



Генеральная Ассамблея

Distr.: General

10 July 2000

Russian

Original: Arabic/English/Russian

Пятьдесят пятая сессия

Пункт 69 предварительной повестки дня*

**Достижения в сфере информатизации
и телекоммуникации в контексте
международной безопасности**

Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности

Доклад Генерального секретаря**

Содержание

	<i>Стр.</i>
I. Введение	2
II. Ответы, полученные от правительств	2
Иордания	2
Катар	3
Российская Федерация	3

* A/55/150.

** Настоящий доклад подготовлен на основе материалов, представленных государствами-членами.

I. Введение

1. В пунктах 2 и 3 своей резолюции 54/49 от 1 декабря 1999 года, озаглавленной «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», Генеральная Ассамблея просила все государства-члены информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам: а) общая оценка проблем информационной безопасности, б) определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов, и с) целесообразность разработки международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и криминалом, а также просила Генерального секретаря представить доклад Генеральной Ассамблее на ее пятьдесят пятой сессии.

2. 14 марта 2000 года Генеральный секретарь направил государствам-членам вербальную ноту с просьбой представить их мнения в ответ на просьбу Ассамблеи. Ответы, полученные от правительств на сегодняшний день, воспроизводятся в главе II настоящего доклада. Любые другие поступающие ответы будут издаваться в качестве добавлений к настоящему докладу.

II. Ответы, полученные от правительств

Иордания

[Подлинный текст на арабском языке]
[16 мая 1999 года]

1. Применение информационно-технологических систем привело к положительным результатам для международного сообщества в плане поддержания стабильности и безопасности, однако злоупотребления этими новыми достижениями и методами:

а) облегчат организацию террористических сетей, элементы которых разбросаны по весьма широкому географическим пространствам, с учетом возможностей быстрой связи;

б) затруднят контроль за современными средствами связи с учетом быстро возникающих технологических сложностей и существования в большинстве стран законов, ограничивающих вмешательство в свободу коммуникации, которой пользуются все люди.

2. С учетом нашей приверженности делу принятия надлежащих мер и в качестве мер предосторожности против террористической деятельности мы рекомендуем следующее:

а) разработать специальное чрезвычайное законодательство, с тем чтобы позволять службам безопасности получать доступ в центры управления

компаниями, связанными с передовыми системами, и частично контролировать их;

b) координировать вместе с компаниями и ведомствами, занимающимися обеспечением связи, усилия по подготовке специалистов из служб безопасности для работы с такими системами в периоды кризисов;

c) оказывать поддержку сектору информационной технологии и техники связи и связанным с ним концепциям безопасности, а также обеспечивать инфраструктуру и надлежащую подготовку для содействия поддержанию международного мира и безопасности.

Катар

[Подлинный текст на арабском языке]
[17 мая 1999 года]

1. Шпионаж: предотвращение доступа неуполномоченной стороны к содержанию глобальных информационных и телекоммуникационных систем.
2. Саботаж: предотвращение частичного или полного уничтожения глобальных информационных и телекоммуникационных систем.
3. Регистрация: регистрация информации, направленной через глобальные информационные системы или телекоммуникационные системы, включая интеллектуальную собственность.
4. Подделка: предотвращение подделки информации, направляемой через глобальные информационные и телекоммуникационные системы.
5. Защита: разработка мер по электронной защите информации, направляемой через глобальные информационные и телекоммуникационные системы.
6. Законодательство: разработка необходимых законов в отношении всех электронных операций в целях обеспечения прав участников и наказания правонарушителей.

Российская Федерация

[Подлинный текст на русском языке]
[12 мая 1999 года]

Принципы, касающиеся международной информационной безопасности

Использование терминов

Для целей настоящих принципов применяются следующие термины:

1. **Информационное пространство** — сфера деятельности, связанная с созданием, преобразованием и использованием информации, включая индивидуальное и общественное сознание, информационно-телекоммуникационную инфраструктуру и собственную информацию.

2. **Информационные ресурсы** — информационная инфраструктура (технические средства и системы формирования, обработки, хранения и передачи информации), включая массивы и базы данных и собственную информацию и ее потоки.
3. **Информационная война** — противоборство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным структурам, подрыва политической, экономической и социальной систем, а также массовой психологической обработки населения с целью дестабилизации общества и государства.
4. **Информационное оружие** — средства и методы, применяемые с целью нанесения ущерба информационным ресурсам, процессам и системам государства, негативного информационного воздействия на оборонные, управленческие, политические, социальные, экономические и другие критически важные системы государства, а также массовой психологической обработки населения с целью дестабилизации общества и государства.
5. **Информационная безопасность** — состояние защищенности основных интересов личности, общества и государства в информационном пространстве, включая информационно-телекоммуникационную инфраструктуру и собственно информацию в отношении таких ее свойств, как целостность, объективность, доступность и конфиденциальность.
6. **Угроза информационной безопасности** — факторы, создающие опасность основным интересам личности, общества и государства в информационном пространстве.
7. **Международная информационная безопасность** — состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.
8. **Неправомерное использование информационно-телекоммуникационных систем и информационных ресурсов** — использование телекоммуникационных и информационных систем и ресурсов без соответствующих прав или с нарушением установленных правил, законодательства или норм международного права.
9. **Несанкционированное вмешательство в информационно-телекоммуникационные системы и информационные ресурсы** — вмешательство в процессы сбора, обработки, накопления, хранения, отображения, поиска, распространения и использования информации с целью нарушения нормального функционирования информационных систем или нарушение целостности, конфиденциальности и доступности информационных ресурсов.
10. **Критически важные структуры** — объекты, системы и институты государства, целенаправленное воздействие на информационные ресурсы которых может иметь последствия, прямо затрагивающие национальную безопасность (транспорт, энергоснабжение, кредитно-финансовая сфера, связь, органы государственного управления, система обороны, правоохранительные

органы, стратегические информационные ресурсы, научные объекты и научно-технические разработки, объекты повышенной технической и экологической опасности, органы ликвидации последствий стихийных бедствий и иных чрезвычайных ситуаций).

11. Международный информационный терроризм — использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в террористических целях.

12. Международная информационная преступность — использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в противоправных целях.

Принцип I

1. Деятельность каждого государства и других субъектов международного права в международном информационном пространстве должна способствовать общему социальному и экономическому развитию и осуществляться таким образом, чтобы быть совместимой с задачами поддержания мировой стабильности и безопасности, суверенными правами других государств, интересами безопасности, принципами мирного урегулирования споров и конфликтов, неприменение силы, невмешательства во внутренние дела, уважения прав и свобод человека.

2. Такая деятельность также должна быть совместимой с правом каждого искать, получать и распространять информацию и идеи, как это зафиксировано в соответствующих документах Организации Объединенных Наций, с учетом того, что такое право может быть ограничено законом в целях защиты интересов безопасности каждого государства.

3. При этом каждое государство и другие субъекты международного права должны иметь равные права на защиту своих информационных ресурсов и критически важных структур от неправомерного использования и несанкционированного информационного вмешательства и могут рассчитывать на поддержку мирового сообщества в реализации этих прав.

Принцип II

Государства будут стремиться к ограничению угроз в сфере международной информационной безопасности и с этой целью воздерживаться от:

- a) разработки, создания и использования средств воздействия и нанесения ущерба информационным ресурсам и системам другого государства;
- b) целенаправленного информационного воздействия на критически важные структуры другого государства;
- c) информационного воздействия с целью подрыва политической, экономической и социальной системы других государств, психологической обработки населения с целью дестабилизации общества;

d) несанкционированного вмешательства в информационно-телекоммуникационные системы и информационные ресурсы, а также их неправомерного использования;

e) действий, ведущих к доминированию и контролю в информационном пространстве;

f) противодействия доступу к новейшим информационным технологиям, создания условий технологической зависимости в сфере информатизации в ущерб другим государствам;

g) поощрения действий международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных правонарушителей, представляющих угрозу информационным ресурсам и критически важным структурам государств;

h) разработки и принятия планов, доктрин, предусматривающих возможность ведения информационных войн и способных спровоцировать гонку вооружений, а также вызвать напряженность в отношениях между государствами и собственно возникновение информационных войн;

i) использования информационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационной сфере;

j) трансграничного распространения информации, противоречащей принципам и нормам международного права, а также внутреннему законодательству конкретных стран;

k) манипулирования информационными потоками, дезинформации и сокрытия информации с целью искажения психологической и духовной среды общества, эрозии традиционных культурных, нравственных, этических и эстетических ценностей;

l) информационной экспансии, приобретения контроля над национальными информационно-телекоммуникационными инфраструктурами другого государства, включая условия их функционирования в международном информационном пространстве.

Принцип III

Организация Объединенных Наций и соответствующие учреждения системы Организации Объединенных Наций будут содействовать международному сотрудничеству, целью которого является ограничение угроз в сфере международной информационной безопасности, и формированию с этой целью международно-правовой основы для:

a) определения признаков и классификации информационных войн;

b) определения признаков и классификации информационного оружия и средств, которые можно отнести к информационному оружию;

c) ограничения оборота информационного оружия;

d) запрещения разработки, распространения и применения информационного оружия;

- e) предотвращения угрозы возникновения информационных войн;
- f) признания опасности применения информационного оружия в отношении критически важных структур, сравнимой с опасностью применения оружия массового поражения;
- g) создания условий для равноправного и безопасного международного информационного обмена на основе общепризнанных норм и принципов международного права;
- h) предотвращения использования информационных технологий и средств в террористических и других преступных целях;
- i) предотвращения использования информационных технологий и средств для воздействия на общественное сознание с целью дестабилизации общества и государства;
- j) разработки процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия;
- k) создания системы международного мониторинга для отслеживания угроз, проявляющихся в информационной сфере;
- l) создания механизма контроля выполнения условий режима международной информационной безопасности;
- m) создания механизма разрешения конфликтных ситуаций в сфере информационной безопасности;
- n) создания международной системы сертификации технологий и средств информатизации и телекоммуникации (в том числе программно-технических) в части гарантий их информационной безопасности;
- o) развития системы международного взаимодействия правоохранительных органов по предотвращению и пресечению правонарушений в информационном пространстве;
- p) гармонизации на основе добровольности национального законодательства в части обеспечения информационной безопасности.

Принцип IV

Государства и другие субъекты международного права должны нести международную ответственность за деятельность в информационном пространстве, осуществляемую ими, под их юрисдикцией или в рамках международных организаций, членами которой они являются, и за соответствие любой такой деятельности принципам, содержащимся в настоящем документе.

Принцип V

Любой спор между государствами и другими субъектами международного права, возникающий из применения настоящих принципов, разрешается с помощью установленных процедур мирного урегулирования споров.