Организация Объединенных Наций A/59/116/Add.1*

# Генеральная Ассамблея

Distr.: General
28 December 2004
Russian
Original: English/Spanish

**Пятьдесят девятая сессия**
Пункт 60 повестки дня
**Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности**

## Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

### Доклад Генерального секретаря**

**Добавление**

## Содержание



* Переиздано по техническим причинам.

** Приведенная в настоящем докладе информация была получена после представления основного доклада.

04-47513* (R) 070105 110105

*0447513*

# Ответы, полученные от государств-членов

## Мексика

[Подлинный текст на испанском языке]
[18 августа 2004 года]

1. В нынешнюю эпоху, характеризуемую стремительным развитием информационных и телекоммуникационных систем, международное сообщество осознало, что параллельно с таким развитием возросла взаимосвязь между пользователями настолько крупномасштабных и разнообразных систем, что этот процесс вышел за рамки существующих государственных границ или существующих национальных правовых норм.

2. Однако по мере возрастания такой взаимосвязи соответственно возрастала и уязвимость в плане национальной и международной безопасности, и это стало еще одним подтверждением того, что информация и системы телекоммуникаций являются областями, оказывающими важное влияние на вопросы мира и международной безопасности.

3. В этой связи Мексика считает, что меры, которые будут приниматься для ограничения угроз в этой области, должны не только учитывать необходимость сохранения свободного обращения информации и способствовать развитию этих элементов в мирных целях, но и должны приносить существенные выгоды в плане разоружения и нераспространения и сближения между народами, а также в плане развития международного сотрудничества в этой области.

4. Мы полагаем, что сфера информации и телекоммуникаций должна рассматриваться во всей ее динамике и с учетом перспективы, так как в результате стремительных темпов научно-технического прогресса возник разрыв между нормами, регулирующими такие системы, и их реальными возможностями, вследствие чего возрастают потенциальные и существующие угрозы в области информационной безопасности.

5. С учетом актуальности этой темы и необходимости рассмотрения понятий, которые позволили бы нам более точно характеризовать это явление с целью принятия необходимых мер, Мексика приветствует инициированные в феврале текущего года усилия по созданию группы правительственных экспертов, которая будет сотрудничать с Генеральным секретарем Организации Объединенных Наций в процессе подготовки исследования о «существующих и потенциальных угрозах в сфере информационной безопасности, о возможных мерах в области сотрудничества для противодействия этим угрозам», а также о «соответствующих международных концепциях, которые были направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем», о чем говорится в пунктах 2 и 4 постановляющей части резолюции 58/32. В этой связи Мексика надеется, что доклад, который должен быть представлен Генеральной Ассамблее на ее шестидесятой сессии, будет содержать рекомендации по существу данного вопроса и что будет обеспечен прогресс в концептуальном и юридическом осмыслении этой темы.

6. Ввиду этого Мексика считает, что весьма полезным в этой связи было бы обсуждение этой темы в рамках других комиссий Генеральной Ассамблеи, изучение соответствующих положений действующих международных документов,

а также рассмотрение наработок других международных организаций, в частности ЮНЕСКО, в таких областях, как международная безопасность, международный терроризм и информация и информационное общество.

7. Что касается пункта 3 постановляющей части указанной резолюции, в котором говорится об «определении основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или противоправное использование информационных и телекоммуникационных систем и информационных ресурсов», то Мексика по-прежнему считает, что понятие несанкционированного вмешательства может вызвать ненужное замешательство, так как оно может ассоциироваться с действиями, предпринимаемыми рядом государств, которые, ссылаясь на сомнительные гуманитарные и иные причины, индивидуально или совместно вмешиваются в дела других государств.

8. В этой связи представляется целесообразным отказаться от этого понятия, заменив его понятиями «несанкционированного доступа» или «противоправного доступа» применительно к действиям, предпринимаемым некоторыми лицами или субъектами в информационных системах.

9. С учетом явной обеспокоенности проблемами безопасности, связанными с возможной уязвимостью информационных систем, которые используются для управления оборонными программами некоторых стран, а также опасности использования информатики и телекоммуникаций в террористических или же подрывных целях, Мексика вновь заявляет, что избежать негативного влияния мер, принимаемых в связи с проблемами информационной безопасности, на свободу информации и коммуникации можно лишь с помощью диалога, переговоров, международного сотрудничества и международного права.

## Соединенные Штаты Америки

[Подлинный текст на английском языке]
[13 июля 2004 года]

1. Эффективная безопасность информационных сетей и инфраструктур является важным условием обеспечения надежности, доступности и целостности национальных и глобальных информационных сетей, в которых все больше нуждаются государства и их граждане с точки зрения предоставления основных услуг и поддержания экономической безопасности. Необходимо решить вопрос о том, какие действия могли бы предпринять страны самостоятельно или совместно в целях укрепления безопасности информационных сетей и инфраструктуры и недопущения наносящих серьезный ущерб нападений.

2. Некоторые государства считают, что этой цели можно достичь путем принятия международной конвенции, налагающей ограничения на разработку или использование различных информационных технологий. Такие предложения подразумевают наделение правительств правом санкционировать передачу информации на территорию страны из-за границы или запрещать ее в тех случаях, когда будет установлено, что такая информация наносит ущерб политической системе, обществу или культуре.

3. Соединенные Штаты Америки считают, что данный подход не отвечает задачам укрепления безопасности глобальных информационных и телекомму

никационных систем, при этом он противоречит принципу свободного обмена информацией, что крайне необходимо для экономического роста и развития всех государств. Обеспечение информационной безопасности не должно ущемлять свободу каждого человека искать, получать и распространять информацию и идеи любыми способами, в том числе с использованием электронных средств, и независимо от государственных границ, как это предусмотрено в статье 19 Всеобщей декларации прав человека.

4. Напротив, Соединенные Штаты Америки считают, что главной угрозой для кибербезопасности являются непрекращающиеся преступные нападения организованных преступных группировок, компьютерных пиратов и негосударственных субъектов, включая террористов. В данном случае получаемые от использования киберпространства выгоды наилучшим образом можно защитить путем одновременно принятия государствами эффективных норм, предусматривающих уголовную ответственность за противоправное использование информационных технологий, и систематического осуществления на национальном уровне мер, препятствующих нанесению ущерба важнейшим информационным инфраструктурам независимо от источника угрозы, что в понимании Соединенных Штатов Америки предусматривает формирование глобальной культуры кибербезопасности. При таком подходе все участники (правительства, деловые круги, гражданское общество) осознают свои обязанности и надлежащим образом действуют в интересах обеспечения кибербезопасности.

5. Что касается использования информационных технологий в военных целях, то совершенно нет необходимости принимать какую-либо международную конвенцию. Применение таких технологий уже регулируется правилами ведения войны и его принципами необходимости, соразмерности и сведения к минимуму побочного ущерба.

**Обеспечение кибербезопасности путем принятия превентивных мер**

6. Наиболее эффективным образом кибербезопасность можно обеспечить в том случае, если государства будут действовать на национальном уровне и сотрудничать на международном уровне в интересах повышения уровня безопасности своих собственных важнейших информационных инфраструктур. Каждому государству надлежит принять национальную программу, предусматривающую следующие меры:

a) организация просветительской деятельности и пропаганда наилучших методов обеспечения безопасности информационных сетей и инфраструктур;

b) принятие эффективного законодательства, предусматривающего уголовную ответственность за противоправное использование информационных технологий;

c) установление партнерских отношений между органами государственного управления и представителями промышленных кругов в интересах создания стимулов для обеспечения безопасности своих национальных систем;

d) создание национального потенциала для предупреждения об инцидентах и принятия ответных мер и определение процедур обмена информацией на национальном и международном уровнях.

7. Каждому государству следует уделять пристальное внимание распространению культуры кибербезопасности среди всех заинтересованных участников, включая органы государственного управления, деловые круги и граждан, а также налаживанию международного сотрудничества государств в интересах создания глобальной культуры кибербезопасности.

8. В докладе Группы правительственных экспертов необходимо подчеркнуть важность подходов, изложенных в резолюциях Генеральной Ассамблеи 55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года, которые озаглавлены «Борьба с преступным использованием информационных технологий», и в резолюции 57/239 от 20 декабря 2002 года, озаглавленной «Создание глобальной культуры кибербезопасности». Указанный доклад можно было бы подготовить с учетом этих подходов путем включения формулировок в поддержку принципов обеспечения кибербезопасности, которые уже приняты государствами-членами. Такие усилия могли бы опираться на информацию о принятых в последнее время на многостороннем уровне мерах по укреплению региональной кибербезопасности, например в рамках Форума Азиатско-тихоокеанского экономического сотрудничества (АТЭС) по вопросам электросвязи, Организации американских государств, Всемирной встречи на высшем уровне по вопросам информационного общества и «большой восьмерки».

9. В подавляющем большинстве случаев источником требующих дорогостоящих ответных мер угроз целостности и работоспособности национальных и глобальных информационных инфраструктур является противоправное использование информационных технологий. По мнению Соединенных Штатов Америки, именно правительства должны принять меры для эффективного расследования такой деятельности и наказания виновных в ней лиц. В связи с этим Соединенные Штаты Америки и еще 34 государства подписали Конвенцию Совета Европы о кибернетической преступности от 23 ноября 2001 года, содержащую руководящие принципы создания соответствующего национального законодательства и трансграничного сотрудничества в правоохранительной области. Совет Европы намеревается открыть эту конвенцию для подписания не входящими в него странами в соответствии со своей практикой и статьей 37 Конвенции. Фактически, все страны, независимо от того, являются ли они участником этой конвенции или нет, могут незамедлительно воспользоваться ею в качестве модели для разработки эффективного внутреннего законодательства по борьбе с кибернетической преступностью.

10. Кроме того, независимо от того, откуда совершено нападение, и от его мотивов используемые средства и виды ущерба, нанесенного информационным системам, являются весьма схожими. Таким образом, необходимо, чтобы все страны на систематической основе предпринимали шаги для уменьшения степени уязвимости своих систем и прививали своим гражданам культуру кибербезопасности, которая представляет собой набор мер безопасности и соответствующих навыков, обеспечивающих сохранность их информационных инфраструктур.

11. Эффективная защита важнейших сетей и информационных инфраструктур предполагает уменьшение уязвимости таких инфраструктур ко всем видам нападений, с тем чтобы сократить ущерб и время, необходимое для ликвидации последствий такого нападения.

12. Помимо этого, эффективная защита невозможна без взаимодействия, координации и сотрудничества на национальном и международном уровнях всех заинтересованных сторон — представителей промышленных и научных кругов, частного сектора и государственных образований, включая учреждения, занимающиеся охраной объектов инфраструктуры, и правоохранительные учреждения. Усилия в этой области необходимо осуществлять с уделением должного внимания обеспечению безопасности информации и соблюдению применимых норм, касающихся предоставления взаимной правовой помощи и охраны неприкосновенности частной жизни. В интересах достижения этих целей государства следует поощрять к применению следующих 11 принципов, которые были разработаны экспертами по вопросам защиты важнейших информационных инфраструктур из стран «большой восьмерки» и впоследствии приняты министрами юстиции и внутренних дел стран «большой восьмерки» в мае 2003 года, в ходе разработки ими стратегии, направленной на уменьшение угрозы для важнейших информационных инфраструктур:

a) страны должны располагать сетями для срочного предупреждения о факторах уязвимости, угрозах и инцидентах в кибернетическом пространстве;

b) страны должны повышать степень информированности заинтересованных сторон, с тем чтобы они более глубоко понимали характер и масштабы своих важнейших информационных инфраструктур и ту роль, которую каждый из них должен играть в защите этих инфраструктур;

c) страны должны анализировать свои инфраструктуры и выявлять факторы взаимозависимости, улучшая тем самым защиту таких инфраструктур;

d) странам следует содействовать развитию партнерских связей между заинтересованными сторонами, включая государственные и частные структуры, для обмена информацией о важнейших инфраструктурах и анализа такой информации с целью предотвращения и расследования причиненного ущерба или попыток нарушения защиты таких инфраструктур, а также с целью принятия необходимых мер в этой связи;

e) странам следует создавать и обеспечивать функционирование и проверку систем коммуникации в кризисной ситуации, с тем чтобы обеспечить их надежную и стабильную работу в чрезвычайных ситуациях;

f) странам следует принять меры к тому, чтобы в стратегиях предоставления доступа к данным учитывалась необходимость защиты важнейших информационных инфраструктур;

g) странам следует содействовать отслеживанию попыток нарушения защиты важнейших информационных инфраструктур и, при необходимости, предоставлять информацию о результатах такого отслеживания другим странам;

h) странам следует обеспечивать учебную подготовку кадров и проводить тренировки с целью укрепления своего потенциала в области реагирования и для опробования планов обеспечения непрерывной работы и планов на случай попыток нарушения защиты информационных инфраструктур, а также побуждать заинтересованные стороны к участию в аналогичных мероприятиях;

i) странам следует обеспечить принятие надлежащих основных и процедурных законоположений, подобных тем, что изложены в Конвенции Совета Европы о кибернетической преступности, а также наличие квалифицированного персонала, который позволял бы им расследовать попытки нарушения защиты важнейших информационных инфраструктур и привлекать к ответственности причастных к этим попыткам лиц, а также, при необходимости, координировать такие расследования с другими странами;

j) страны, при необходимости, должны участвовать в международном сотрудничестве для обеспечения безопасности важнейших информационных инфраструктур, в том числе путем создания и координации систем срочного предупреждения, обмена информацией о факторах уязвимости, угрозах и инцидентах и анализа этой информации, а также путем координации расследований попыток нарушения защиты таких инфраструктур в соответствии с национальным законодательством;

k) странам следует поощрять национальные и международные научные исследования и научно-технические разработки, а также применение технологий обеспечения безопасности, сертифицированных в соответствии с международными стандартами.

13. Повышения уровня безопасности сетей и информационных инфраструктур можно добиться путем организации просветительских и учебных мероприятий, разработки соответствующей политики и законодательства и налаживания международного сотрудничества, а также путем применения соответствующих технологий.

14. Организации Объединенных Наций и другим многосторонним учреждениям необходимо оказать поддержку в их усилиях, направленных на принятие государствами-членами следующих мер:

a) проведение оценки степени защищенности их важнейших национальных сетей и информационных инфраструктур, включая углубленное понимание факторов их уязвимости и взаимозависимости;

b) организация просветительских мероприятий и повышение уровня осведомленности национальных участников о наилучших методах обеспечения безопасности информационных сетей и инфраструктур;

c) принятие эффективного законодательства, предусматривающего уголовную ответственность за противоправное использование информационных технологий, и содействие трансграничному расследованию кибернетических преступлений;

d) установление партнерских отношений между органами государственного управления и промышленными кругами, стимулирующих обеспечение безопасности их национальных систем;

e) создание национального потенциала для предупреждения инцидентов и принятия ответных мер и разработка процедур обмена информацией на национальном и международном уровнях.

## Венесуэла

[Подлинный текст на испанском языке]
[28 июня 2004 года]

1. Правительство Боливарианской Республики Венесуэла считает, что любое нарушение информационной безопасности является посягательством на законное право государства полностью осуществлять свой суверенитет, и поэтому использование информационных средств и технологий в целях политической и экономической дестабилизации идет вразрез с основополагающими принципами демократии.

2. Таким образом, информационная безопасность имеет два основных аспекта: один из них связан с обеспечением безопасности и защиты информации; а другой — с правомерным использованием и достоверностью этой информации. Как незаконное использование, так и преднамеренное неиспользование информационных и телекоммуникационных систем или информационных ресурсов в целях дестабилизации является фактором, подрывающим международную безопасность.

3. Боливарианская Республика Венесуэла поддерживает разработку международных принципов, направленных на повышение безопасности глобальных информационных и телекоммуникационных систем и позволяющих вести борьбу с терроризмом и преступностью в информационной сфере или способствующих такой борьбе, без ущемления суверенитета государств.