту с работой исследовательских комиссий МСЭ-D по этой теме, а также с деятельностью в рамках соответствующих программ и деятельностью Генерального секретариата;

6 продолжать сотрудничать с соответствующими организациями с целью обмена передовым опытом и распространения информации, например путем проведения совместных семинаров-практикумов и курсов профессиональной подготовки;

7 ежегодно представлять Совету отчет об этой деятельности и в надлежащих случаях вносить предложения,

далее поручает Директору Бюро стандартизации электросвязи и Директору Бюро развития электросвязи

в рамках сферы ответственности каждого:

1 выполнять соответствующие Резолюции ВАСЭ-12 и ВКРЭ-14, в том числе программу действий по обеспечению поддержки и помощи развивающимся странам в укреплении доверия и безопасности при использовании ИКТ;

2 выявлять наличие и содействовать доступности для Государств-Членов, Членов Секторов и соответствующих организаций информации об укреплении доверия и безопасности при использовании ИКТ, в частности связанной с инфраструктурой на базе ИКТ;

3 не допуская дублирования работы в рамках Вопроса 22-1/1 МСЭ-D, выявлять примеры передового опыта в области создания групп CIRT и подготовить справочное руководство для Государств-Членов, а также, в надлежащих случаях, участвовать в работе по Вопросу 22-1/1;

4 взаимодействовать с соответствующими организациями и, при необходимости, с другими соответствующими международными и национальными экспертами, с тем чтобы выявлять примеры передового опыта в области создания групп реагирования на компьютерные инциденты (CIRT);

5 принять меры к тому, чтобы новые Вопросы рассматривались исследовательскими комиссиями в рамках Секторов в аспекте формирования доверия и безопасности при использовании ИКТ;

6 оказывать поддержку в области стратегии, организации, информационно-пропагандистской деятельности, сотрудничества, оценки и развития профессиональных навыков;

7 обеспечивать необходимую техническую и финансовую помощь в пределах существующих бюджетных ресурсов в соответствии с Резолюцией 58 (Пересм. Дубай, 2012 г.);

8 осуществлять мобилизацию требуемых внебюджетных ресурсов вне регулярного бюджета Союза на выполнение настоящей Резолюции в целях оказания помощи развивающимся странам,

поручает Генеральному секретарю

в соответствии с его инициативой по данному вопросу:

1 изучить в рамках Совета вопрос, связанный с выполнением эффективного плана действий по укреплению роли МСЭ в создании доверия и безопасности при использовании ИКТ, принимая во внимание деятельность трех Секторов в этом отношении;

2 осуществлять сотрудничество в этом отношении с соответствующими международными организациями, в том числе путем принятия меморандумов о взаимопонимании, при условии утверждения Советом согласно Резолюции 100 (Миннеаполис, 1998 г.) Полномочной конференции,

просит Совет

включить отчет Генерального секретаря в документы, рассылаемые Государствам-Членам в соответствии с п. 81 Конвенции,

предлагает Государствам-Членам

1 рассмотреть присоединение к соответствующим надлежащим международным и региональным инициативам по совершенствованию национальных нормативно-правовых баз, имеющих отношение к безопасности информационных сетей и сетей связи;

2 укреплять региональное и международное сотрудничество, принимая во внимание Резолюцию 45 (Пересм. Дубай, 2014 г.), с помощью заключения соглашений и внедрения мер, направленных на содействие уменьшению рисков и угроз доверию и безопасности при использовании ИКТ;

3 воздерживаться от использования ИКТ для деятельности:

i) связанной с экстерриториальным перехватом и мониторингом сообщений таким образом, который нарушает конфиденциальность связи и защиту личных данных пользователей;

ii) угрожающей доверию и безопасности при использовании ИКТ, сохранению мира и социально-экономическому развитию других Государств-Членов; и

iii) отрицательно воздействующей на маршрутизацию трафика и качество услуг электросвязи;

4 информировать Генерального секретаря о любых инцидентах такого рода, которые упоминаются выше,

предлагает Государствам-Членам, Членам Секторов и Ассоциированным членам

1 представлять вклады по этой теме соответствующим исследовательским комиссиям МСЭ и в отношении любой другой деятельности, за которую Союз несет ответственность;

2 вносить вклад в укрепление доверия и безопасности при использовании ИКТ на национальном, региональном и международном уровнях путем осуществления деятельности, определенной в п. 12 Женевского плана действий, и содействовать подготовке исследований в этих областях;

3 содействовать разработке образовательных и учебных программ для повышения осведомленности пользователя о рисках в киберпространстве.

# III Пересмотр Резолюции 174 (Гвадалахара, 2010 г.)

Роль МСЭ в связи с вопросами международной государственной
политики, касающимися риска незаконного использования
информационно-коммуникационных технологий

# 1 Резюме

В настоящем вкладе предлагается обновить Резолюцию 174 (Гвадалахара, 2010 г.) "Роль МСЭ в связи с вопросами международной государственной политики, касающимися риска незаконного использования информационно-коммуникационных технологий" в связи с усилением тенденции к незаконному использованию ИКТ. Предлагается добавить в раздел *решает* новый абзац, в котором указывается, что МСЭ следует продолжать содействовать информированности о необходимости защиты информационных систем и систем электросвязи от угроз кибератак и продолжать содействовать сотрудничеству между международными и региональными организациями в этих целях.

# 2 Базовая информация

После Полномочной конференции (Гвадалахара, 2010 г.) Всемирная ассамблея по стандартизации электросвязи и Всемирная конференция по развитию электросвязи изучали вопрос об угрозе кибератак, приняв следующие резолюции:

i) резолюции, принятые ВКРЭ (Дубай, 2014 г.), в частности Резолюции 45 "Механизмы совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним" и 69 "Содействие созданию национальных групп реагирования на компьютерные инциденты, в частности в развивающихся странах, и сотрудничеству между ними";

ii) резолюции, принятые ВАСЭ (Дубай, 2012 г.), в частности Резолюции 52 "Противодействие распространению спама и борьба со спамом" и 50 "Кибербезопасность", в которых, посредством следующего раздела решает, признается необходимость осуществлять мониторинг воздействия таких угроз:

 "что МСЭ-Т в рамках своей деятельности и своего влияния следует продолжать пропагандировать необходимость защищать информационные системы и системы электросвязи от угрозы 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".

В связи с вышеизложенным, администрация Кубы предлагает пересмотр Резолюции 174 (Гвадалахара, 2010 г.) для учета предложений, кратко изложенных ниже.

# 3 Предлагаемые изменения к Резолюции 174 (Гвадалахара, 2010 г.)

Прилагаем, в установленном для Полномочной конференции 2014 года формате, предлагаемые изменения, при этом основные исправления являются следующими:

3.1 Внесение изменений в раздел *вновь подтверждая* Резолюции 174 путем добавления следующего положения:

ADD: *e)* резолюцию 68/243 Генеральной Ассамблеи Организации Объединенных Наций о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности.

3.2 Внесение изменений в раздел *напоминая* Резолюции 174 путем добавления следующего положения:

ADD: *h)* что Вопрос 22/1 Сектора развития электросвязи МСЭ (МСЭ-D) касается обеспечения безопасности информационно-коммуникационных сетей с помощью выявления передового опыта в целях развития культуры кибербезопасности, а также что ВКРЭ-14 приняла Резолюцию 45 (Пересм. Дубай, 2014 г.) "Механизмы совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним".

3.3 Внесение изменений в постановляющую часть Резолюции путем добавления следующего положения в раздел *решает поручить Генеральному секретарю*:

ADD: iii) в рамках своей деятельности и своего влияния продолжать пропагандировать необходимость защищать информационные системы и системы электросвязи от угроз 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** В связи с вышеизложенным, администрация Кубы предлагает Конференции утвердить изменения к Резолюции 174, содержащиеся в предложении CUB/70/3.

MOD CUB/70/3

РЕЗОЛЮЦИЯ 174 (ПЕРЕСМ. ПУСАН, 2014 Г.)

Роль МСЭ в связи с вопросами международной государственной
политики, касающимися риска незаконного использования
информационно-коммуникационных технологий

Полномочная конференция Международного союза электросвязи (Пусан, 2014 г.),

отдавая себе отчет в том,

*a)* что технические инновации, обусловленные информационно-коммуникационными технологиями (ИКТ), существенным образом изменили способы, с помощью которых люди получают доступ к электросвязи;

*b)* что незаконное использование ИКТ может причинять вред инфраструктуре, национальной безопасности и экономическому развитию Государств-Членов;

c) что согласно определению, содержащемуся в Уставе МСЭ, электросвязь – это "любая передача, излучение или прием знаков, сигналов, письменного текста, изображений и звуков или сведений любого рода по проводной, радио-, оптической или другим электромагнитным системам",

вновь подтверждая

*a)* резолюции 55/63 и 56/121 Генеральной Ассамблеи Организации Объединенных Наций, в которых создается нормативно-правовая база для борьбы с неправомерным использованием информационных технологий в преступных целях;

*b)* резолюцию 57/239 Генеральной Ассамблеи Организации Объединенных Наций о создании глобальной культуры кибербезопасности;

*с)* резолюцию 58/199 Генеральной Ассамблеи Организации Объединенных Наций о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур;

*d)* резолюцию 41/65 Генеральной Ассамблеи Организации Объединенных Наций о принципах, касающихся дистанционного зондирования Земли из космоса;

e) резолюцию 68/243 Генеральной Ассамблеи Организации Объединенных Наций о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности,

учитывая,

*a)* что в Женевской декларации принципов, принятой на Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО) (Женева, 2003 г.), поддерживается деятельность Организации Объединенных Наций по предотвращению потенциального использования ИКТ в целях, которые несовместимы с задачами поддержания международной стабильности и безопасности и могут отрицательно влиять на целостность инфраструктуры в государствах, нанося ущерб их безопасности, и что необходимо предотвращать использование информационных ресурсов и технологий в преступных и террористических целях, соблюдая при этом права человека (пункт 36 Женевской декларации принципов ВВУИО);

*b)* что в Направлении деятельности C5 (Укрепление доверия и безопасности при использовании ИКТ) Женевского плана действий говорится: "*Органам государственного управления в сотрудничестве с частным сектором необходимо предупреждать, обнаруживать проявления киберпреступности и ненадлежащего использования ИКТ и реагировать на эти проявления путем разработки руководящих принципов, которые учитывали бы ведущуюся в этой области работу; изучения законодательства, которое дает возможность эффективно расследовать и подвергать преследованию ненадлежащее использование; содействия эффективным мерам взаимопомощи; усиления на международном уровне институциональной поддержки профилактики таких инцидентов, их обнаружения и ликвидации их последствий; а также путем содействия образованию и повышению осведомленности*",

учитывая далее,

что ВВУИО (Тунис, 2005 г.) определила МСЭ в качестве ведущей организации по выполнению Направления деятельности C5 (Укрепление доверия и безопасности при использовании ИКТ),

напоминая

*a)* Резолюцию 130 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции по усилению роли МСЭ в укреплении доверия и безопасности при использовании ИКТ;

*b)* Резолюцию 102 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции о роли МСЭ в вопросах международной государственной политики, касающихся интернета и управления ресурсами интернета, включая наименования доменов и адреса;

c) Резолюцию 71 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции, в частности Стратегическую цель 4: "Разрабатывать инструменты, основываясь на вкладах членов, для содействия созданию доверия у конечных пользователей, а также для гарантии эффективности, безопасности, целостности и возможности взаимодействия сетей";

*d)* Резолюции 1282 и 1305 Совета МСЭ, в последней из которых в числе основных задач Специализированной группы в определении вопросов международной государственной политики, касающихся интернета, перечислены вопросы, относящиеся к использованию и ненадлежащему использованию интернета;

*e)* Резолюцию 45 (Пересм. Дубай, 2014 г.) Всемирной конференции по развитию электросвязи (ВКРЭ) по механизмам совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу со спамом;

*f)* Дубайскую декларацию, принятую ВКРЭ, в частности Программу по кибербезопасности;

*g)* Резолюции 50 и 52 (Пересм. Дубай, 2012 г.) Всемирной ассамблеи по стандартизации электросвязи о кибербезопасности и противодействии спаму и борьбе со спамом, соответственно;

*h)* что Вопрос 22/1 Сектора развития электросвязи МСЭ (МСЭ-D) касается обеспечения безопасности информационно-коммуникационных сетей с помощью выявления передового опыта в целях развития культуры кибербезопасности, а также что ВКРЭ-14 приняла Резолюцию 45 (Пересм. Дубай, 2014 г.) "Механизмы совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним",

признавая далее,

*a)* что глобальное взаимодействие и сотрудничество между международными организациями необходимы для изучения и предотвращения незаконного использования ИКТ;

*b)* ведущую и содействующую роль, возложенную на Союз по Направлению деятельности С5, упомянутому выше,

отмечая

*a)* большое значение ИКТ, включая электросвязь, для социально-экономического развития стран, в частности развивающихся стран, благодаря созданию новых служб общего пользования, которые содействуют доступу населения к информации и увеличению прозрачности государственных администраций и могут быть полезными для осуществления мониторинга и наблюдения за изменением климата, управления природными ресурсами и сокращения риска стихийных бедствий;

*b)* уязвимость важнейших национальных инфраструктур, их растущую зависимость от ИКТ и угрозы, являющиеся результатом незаконного использования ИКТ,

решает поручить Генеральному секретарю

принять необходимые меры, для того чтобы:

i) повышать уровень информированности Государств-Членов о неблагоприятном воздействии, которое может явиться результатом незаконного использования информационно-коммуникационных ресурсов;

ii) поддерживать роль МСЭ в целях сотрудничества, в рамках своего мандата, с другими органами Организации Объединенных Наций в борьбе с незаконным использованием ИКТ;

iii) в рамках своей деятельности и своего влияния продолжать пропагандировать необходимость защищать информационные системы и системы электросвязи от угроз 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,

просит Генерального секретаря

в качестве руководителя содействующей организации по осуществлению Направления деятельности 5, касающегося укрепления безопасности и доверия при использовании ИКТ, организовывать собрания Государств-Членов и соответствующих заинтересованных сторон в области ИКТ, в том числе поставщиков геопространственных и информационных услуг, для того чтобы обсудить альтернативные подходы к решениям, направленным на устранение и предотвращение незаконного использования ИКТ, принимая при этом во внимание общие интересы отрасли ИКТ,

предлагает Государствам-Членам и соответствующим заинтересованным сторонам в области ИКТ

продолжать диалог на региональном и национальном уровнях в целях поиска взаимоприемлемых решений,

предлагает Генеральному секретарю

осуществлять сбор информации о передовых методах с точки зрения мер, принимаемых Государствами-Членами для предотвращения незаконного использования ИКТ и оказания помощи заинтересованным Государствам-Членам, в соответствующих случаях,

поручает Генеральному секретарю

представить отчет Совету и следующей полномочной конференции о выполнении настоящей Резолюции,

предлагает Государствам-Членам

оказать необходимую поддержку для выполнения настоящей Резолюции.

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