Генеральная Ассамблея

Distr.: General
31 January 2003

Пятьдесят седьмая сессия
Пункт 84 *с* повестки дня

Резолюция, принятая Генеральной Ассамблеей

[*по докладу Второго комитета (A/57/529/Add.3)*]

57/239. Создание глобальной культуры кибербезопасности

Генеральная Ассамблея,

отмечая растущую зависимость государственных органов, предприятий, других организаций и индивидуальных пользователей от информационных технологий в плане предоставления насущно необходимых товаров и услуг, ведения дел и обмена информацией,

признавая, что по мере все большего вовлечения стран в информационное общество возрастает необходимость обеспечения кибербезопасности,

ссылаясь на свои резолюции 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,

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 и 57/53 от 22 ноября 2002 года о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности,

сознавая, что эффективная кибербезопасность зависит не только от действий государственных или правоохранительных органов и что она должна достигаться превентивными мерами и пользоваться поддержкой во всем обществе,

сознавая также, что кибербезопасность нельзя обеспечить с помощью одной только технологии и что приоритет должен отдаваться планированию кибербезопасности и управлению ее обеспечением во всем обществе,

признавая, что государственные органы, предприятия, другие организации и индивидуальные владельцы и пользователи информационных технологий должны, с учетом их соответствующей роли, знать о соответствующих факторах, угрожающих кибербезопасности, и о превентивных мерах и должны сознавать свою ответственность и принимать меры в отношении повышения безопасности этих информационных технологий,

признавая также, что несоответствия в уровне доступа различных государств к информационным технологиям и их использования могут снизить эффективность международного 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 в целях достижения кибербезопасности 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 безопасных информационно-коммуникационных технологий и сетей и содействия обеспечению всеобщего доступа,

отмечая, что в результате усиливающейся взаимосвязанности информационные системы и сети подвергаются сейчас все более многочисленным и разнообразным угрозам и факторам уязвимости, которые создают для всех новые проблемы в плане безопасности,

отмечая также работу соответствующих международных и региональных организаций над повышением кибербезопасности и безопасности информационных технологий,

1. *принимает к сведению* элементы, прилагаемые к настоящей резолюции, в интересах создания глобальной культуры кибербезопасности;

2. *предлагает* всем соответствующим международным организациям учитывать, в частности, эти элементы для создания такой культуры в любой будущей работе по вопросам кибербезопасности;

3. *предлагает* государствам-членам учитывать эти элементы, в частности, в рамках их усилий по развитию у себя в обществе культуры кибербезопасности при применении и использовании информационных технологий;

4. *предлагает* государствам-членам и всем соответствующим международным организациям учитывать, в частности, эти элементы и необходимость глобальной культуры кибербезопасности при подготовке к Всемирной встрече на высшем уровне по вопросам информационного общества, которая состоится в Женеве 10–12 декабря 2003 года и в Тунисе в 2005 году;

5. *подчеркивает* необходимость сод–ействия передаче информационной технологии развивающимся странам и созданию в них потенциала в целях оказания им помощи в принятии мер в области кибербезопасности.

78-е пленарное заседание,
20 декабря 2002 года

Приложение

Элементы для создания глобальной культуры кибербезопасности

Стремительное развитие информационной технологии изменило то, как государственные органы, предприятия, другие организации и индивидуальные пользователи, которые разрабатывают эти информационные системы и сети, имеют, поставляют их, управляют ими, обслуживают и используют их («участники»), должны подходить к кибербезопасности. Глобальная культура

кибербезопасности будет требовать от всех участников учета следующих девяти взаимодополняющих элементов:

a) *осведомленность*. Участники должны быть осведомлены о необходимости безопасности информационных систем и сетей и о том, что они могут сделать для повышения безопасности;

b) *ответственность*. Участники отвечают за безопасность информационных систем и сетей сообразно с ролью каждого из них. Участники должны подвергать свои политику, практику, меры и процедуры регулярному обзору и оценивать, соответствуют ли они среде их применения;

c) *реагирование*. Участники должны принимать своевременные и совместные меры по предупреждению инцидентов, затрагивающих безопасность, их обнаружению и реагированию на них. Они должны обмениваться в надлежащих случаях информацией об угрозах и факторах уязвимости и вводить процедуры, предусматривающие оперативное и эффективное сотрудничество в деле предупреждения таких инцидентов, их обнаружения и реагирования на них. Это может предполагать трансграничный информационный обмен и сотрудничество;

d) *этика*. Поскольку информационные системы и сети проникли во все уголки современного общества, участникам необходимо учитывать законные интересы других и признавать, что их действия или бездействие могут повредить другим;

e) *демократия*. Безопасность должна обеспечиваться так, чтобы это соответствовало ценностям, которые признаются демократическим обществом, включая свободу обмена мыслями и идеями, свободный поток информации, конфиденциальность информации и коммуникации, надлежащая защита информации личного характера, открытость и гласность;

f) *оценка риска*. Все участники должны выполнять периодическую оценку риска, которая: позволяет выявлять угрозы и факторы уязвимости; имеет достаточно широкую базу, чтобы охватить такие ключевые внутренние и внешние факторы, как технология, физические и человеческие факторы, применяемая методика и услуги третьих лиц, сказывающиеся на безопасности; дает возможность определить допустимую степень риска; и помогает выбрать надлежащие инструменты контроля, позволяющие регулировать риск потенциального ущерба информационным системам и сетям с учетом характера и значимости защищаемой информации;

g) *проектирование и внедрение средств обеспечения безопасности*. Участники должны рассматривать соображения безопасности в качестве важнейшего элемента планирования и проектирования, эксплуатации и использования информационных систем и сетей;

h) *управление обеспечением безопасности*. Участники должны принять комплексный подход к управлению обеспечением безопасности, опираясь на динамичную оценку риска, охватывающую все уровни деятельности участников и все аспекты их операций;

i) *переоценка*. Участники должны подвергать вопросы безопасности информационных систем и сетей обзору и повторной оценке и вносить надлежащие изменения в политику, практику, меры и процедуры обеспечения безопасности, учитывая при этом появление новых и изменение прежних угроз и факторов уязвимости.