



# Генеральная Ассамблея

Distr.: General  
15 December 2009  
Russian  
Original: English

---

## Шестьдесят четвертая сессия

Пункт 55(с) повестки дня

### **Глобализация и взаимозависимость: наука и техника в целях развития**

#### **Доклад Второго комитета\***

*Докладчик:* г-жа Денис Маккуэйд (Ирландия)

#### **I. Введение**

1. Второй комитет провел обсуждения по существу пункта 55 повестки дня (см. A/64/422, пункт 2). Решения по подпункту (с) принимались на 30, 33, 37 и 38-м заседаниях 3, 10 и 25 ноября и 1 декабря 2009 года. Информация о ходе рассмотрения Комитетом этого подпункта содержится в соответствующих кратких отчетах (A/C.2/64/SR.30, 33, 37 и 38).

#### **II. Рассмотрение проектов резолюций**

##### **A. Проекты резолюций A/C.2/64/L.8 и Rev.1**

2. На 30-м заседании 3 ноября представитель Соединенных Штатов Америки от имени Австралии, Болгарии, Израиля, Канады, Маршалловых Островов, Республики Корея, Соединенного Королевства Великобритании и Северной Ирландии, Эстонии и Японии внес на рассмотрение проект резолюции, озаглавленный «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» (A/C.2/64/L.8), следующего содержания:

*«Генеральная Ассамблея,*

*ссылаясь на свои резолюции 55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года о борьбе с преступным использованием информационных технологий, 57/239 от 20 декабря 2002 года о создании глобальной культуры кибербезопасности и 58/199 от 23 декабря 2003 года о создании*

---

\* Доклад Комитета по данному пункту публикуется в четырех частях под условными обозначениями A/64/422 и Add.1–3.



глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур,

*ссылаясь также* на свои резолюции 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года и 63/37 от 2 декабря 2008 года о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности,

*ссылаясь далее* на итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества, состоявшейся 10–12 декабря 2003 года в Женеве (первый этап) и 16–18 ноября 2005 года в Тунисе (второй этап), в которых государства признали, что свобода выражения мнений и свободный поток информации, идей и знаний имеют существенное значение для информационного общества и благоприятствуют развитию и что, поскольку доверие и безопасность относятся к главным опорам информационного общества, необходимо поощрять, формировать, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности,

*признавая* все более незаменимый вклад сетевых информационных технологий в выполнение большинства важнейших функций в повседневной жизни, торговлю и обеспечение товарами и услугами, научные исследования, инновационную деятельность и предпринимательство и свободную передачу информации между физическими лицами, организациями и правительствами;

*отмечая*, что правительства, деловые круги, гражданское общество и физические лица все более зависят от глобальной сети информационных инфраструктур и что такая зависимость будет лишь возрастать,

*отмечая также*, что отсутствие равного доступа к информационным технологиям и возможностей их использования государствами может подорвать их социально-экономическое процветание, и особо отмечая потребности менее развитых стран в передовых практических методах и профессиональной подготовке в вопросах кибербезопасности,

*выражая обеспокоенность* по поводу того, что угрозы надежному функционированию важнейших информационных инфраструктур и целостности информации, передаваемой по этим сетям, приобретают все более изощренный и серьезный характер, отрицательно сказываясь на уровне семейного, национального и международного благополучия,

*подтверждая*, что обеспечение защищенности важнейших информационных инфраструктур — это обязанность, которую правительства должны систематически выполнять, выступая с соответствующими инициативами на национальном уровне, в координации с заинтересованными сторонами, которые, в свою очередь, должны знать о соответствующих рисках, превентивных мерах и эффективных мерах реагирования, соответствующих возложенным на них функциям,

*признавая*, что национальные усилия должны подкрепляться обменом информацией и взаимодействием на национальном, региональном и международном уровнях, с тем чтобы можно было эффективно противостоять таким угрозам, приобретающим все более транснациональный характер,

*отмечая* работу соответствующих региональных и международных организаций по укреплению кибербезопасности, особенно тех из них, которые поддерживают национальные усилия и поощряют международное сотрудничество,

*отмечая также* подготовленный Международным союзом электросвязи в 2009 году доклад “Securing information and communication networks: best practices for developing a culture of cybersecurity” («Обеспечение защищенности информационно-коммуникационных сетей: передовая практика в области создания культуры кибербезопасности»), основное внимание в котором уделяется всеобъемлющему национальному подходу к кибербезопасности, не нарушающему свободу слова, свободу передачи информации и надлежащих правовых процедур,

*признавая*, что национальные усилия по защите важнейших информационных инфраструктур выигрывают от периодической оценки их прогресса,

1. *предлагает* государствам-членам на добровольной основе представлять краткую информацию об их ключевых инициативах в области кибербезопасности и защиты важнейших информационных инфраструктур, с тем чтобы выделить национальные достижения и передовую практику, извлеченные уроки и направления будущей деятельности;

2. *предлагает* в этой связи вниманию государств-членов прилагаемый национальный вопросник для самооценки усилий в области кибербезопасности в качестве одного из возможных инструментов для оказания им, в соответствующих случаях, содействия в оценке национальных усилий в области кибербезопасности и защиты важнейших информационных инфраструктур;

3. *предлагает* всем государствам-членам, разработавшим стратегии действий в области кибербезопасности и защиты важнейших информационных инфраструктур, информировать Генерального секретаря к шестидесятой сессии Генеральной Ассамблеи о передовой практике и мерах, которые могли бы помочь другим государствам-членам, региональным и международным организациям, заинтересованным лицам в частном секторе и в гражданском обществе в их усилиях по созданию глобальной культуры кибербезопасности.

## Приложение

### **Инструмент самооценки национальных усилий по защите важнейших информационных инфраструктур**

#### *Анализ потребностей и стратегий в области кибербезопасности*

1. Оцените роль информационно-коммуникационных технологий в вашей национальной экономике, национальной безопасности, важнейших инфраструктурах (таких, как транспорт, водоснабжение и обеспечение продовольствием, общественное здравоохранение, энергетика, финансы, службы экстренной помощи) и гражданском обществе.

2. Определите риски в области кибербезопасности и защиты важнейших информационных инфраструктур для вашей экономики, национальной безопасности, важнейших инфраструктур и гражданского общества, которые нуждаются в регулировании.

3. Проанализируйте слабые места в используемых сетях, относительные уровни текущих угроз в каждом секторе и существующий план управления; отметьте, как на этих расчетах сказываются изменения в экономической ситуации, приоритетах в области национальной безопасности и потребностях гражданского общества.

4. Определите цели вашей национальной стратегии по обеспечению кибербезопасности и защиты важнейших информационных инфраструктур, опишите эти цели, нынешний уровень достижения, существующие меры по оценке хода их достижения, их связь с задачами национальной политики, а также как эта стратегия вписывается в региональные и международные инициативы.

#### *Роли и обязанности заинтересованных сторон*

5. Определите ключевые заинтересованные стороны, участвующие в обеспечении кибербезопасности и защиты важнейших информационных инфраструктур, и опишите роль каждой из них в разработке соответствующих стратегий и операций, включая:

- национальные государственные министерства и ведомства с указанием главных лиц для контактов и обязанностей каждого из них;
- других государственных (местных и региональных) участников;
- неправительственных участников, включая представителей промышленности, гражданского общества и научных кругов;
- отдельных граждан с указанием того, имеют ли рядовые пользователи Интернета доступ к базовой подготовке, позволяющей избегать угроз в Интернете, и проводится ли национальная кампания распространения информации по вопросу кибербезопасности.

*Стратегические процессы и участие*

6. Перечислите существующие в настоящее время формальные и неформальные механизмы взаимодействия между правительством и промышленностью в разработке стратегий и операций в области кибербезопасности и защиты важнейших информационных инфраструктур; определите участников, роль(и) и задачи, методы мобилизации и анализа вклада в эту деятельность и насколько он обеспечивает достижение соответствующих целей в области кибербезопасности и защиты важнейших информационных инфраструктур.

7. Определите форумы или структуры, которые могут в дальнейшем понадобиться для интеграции позиций правительства и неправительственных участников и их знаний, что необходимо для достижения национальных целей в области кибербезопасности и защиты важнейших информационных инфраструктур.

*Сотрудничество между государственным и частным секторами*

8. Представьте сводную информацию о всех принятых мерах и планах по развитию сотрудничества между правительством и частным сектором, включая любые механизмы распространения информации и реагирования на инциденты.

9. Представьте сводную информацию о всех осуществляемых и запланированных инициативах по отстаиванию общих интересов и решению общих проблем как среди пользователей важнейших инфраструктур, так и среди представителей частного сектора, в равной степени зависящих от использования одних и тех же взаимосвязанных важнейших инфраструктур.

*Деятельность в связи с инцидентами и восстановление после сбоев*

10. Укажите государственное ведомство, выполняющее функции координатора деятельности в связи с инцидентами, включая возможные функции наблюдения, предупреждения, реагирования и восстановления; сотрудничающие с ним государственные учреждения; сотрудничающих неправительственных участников, включая представителей промышленности и других партнеров; и любые существующие механизмы сотрудничества и обмена достоверной информацией.

11. Отдельно укажите общенациональный механизм реагирования на компьютерные сбои, включая любую группу реагирования на компьютерные сбои, выполняющую общенациональные функции, и перечислите ее функции и обязанности, в том числе опишите существующий инструментарий и процедуры защиты правительственных компьютерных сетей и существующие инструменты и процедуры распространения информации о деятельности в связи с инцидентами.

12. Укажите сети и процессы международного сотрудничества, которые могут укрепить потенциал реагирования на инциденты и планирования на случай чрезвычайных ситуаций, отдельно выделив в соответствующих случаях партнеров и механизмы двустороннего и многостороннего сотрудничества.

*Правовые рамки*

13. Проанализируйте и обновите список национальных правовых органов (в том числе занимающихся вопросами киберпреступности, охраны личной информации, защиты данных, коммерческого права, цифровых подписей и шифрования), которые могут устареть или утратить актуальность в результате быстрого развития новых информационно-коммуникационных технологий и формирования зависимости от них, используя в ходе этого рассмотрения региональные и международные конвенции, механизмы и прецеденты. Определите, является ли ваше государство участником Будапештской конвенции о киберпреступности, планирует ли присоединиться к ней или же планирует принять сопоставимые законы.

14. Определите нынешнее состояние национальных органов по борьбе с киберпреступностью и соответствующих процедур, включая правовые органы и национальные группы по борьбе с киберпреступностью, и уровень взаимопонимания между прокурорами, судьями и законодателями, занимающимися вопросами киберпреступности.

15. Оцените, насколько существующие правовые кодексы и правовые органы соответствуют задаче решения существующих и будущих проблем киберпреступности и киберпространства в целом.

16. Проанализируйте, участвует ли ваше государство в международной деятельности по борьбе с киберпреступностью, такой как функционирующая круглосуточно без выходных Сеть контактных пунктов по киберпреступности, и определите, в какой мере такое участие способствует достижению национальных целей в области кибербезопасности.

17. Установите для ваших национальных правоохранительных органов требование сотрудничать с международными коллегами в расследовании транснациональных киберпреступлений в тех случаях, когда инфраструктура или лица, обвиняемые в совершении этих преступлений, находятся на вашей национальной территории, а жертва находится за пределами вашей страны.

*Создание глобальной культуры кибербезопасности*

18. Представьте сводную информацию о принятых мерах и планах по созданию национальной культуры кибербезопасности, о которой говорится в резолюциях 57/239 и 58/199 Генеральной Ассамблеи Организации Объединенных Наций, включая реализацию плана кибербезопасности для систем, управление которыми осуществляет правительство, национальных программ повышения уровня осведомленности и распространения знаний среди, в частности, детей и индивидуальных пользователей, а также о потребностях в профессиональной подготовке в области национальной кибербезопасности и защиты важнейших информационных инфраструктур».

3. На 37-м заседании 25 ноября Комитет имел в своем распоряжении пересмотренный проект резолюции «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» (A/C.2/64/L.8/Rev.1), представленный Соединенными Штатами от имени Австралии, Антигуа и Барбуды, Аргентины, Белиза, Болгарии, Венгрии, Германии, Доминиканской Республики, Израиля, Ирландии, Испании, Италии, Канады, Латвии, Маршалловых Островов, Мексики, Нигерии, Панамы, Польши, Португалии, Республики Корея, Республики Молдова, Румынии, Сингапура, Словении, Соединенного Королевства Великобритании и Северной Ирландии, Украины, Финляндии, Франции, Хорватии, Черногории, Чили, Швеции, Эстонии и Японии.
4. На том же заседании Комитет был информирован о том, что этот пересмотренный проект резолюции не имеет последствий для бюджета по программам.
5. Также на том же заседании представитель Соединенных Штатов внес в этот проект резолюции устное исправление.
6. Также на 37-м заседании к числу авторов этого проекта резолюции присоединились Греция, Индия, Литва и Ямайка.
7. Комитет принял проект резолюции A/C.2/64/L.8/Rev.1 с внесенным в него устным исправлением (см. пункт 14, проект резолюции I).

## **В. Проекты резолюций A/C.2/64/L.17 и A/C.2/64/L.49**

8. На 33-м заседании 10 ноября представитель Судана от имени государств — членов Организации Объединенных Наций, входящих в Группу 77 и Китая, внес на рассмотрение проект резолюции, озаглавленный «Наука и техника в целях развития» (A/C.2/64/L.17), следующего содержания:

*«Генеральная Ассамблея,*

*ссылаясь на свои резолюции 58/200 от 23 декабря 2003 года, 59/220 от 22 декабря 2004 года, 60/205 от 22 декабря 2005 года и 62/201 от 19 декабря 2007 года,*

*ссылаясь также на свою резолюцию 61/207 от 20 декабря 2006 года и ее положения, касающиеся науки и техники,*

*ссылаясь далее на резолюцию 2006/46 Экономического и Социального Совета от 28 июля 2006 года,*

*признавая жизненно важную роль, которую наука и техника, включая экологически безопасные технологии, способны играть в развитии и в облегчении усилий по искоренению нищеты, обеспечению продовольственной безопасности, борьбе с болезнями, совершенствованию систем образования, охране окружающей среды, ускорению темпов экономической диверсификации и преобразований и повышению производительности труда и конкурентоспособности,*

*ссылаясь на Итоговый документ Всемирного саммита 2005 года,*

*ссылаясь также* на итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества,

*признавая*, что международная поддержка способна помочь развивающимся странам использовать технические достижения в своих интересах и может укрепить их производственный потенциал,

*особо указывая* на ту роль, которую традиционные знания способны играть в техническом развитии и в сбалансированном и рациональном использовании природных ресурсов,

*признавая* насущную необходимость преодоления «цифровой пропасти» и оказания развивающимся странам помощи в получении доступа к потенциальным преимуществам информационно-коммуникационных технологий,

*с удовлетворением отмечая* принятие Балийского стратегического плана по оказанию технической поддержки и созданию потенциала, разработанного Программой Организации Объединенных Наций по окружающей среде,

*вновь подтверждая* необходимость укрепления научно-технических программ соответствующих органов системы Организации Объединенных Наций,

*с признательностью отмечая* сотрудничество между Комиссией по науке и технике в целях развития и Конференцией Организации Объединенных Наций по торговле и развитию в деле создания сети центров передового опыта в научно-технической области для развивающихся стран и в разработке планов и проведении обзоров научно-технической и инновационной политики,

*с интересом принимая к сведению* создание межучрежденческой сети сотрудничества в области биотехнологии «ООН-биотех», о которой говорится в докладе Генерального секретаря о науке и технике в целях развития,

*принимая к сведению* доклад Генерального секретаря,

*принимая к сведению также* резолюцию 2009/8 Экономического и Социального Совета от 24 июля 2009 года о науке и технике в целях развития,

1. *подтверждает свою решимость:*

а) укреплять и усиливать существующие механизмы и поддерживать инициативы в области научных исследований и опытно-конструкторских разработок, в том числе посредством добровольного налаживания партнерских связей между государственным и частным секторами, для удовлетворения особых нужд развивающихся стран, связанных со здравоохранением, сельским хозяйством, охраной окружающей среды, рациональным использованием природных ресурсов и природопользованием, энергетикой, лесным хозяйством и последствиями изменения климата;



b) поощрять и облегчать, в зависимости от обстоятельств, доступ развивающихся стран к технологиям, включая экологически безопасные технологии и соответствующие «ноу-хау», а также их разработку и передачу развивающимся странам и их распространение среди этих стран;

c) оказывать развивающимся странам помощь в их усилиях, направленных на содействие разработке и разработку национальных стратегий в области людских ресурсов и науки и техники, которые являются главной движущей силой в деле наращивания национального потенциала в целях развития;

d) поощрять и поддерживать более активные усилия по разработке технологий для освоения энергии из возобновляемых источников, такой, как солнечная энергия, энергия биомассы, гидроэнергия, энергия ветра и геотермальная энергия;

e) осуществлять на национальном и международном уровнях стратегии для привлечения как отечественных, так и зарубежных государственных и частных инвестиций, которые способствуют расширению знаний, передаче технологий на взаимно согласованных условиях и повышению производительности труда;

f) поддерживать усилия развивающихся стран, прилагаемые на индивидуальной и коллективной основе, по освоению новых технологий в сельском хозяйстве в целях повышения продуктивности сельского хозяйства путем использования экологически безопасных средств;

2. *признает*, что наука и техника, включая информационно-коммуникационные технологии, имеют жизненно важное значение для достижения согласованных на международном уровне целей в области развития, в том числе сформулированных в Декларации тысячелетия, и для обеспечения всестороннего участия развивающихся стран в мировой экономике;

3. *просит* Комиссию по науке и технике в целях развития выступать в качестве форума для дальнейшего оказания содействия Экономическому и Социальному Совету в качестве центра по координации общесистемной последующей деятельности в связи с итогами Всемирной встречи на высшем уровне по вопросам информационного общества и для рассмотрения — в рамках ее мандата в соответствии с резолюцией 2006/46 Совета — особых нужд развивающихся стран в таких областях, как сельское хозяйство, развитие сельских районов, информационно-коммуникационные технологии и природопользование;

4. *рекомендует* Конференции Организации Объединенных Наций по торговле и развитию, действуя в сотрудничестве с соответствующими партнерами, продолжать проведение обзоров научно-технической и инновационной политики в целях оказания развивающимся странам и странам с переходной экономикой помощи в определении мер, необходимых для обеспечения увязки научно-технической и инновационной политики с их национальными стратегиями развития;

5. *рекомендует* Конференции Организации Объединенных Наций по торговле и развитию и другим соответствующим организациям оказывать развивающимся странам помощь в их усилиях по обеспечению увязки научно-технической и инновационной политики с национальными стратегиями развития;

6. *рекомендует* правительствам расширять и стимулировать инвестиции в научные исследования и опытно-конструкторские разработки в области экологически безопасных технологий и поощрять участие деловых и финансовых секторов в развитии этих технологий и предлагает международному сообществу оказывать поддержку этим усилиям;

7. *поддерживает* существующие механизмы и рекомендует продолжать содействовать осуществлению совместных региональных, субрегиональных и межрегиональных проектов научных исследований и опытно-конструкторских разработок посредством, когда это практически осуществимо, мобилизации существующих научных ресурсов и ресурсов в области научных исследований и опытно-конструкторских разработок и создания сетевых объединений современных научно-исследовательских центров и совместного использования современного научно-исследовательского оборудования;

8. *рекомендует* международному сообществу ввиду неодинаковости уровня развития разных стран продолжать содействовать обеспечению надлежащего распространения научно-технических знаний и передачи технологий развивающимся странам, доступа этих стран к технологиям и получения ими технологий на справедливых, транспарентных и взаимно согласованных условиях таким образом, чтобы это способствовало социально-экономическому благосостоянию на благо общества;

9. *призывает* продолжать сотрудничество между подразделениями системы Организации Объединенных Наций и другими международными организациями, гражданским обществом и частным сектором в деле выполнения решений Всемирной встречи на высшем уровне по вопросам информационного общества, с тем чтобы поставить потенциал информационно-коммуникационных технологий на службу развитию путем проведения стратегических аналитических исследований для изучения «цифровой пропасти» и новых вызовов информационного общества, а также путем осуществления мероприятий в области технической помощи с привлечением партнерских объединений с участием большого числа заинтересованных сторон;

10. *просит* Генерального секретаря представить Генеральной Ассамблее на ее шестьдесят шестой сессии доклад об осуществлении настоящей резолюции и рекомендации в отношении последующей деятельности, включая накопленный опыт в деле обеспечения увязки научно-технической и инновационной политики с национальными стратегиями развития».

9. На 38-м заседании 1 декабря Комитет имел в своем распоряжении проект резолюции «Наука и техника в целях развития» (A/C.2/64/L.49), представленный заместителем Председателя Комитета Мохамедом Шерифом Диалло (Гвинея) на основе неофициальных консультаций по проекту резолюции A/C.2/64/L.17.
10. На том же заседании по предложению Председателя Комитет согласился не применять соответствующее положение правила 120 правил процедуры Генеральной Ассамблеи и приступил к принятию решения по проекту резолюции A/C.2/64/L.49.
11. Также на том же заседании Комитет был информирован о том, что проект резолюции A/C.2/64/L.49 не имеет последствий для бюджета по программам.
12. Также на 38-м заседании Комитет принял проект резолюции A/C.2/64/L.49 (см. пункт 14, проект резолюции II).
13. В связи с принятием проекта резолюции A/C.2/64/L.49 проект резолюции A/C.2/64/L.17 был снят с рассмотрения его авторами.

### III. Рекомендации Второго комитета

14. Второй комитет рекомендует Генеральной Ассамблее принять следующие проекты резолюций:

#### **Проект резолюции I Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур**

*Генеральная Ассамблея,*

*ссылаясь* на свои резолюции 55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года о борьбе с преступным использованием информационных технологий, 57/239 от 20 декабря 2002 года о создании глобальной культуры кибербезопасности и 58/199 от 23 декабря 2003 года о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур,

*ссылаясь также* на свои резолюции 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года и 63/37 от 2 декабря 2008 года о достижениях в области информационных технологий в контексте международной безопасности,

*ссылаясь далее* на итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества, состоявшейся в 2003 году (первый этап) и в 2005 году (второй этап)<sup>1</sup>,

*признавая*, что доверие и безопасность в использовании информационно-коммуникационных технологий относятся к главным опорам информационного общества и что необходимо поощрять, формировать, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности,

*признавая также* растущий вклад сетевых информационных технологий в выполнение многих важнейших функций в повседневной жизни, торговлю и обеспечение товарами и услугами, научные исследования, инновационную деятельность, предпринимательство и свободную передачу информации между физическими лицами и организациями, правительствами, деловыми кругами и гражданским обществом;

*признавая далее*, что правительства, деловые круги, другие организации и индивидуальные владельцы и пользователи информационных технологий должны нести ответственность, сообразную их функциям, за обеспечение безопасности этих информационных технологий и принимать надлежащие меры для ее укрепления,

<sup>1</sup> См. A/C.2/59/3 и A/60/687.

*признавая* важность мандата Форума по вопросам управления Интернетом как площадки для диалога между многими заинтересованными сторонами для обсуждения различных вопросов, включая, в частности, вопросы государственной политики в связи с ключевыми элементами управления Интернетом, для содействия обеспечению устойчивого характера, надежности, безопасности, стабильности и развития Интернета и вновь заявляя о том, что все правительства должны иметь равные задачи и обязанности в сфере управления Интернетом на международной основе и обеспечения стабильности, безопасности и непрерывности Интернета,

*вновь подтверждая* сохраняющуюся необходимость упрочения сотрудничества — с тем чтобы правительства могли на равной основе играть свою роль и выполнять свои обязательства — в решении вопросов международной государственной политики, касающихся Интернета, а не в сфере повседневной деятельности технического и эксплуатационного характера, которая не влияет на вопросы международной государственной политики,

*признавая*, что каждая страна будет сама определять свои собственные важнейшие информационные инфраструктуры,

*вновь подтверждая* необходимость использования потенциала информационно-коммуникационных технологий для содействия достижению согласованных на международном уровне целей в области развития, в том числе сформулированных в Декларации тысячелетия, признавая, что отсутствие равного доступа к информационным технологиям и возможностей их использования государствами может подорвать их экономическое процветание, и вновь подтверждая также эффективность сотрудничества в борьбе с преступным использованием информационных технологий и в создании глобальной культуры кибербезопасности,

*подчеркивая* необходимость активизации усилий по преодолению «цифровой пропасти» для обеспечения универсального доступа к информационно-коммуникационным технологиям и для защиты важнейших информационных инфраструктур путем облегчения передачи информационных технологий развивающимся странам, особенно наименее развитым странам, и наращивания их потенциала в вопросах передовой практики и профессиональной подготовки в области кибербезопасности,

*выражая озабоченность* по поводу того, что угрозы надежному функционированию важнейших информационных инфраструктур и целостности информации, передаваемой по этим сетям, приобретают все более изощренный и серьезный характер, отрицательно сказываясь на уровне семейного, национального и международного благополучия,

*подтверждая*, что обеспечение защищенности важнейших информационных инфраструктур — это обязанность, которую правительства должны систематически выполнять, выступая с соответствующими инициативами на национальном уровне, в координации с заинтересованными сторонами, которые, в свою очередь, должны знать о соответствующих рисках, превентивных мерах и эффективных мерах реагирования, соответствующих возложенным на них функциям,

*признавая*, что национальные усилия должны подкрепляться обменом информацией и взаимодействием на международном уровне, с тем чтобы можно было эффективно противостоять таким угрозам, приобретающим все более транснациональный характер,

*отмечая* работу соответствующих региональных и международных организаций по укреплению кибербезопасности и вновь указывая на их роль в поддержании национальных усилий и поощрении международного сотрудничества,

*отмечая также* подготовленный Международным союзом электросвязи в 2009 году доклад “Securing information and communication networks: best practices for developing a culture of cybersecurity” («Обеспечение защищенности информационно-коммуникационных сетей: передовая практика в области формирования культуры кибербезопасности»), основное внимание в котором уделяется всеобъемлющему национальному подходу к кибербезопасности, не нарушающему свободы слова, свободы передачи информации и надлежащих правовых процедур,

*признавая*, что периодическая оценка прогресса в рамках национальных усилий по защите важнейших информационных инфраструктур благоприятно отражается на таких усилиях,

1. *предлагает* государствам-членам использовать, если и когда они сочтут это целесообразным, прилагаемый инструмент добровольной самооценки национальных усилий по защите важнейших информационных инфраструктур, призванный помочь им в анализе их усилий по защите важнейших информационных инфраструктур и укреплению кибербезопасности, с тем чтобы выявить области, в которых требуется принятие дополнительных мер, в целях повышения глобальной культуры кибербезопасности;

2. *рекомендует* государствам-членам и соответствующим региональным и международным организациям, разработавшим стратегии действий в области кибербезопасности и защиты важнейших информационных инфраструктур, поделиться сведениями о передовой практике и мерах, которые могли бы помочь другим государствам-членам в их усилиях по содействию обеспечению кибербезопасности, путем представления такой информации Генеральному секретарю для ее обобщения и распространения среди государств-членов.

## Приложение

### **Инструмент добровольной самооценки национальных усилий по защите важнейших информационных инфраструктур<sup>2</sup>**

#### **Анализ потребностей и стратегий в области кибербезопасности**

1. Проанализируйте роль информационно-коммуникационных технологий в Вашей национальной экономике, национальной безопасности, важнейших инфраструктурах (таких, как транспорт, водоснабжение и обеспечение продовольствием, общественное здравоохранение, энергетика, финансы, службы экстренной помощи) и гражданском обществе.

2. Определите риски в области кибербезопасности и защиты важнейших информационных инфраструктур для экономики, национальной безопасности, важнейших инфраструктур и гражданского общества Вашей страны, которые нуждаются в управлении.

3. Выявите слабые места в используемых сетях, относительные уровни текущих угроз в каждом секторе и существующий план управления; обратите внимание, как на этих расчетах сказываются изменения в экономической ситуации, приоритетах в области национальной безопасности и потребностях гражданского общества.

4. Определите цели национальной стратегии по обеспечению кибербезопасности и защиты важнейших информационных инфраструктур; опишите эти цели, нынешний уровень достижения, существующие меры по оценке достигнутого прогресса, связь стратегии с задачами национальной политики, а также, как эта стратегия вписывается в региональные и международные инициативы.

#### **Роли и обязанности заинтересованных сторон**

5. Определите ключевые заинтересованные стороны, участвующие в обеспечении кибербезопасности и защиты важнейших информационных инфраструктур, и опишите роль каждой из них в разработке соответствующих стратегий и операций, включая:

- национальные государственные министерства и ведомства с указанием главных лиц для контактов и обязанностей каждого из них;
- других государственных (местных и региональных) участников;
- неправительственных участников, включая представителей отрасли, гражданского общества и научных кругов;
- отдельных граждан с указанием того, имеют ли рядовые пользователи Интернета доступ к базовой подготовке, позволяющей избегать угроз в Интернете, и проводится ли национальная кампания распространения информации по вопросу кибербезопасности.

---

<sup>2</sup> Это добровольный инструмент, который может использоваться государствами-членами (полностью или частично, если и когда они сочтут это целесообразным) и который призван помочь им в анализе их усилий по защите важнейших информационных инфраструктур и укреплению кибербезопасности.

### **Стратегические процессы и участие**

6. Перечислите существующие в настоящее время формальные и неформальные механизмы взаимодействия между правительством и отраслью в разработке стратегий и операций в области кибербезопасности и защиты важнейших информационных инфраструктур; определите участников, роль(и) и задачи, методы мобилизации и анализа вклада в эту деятельность и то, насколько он обеспечивает достижение соответствующих целей в области кибербезопасности и защиты важнейших информационных инфраструктур.

7. Определите форумы или структуры, которые могут в дальнейшем понадобиться для интеграции позиций правительства и неправительственных участников и их знаний, что необходимо для достижения национальных целей в области кибербезопасности и защиты важнейших информационных инфраструктур.

### **Сотрудничество между государственным и частным секторами**

8. Представьте сводную информацию о всех принятых мерах и планах по развитию сотрудничества между правительством и частным сектором, включая любые механизмы распространения информации и реагирования на инциденты.

9. Представьте сводную информацию о всех осуществляемых и запланированных инициативах по отстаиванию общих интересов и решению общих проблем как среди участников важнейших инфраструктур, так и среди представителей частного сектора, в равной степени зависящих от пользования одними и теми же взаимосвязанными важнейшими инфраструктурами.

### **Деятельность в связи с инцидентами и восстановление после сбоев**

10. Укажите государственное ведомство, выполняющее функции координатора деятельности в связи с инцидентами, включая возможные функции наблюдения, предупреждения, реагирования и восстановления; сотрудничающие с ним государственные ведомства; сотрудничающих неправительственных участников, включая представителей отрасли и других партнеров; и любые существующие механизмы сотрудничества и обмена достоверной информацией.

11. Отдельно укажите общенациональный механизм реагирования на компьютерные сбои, включая любую группу реагирования на компьютерные сбои, выполняющую общенациональные функции, и перечислите ее функции и обязанности, в том числе опишите существующий инструментарий и процедуры защиты правительственных компьютерных сетей и существующие инструменты и процедуры распространения информации о деятельности в связи с инцидентами.

12. Укажите сети и процессы международного сотрудничества, которые могут укрепить потенциал реагирования на инциденты и планирования на случай чрезвычайных ситуаций, отдельно выделив в соответствующих случаях партнеров и механизмы двустороннего и многостороннего сотрудничества.



### **Правовые рамки**

13. Проанализируйте и обновите список национальных правовых органов (в том числе занимающихся вопросами киберпреступности, охраны личной информации, защиты данных, коммерческого права, цифровых подписей и шифрования), которые могут устареть или утратить актуальность в результате быстрого развития новых информационно-коммуникационных технологий и формирования зависимости от них, используя в ходе этого рассмотрения региональные и международные конвенции, механизмы и прецеденты. Установите, разработала ли Ваша страна необходимое законодательство для расследования киберпреступлений и преследования лиц, виновных в их совершении, обратив внимание на существующие механизмы, например на резолюции 55/63 и 56/121 Генеральной Ассамблеи о борьбе с преступным использованием информационных технологий и на региональные инициативы, включая Конвенцию Совета Европы о киберпреступности.

14. Определите нынешнее состояние национальных органов по борьбе с киберпреступностью и соответствующих процедур, включая правовые органы, национальные группы по борьбе с киберпреступностью, и уровень взаимопонимания между прокурорами, судьями и законодателями, занимающимися вопросами киберпреступности.

15. Оцените, насколько существующие правовые кодексы и правовые органы соответствуют задаче решения существующих и будущих проблем киберпреступности и киберпространства в целом.

16. Изучите уровень национального участия в международной деятельности по борьбе с киберпреступностью, такой как круглосуточно функционирующая Сеть контактных пунктов по киберпреступности.

17. Определите потребности национальных правоохранительных органов в сотрудничестве с международными коллегами при расследовании транснациональных киберпреступлений в тех случаях, когда инфраструктура или лица, обвиняемые в совершении этих преступлений, находятся на Вашей национальной территории, а жертва находится за пределами Вашей страны.

### **Формирование глобальной культуры кибербезопасности**

18. Представьте сводную информацию о принятых мерах и планах по формированию национальной культуры кибербезопасности, о которой говорится в резолюциях 57/239 и 58/199 Генеральной Ассамблеи, включая реализацию плана кибербезопасности для систем, управление которыми осуществляет правительство, национальных программ повышения уровня осведомленности и распространения знаний среди, в частности, детей и индивидуальных пользователей, а также о потребностях в профессиональной подготовке в области национальной кибербезопасности и защиты важнейших информационных инфраструктур.

## Проект резолюции II Наука и техника в целях развития

*Генеральная Ассамблея,*

*ссылаясь* на свои резолюции 58/200 от 23 декабря 2003 года, 59/220 от 22 декабря 2004 года, 60/205 от 22 декабря 2005 года и 62/201 от 19 декабря 2007 года,

*ссылаясь также* на свою резолюцию 61/207 от 20 декабря 2006 года и ее положения, касающиеся науки и техники,

*принимая к сведению* резолюции Экономического и Социального Совета 2006/46 от 28 июля 2006 года и 2009/8 от 24 июля 2009 года,

*признавая* жизненно важную роль, которую наука и техника, включая экологически безопасные технологии, способны играть в развитии и в облегчении усилий по искоренению нищеты, обеспечению продовольственной безопасности, борьбе с болезнями, совершенствованию систем образования, охране окружающей среды, ускорению темпов экономической диверсификации и преобразований и повышению производительности труда и конкурентоспособности,

*ссылаясь* на Итоговый документ Всемирного саммита 2005 года<sup>1</sup>,

*ссылаясь также* на итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества<sup>2</sup>,

*признавая*, что международная поддержка способна помочь развивающимся странам использовать технические достижения в своих интересах и может укрепить их производственный потенциал,

*особо указывая* на ту роль, которую традиционные знания способны играть в техническом развитии и в сбалансированном и рациональном использовании природных ресурсов,

*принимая во внимание* насущную необходимость преодоления «цифровой пропасти» и оказания развивающимся странам помощи в получении доступа к потенциальным преимуществам информационно-коммуникационных технологий,

*рекомендуя* продолжать усилия по осуществлению Балийского стратегического плана по оказанию технической поддержки и созданию потенциала, разработанного Программой Организации Объединенных Наций по окружающей среде<sup>3</sup>,

*вновь подтверждая* необходимость укрепления научно-технических программ соответствующих органов системы Организации Объединенных Наций,

---

<sup>1</sup> См. резолюцию 60/1.

<sup>2</sup> См. A/60/687 и A/C.2/59/3, приложение, глава I.

<sup>3</sup> UNEP/GC.23/6/Add.1 и Corr. 1, приложение.

*с удовлетворением отмечая* сотрудничество между Комиссией по науке и технике в целях развития и Конференцией Организации Объединенных Наций по торговле и развитию в деле создания сети центров передового опыта в научно-технической области для развивающихся стран и в разработке планов и проведении обзоров научно-технической и инновационной политики,

*с интересом принимая к сведению* создание межучрежденческой сети сотрудничества в области биотехнологии «ООН-биотех», о которой говорится в докладе Генерального секретаря о науке и технике в целях развития<sup>4</sup>,

*принимая к сведению* доклад Генерального секретаря,

*рекомендуя* разрабатывать инициативы по стимулированию вовлечения частного сектора в процессы передачи технологий и научно-технического сотрудничества,

1. *вновь подтверждает* свою решимость:

a) укреплять и совершенствовать существующие механизмы и поддерживать инициативы в области научных исследований и опытно-конструкторских разработок, в том числе посредством добровольного налаживания партнерских связей между государственным и частным секторами, для удовлетворения особых нужд развивающихся стран, связанных со здравоохранением, сельским хозяйством, охраной окружающей среды, рациональным использованием природных ресурсов и природопользованием, энергетикой, лесным хозяйством и последствиями изменения климата;

b) стимулировать и облегчать, в зависимости от обстоятельств, доступ развивающихся стран к технологиям, включая экологически безопасные технологии и соответствующие «ноу-хау», а также их разработку и передачу развивающимся странам и их распространение среди этих стран;

c) оказывать развивающимся странам помощь в их усилиях, направленных на содействие разработке и разрабатку национальных стратегий в области людских ресурсов и науки и техники, которые являются главной движущей силой в деле наращивания национального потенциала в целях развития;

d) стимулировать и поддерживать более активные усилия по освоению возобновляемых источников энергии, включая разработку соответствующих технологий;

e) осуществлять на национальном и международном уровнях стратегии для привлечения как отечественных, так и зарубежных государственных и частных инвестиций, которые способствуют расширению знаний, передаче технологий на взаимно согласованных условиях и повышению производительности труда;

f) поддерживать усилия развивающихся стран, прилагаемые на индивидуальной и коллективной основе, по освоению новых технологий в сельском хозяйстве в целях повышения продуктивности сельского хозяйства путем использования экологически безопасных средств;

---

<sup>4</sup> A/64/168.

2. *признает*, что наука и техника, включая информационно-коммуникационные технологии, имеют жизненно важное значение для достижения согласованных на международном уровне целей в области развития, в том числе сформулированных в Декларации тысячелетия, и для обеспечения всестороннего участия развивающихся стран в мировой экономике;

3. *просит* Комиссию по науке и технике в целях развития выступать в качестве форума для дальнейшего оказания содействия Экономическому и Социальному Совету в качестве центра по координации общесистемной последующей деятельности в связи с итогами Всемирной встречи на высшем уровне по вопросам информационного общества<sup>2</sup> и для рассмотрения — в рамках ее мандата в соответствии с резолюцией 2006/46 Совета — особых нужд развивающихся стран в таких областях, как сельское хозяйство, развитие сельских районов, информационно-коммуникационные технологии и природопользование;

4. *рекомендует* Конференции Организации Объединенных Наций по торговле и развитию, действуя в сотрудничестве с соответствующими партнерами, продолжать проведение обзоров научно-технической и инновационной политики в целях оказания развивающимся странам и странам с переходной экономикой помощи в определении мер, необходимых для обеспечения увязки научно-технической и инновационной политики с их национальными стратегиями развития;

5. *рекомендует* Конференции Организации Объединенных Наций по торговле и развитию и другим соответствующим организациям оказывать развивающимся странам помощь в их усилиях по обеспечению увязки научно-технической и инновационной политики с национальными стратегиями развития;

6. *рекомендует* правительствам расширять и стимулировать инвестиции в научные исследования и опытно-конструкторские разработки в области экологически безопасных технологий и поощрять участие деловых и финансовых секторов в развитии этих технологий и предлагает международному сообществу оказывать поддержку этим усилиям;

7. *поддерживает* существующие механизмы и рекомендует продолжать содействовать осуществлению совместных региональных, субрегиональных и межрегиональных проектов научных исследований и опытно-конструкторских разработок посредством, когда это практически осуществимо, мобилизации существующих научных ресурсов и ресурсов в области научных исследований и опытно-конструкторских разработок и создания сетевых объединений современных научно-исследовательских центров и совместного использования современного научно-исследовательского оборудования;

8. *рекомендует* международному сообществу ввиду неодинаковости уровня развития разных стран продолжать содействовать обеспечению надлежащего распространения научно-технических знаний и передачи технологий развивающимся странам, доступа этих стран к технологиям и получения ими технологий на справедливых, транспарентных и взаимно согласованных условиях таким образом, чтобы это способствовало социально-экономическому благосостоянию на благо общества;

9. *призывает* продолжать сотрудничество между структурами системы Организации Объединенных Наций и другими международными организациями, гражданским обществом и частным сектором в деле выполнения решений Всемирной встречи на высшем уровне по вопросам информационного общества, с тем чтобы поставить потенциал информационно-коммуникационных технологий на службу развитию путем проведения стратегических аналитических исследований для изучения «цифровой пропасти» и новых вызовов информационного общества, а также осуществления мероприятий в области технической помощи с привлечением партнерских объединений с участием многих заинтересованных сторон;

10. *просит* Генерального секретаря представить Генеральной Ассамблее на ее шестьдесят шестой сессии доклад об осуществлении настоящей резолюции и рекомендации в отношении последующей деятельности, включая информацию о накопленном опыте в деле обеспечения увязки научно-технической и инновационной политики с национальными стратегиями развития.

---