



## Генеральная Ассамблея

Distr.: Limited  
10 December 2003  
Russian  
Original: English

Пятьдесят восьмая сессия

**Второй комитет**

Пункт 91(b) повестки дня

**Вопросы макроэкономической политики:  
наука и техника в целях развития**

**Проект резолюции, представленный заместителем Председателя Комитета г-ном Генри С. Раубенхаймером (Южная Африка) на основе результатов неофициальных консультаций, проведенных по проекту резолюции A/C.2/58/L.19**

**Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур**

*Генеральная Ассамблея,*

*ссылаясь* на свои резолюции 57/239 от 20 декабря 2002 года о создании глобальной культуры кибербезопасности, 55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года о создании правовой основы для борьбы с преступным использованием информационных технологий и 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 и 57/53 от 22 ноября 2002 года о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности,

*признавая* растущее значение информационных технологий с точки зрения содействия социально-экономическому развитию и предоставления насущно необходимых товаров и услуг, ведения дел и обмена информацией для правительств, предприятий, организаций и индивидуальных пользователей,

*отмечая* усиление связей между важнейшими инфраструктурами большинства стран, такими, как инфраструктуры, используемые, в частности, для производства, передачи и распределения энергии и в секторах воздушного и морского транспорта, банковских и финансовых услуг, электронной торговли, водоснабжения, распределения продовольствия и общественного здравоохранения, и важнейшими информационными инфраструктурами, которые во все большей степени обеспечивают взаимосвязанность их функционирования и влияют на него,

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

*признавая также*, что такая растущая технологическая взаимозависимость базируется на сложной сети компонентов важнейших информационных инфраструктур,

*отмечая*, что в результате усиливающейся взаимосвязанности важнейшие информационные инфраструктуры подвергаются сейчас все более многочисленным и разнообразным угрозам и факторам уязвимости, которые создают новые проблемы в плане безопасности,

*отмечая также*, что действенная защита важнейших инфраструктур включает, в частности, выявление угроз и уменьшение уязвимости важнейших информационных инфраструктур, уменьшение ущерба и времени на восстановление в случае повреждения или попыток нарушения защиты, а также выявление причин повреждения или источника таких попыток,

*признавая*, что действенная защита требует коммуникации и сотрудничества на национальном и международном уровнях между всеми заинтересованными сторонами и что национальные усилия должны поддерживаться эффективным, реальным международным и региональным сотрудничеством между заинтересованными сторонами,

*признавая также*, что несоответствия в уровнях доступа различных государств к информационным технологиям и их использования могут снизить эффективность сотрудничества в борьбе с преступным использованием информационных технологий и в деле создания глобальной культуры кибербезопасности, и отмечая необходимость содействия передаче информационных технологий, в частности развивающимся странам,

*признавая далее* важное значение международного сотрудничества для обеспечения кибербезопасности и защиты важнейших информационных инфраструктур посредством поддержки национальных усилий, направленных на укрепление человеческого потенциала, расширение возможностей в плане обучения и занятости, улучшение государственных услуг и повышение качества жизни за счет использования передовых, надежных и защищенных информационно-коммуникационных технологий и сетей и содействия обеспечению всеобщего доступа,

*отмечая* работу соответствующих международных и региональных организаций над повышением безопасности важнейших информационных инфраструктур,

*признавая*, что усилия по защите важнейших информационных инфраструктур должны прилагаться с должным учетом применимых национальных законов о неприкосновенности частной жизни и другого соответствующего законодательства,

1. *принимает к сведению* изложенные в приложении к настоящей резолюции элементы для защиты важнейших информационных инфраструктур;

2. *предлагает* всем соответствующим международным организациям, включая соответствующие органы Организации Объединенных Наций, в надлежащем порядке учитывать, среди прочего, эти элементы для защиты важнейших информационных инфраструктур в любой будущей работе по вопросам кибербезопасности или защиты важнейших инфраструктур;

3. *предлагает* государствам-членам учитывать, среди прочего, эти элементы при разработке своих стратегий уменьшения рисков для важнейших информационных инфраструктур в соответствии с национальными законами и нормами;

4. *предлагает* государствам-членам и всем соответствующим международным организациям принимать во внимание, среди прочего, эти элементы и необходимость защиты важнейших информационных инфраструктур при подготовке ко второму этапу Всемирной встречи на высшем уровне по вопросам информационного общества, который состоится в 2005 году в Тунисе;

5. *рекомендует* государствам-членам и соответствующим региональным и международным организациям, которые разработали стратегии обеспечения кибербезопасности и защиты важнейших информационных инфраструктур, поделиться информацией о своем передовом опыте и мерах, которая могла бы оказать другим государствам-членам содействие в их усилиях в направлении содействия обеспечению кибербезопасности;

6. *подчеркивает* необходимость активизации усилий по преодолению «цифровой пропасти», обеспечению всеобщего доступа к информационно-коммуникационным технологиям и защите важнейших информационных инфраструктур путем содействия передаче информационной технологии и наращиванию потенциала, в частности в интересах развивающихся стран, особенно наименее развитых из них, с тем чтобы все государства могли в полной мере использовать информационно-коммуникационные технологии для целей своего социально-экономического развития.

## **Приложение**

### **Элементы для защиты важнейших информационных инфраструктур**

1. Наличие сетей для срочного предупреждения о факторах уязвимости, угрозах и инцидентах в кибернетическом пространстве.

2. Повышение степени информированности заинтересованных сторон, с тем чтобы они более глубоко понимали характер и масштабы своих важнейших информационных инфраструктур и ту роль, которую каждая из них должна играть в защите этих инфраструктур.

3. Анализ инфраструктур и выявление факторов их взаимозависимости для усиления защиты таких инфраструктур.

4. Содействие развитию партнерских отношений между заинтересованными сторонами, представляющими как государственный, так и частный секторы, для обмена информацией о важнейших инфраструктурах и анализа такой информации в целях предотвращения нанесения ущерба таким инфраструктурам или попыток нарушения их защиты, расследования таких случаев и принятия мер в связи с ними.

5. Создание и обеспечение функционирования систем коммуникации в кризисной ситуации и проверка их функционирования для обеспечения их надежной и стабильной работы в чрезвычайных ситуациях.

6. Обеспечение того, чтобы процедуры предоставления доступа к данным учитывали необходимость защиты важнейших информационных инфраструктур.

7. Содействие отслеживанию попыток нарушения защиты важнейших информационных инфраструктур и, в надлежащих случаях, предоставление информации о результатах такого отслеживания другим государствам.

8. Организация профессиональной подготовки и проведение тренировок для укрепления потенциала реагирования и апробирования планов обеспечения непрерывной работы и резервных планов на случай попыток нарушения защиты информационных инфраструктур, а также побуждение заинтересованных сторон к участию в аналогичных мероприятиях.

9. Наличие адекватных материальных и процессуальных законов и квалифицированного персонала для обеспечения государствам возможности расследовать попытки нарушения защиты важнейших информационных инфраструктур и привлекать к ответственности причастных к этим попыткам лиц, а также в надлежащем порядке координировать такие расследования с другими государствами.

10. Участие, когда это уместно, в международном сотрудничестве для обеспечения защищенности важнейших информационных инфраструктур, в том числе путем создания и координации работы систем срочного предупреждения, обмена информацией о факторах уязвимости, угрозах и инцидентах и анализа такой информации, а также путем координации расследований попыток нарушения защиты таких инфраструктур в соответствии с национальным законодательством.

11. Содействие национальным и международным научным исследованиям и опытно-конструкторским разработкам и поощрение применения технологий обеспечения защиты, отвечающих международным стандартам.

---