Организация Объединенных Наций A/61/161

Генеральная Ассамблея

Distr.: General
18 July 2006
Russian
Original: Arabic/Chinese/English/
Spanish

Шестьдесят первая сессия
Пункт 82 предварительной 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

Содержание

*A/61/150.

06-43427 (R) 110806 110806

I. Введение

1. В пункте 3 своей резолюции 60/45, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», Генеральная Ассамблея просила все государства-члены продолжать информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам: a) общая оценка проблем информационной безопасности; b) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области; c) содержание концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем; и d) возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне.

2. 23 февраля 2006 года государствам-членам была направлена вербальная нота, в которой им предлагалось сообщать Генеральному секретарю свои мнения и оценки по этому вопросу. Полученные ответы содержатся в разделе II ниже. По мере поступления новых ответов они будут издаваться в качестве добавлений к настоящему докладу.

II. Ответы, полученные от правительств

Боливия

[Подлинный текст на испанском языке]
[13 июня 2006 года]

В резолюции 60/45, принятой Генеральной Ассамблеей Организации Объединенных Наций, содержится призыв к рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных мер по ограничению угроз, возникающих в этой сфере, исходя из необходимости сохранить свободный поток информации.

Общий обзор проблем в сфере информационной безопасности

Значительный прогресс, достигнутый в области развития и применения новых информационных технологий и средств телекоммуникации, таких, как Интернет, факсимильная связь и спутниковые сотовые телефоны, открывает для всех людей в мире неограниченный доступ к информации, в том числе потенциально, и к секретной информации.

В то же время этот процесс открывает большие возможности для развития цивилизации путем расширения сотрудничества ради общего блага государств и достижения новых целей в интересах всего человечества.

С точки зрения защиты информации уровень информационной безопасности неудовлетворителен (он зависит от того, какая компания обеспечивает такие услуги). Никакой внутренней политики обеспечения безопасности не существует.

Меры, принимаемые на национальном уровне для обеспечения информационной безопасности и участия в международном сотрудничестве в этой сфере

С учетом существующих и потенциальных угроз в сфере информационной безопасности и безопасности телекоммуникаций в рамках возможных мер сотрудничества разработаны процедуры доведения своевременно полученной информации до сведения министерств информации, которая регулируется Управлением телекоммуникаций.

С точки зрения защиты информации меры, принимаемые для обеспечения ее безопасности, не соответствуют современному уровню технического развития.

В настоящее время осуществляются проекты в области телекоммуникаций, в рамках которых принимаются меры для обеспечения максимально возможной безопасности информации путем использования систем кодирования передаваемой информации, для того чтобы частично или полностью устранить эти недостатки.

Содержание концепций, упомянутых в пункте 2 резолюции 60/45 Генеральной Ассамблеи

Содействовать достижению целей, предложенных в пункте 2, можно было бы, вероятно, с помощью анализа соответствующих международных концепций в целях укрепления безопасности мировых информационных и телекоммуникационных систем.

Меры, которые могло бы принять международное сообщество для укрепления информационной безопасности в глобальном масштабе

- Осуществить анализ проблем в области информационной безопасности и безопасности телекоммуникаций на международном уровне;
- определить основные критерии, касающиеся безопасности информации и телекоммуникаций, несанкционированного доступа или незаконного использования этих систем с помощью Интернета;
- разработать международные принципы, которые позволили бы повысить безопасность информационных и телекоммуникационных систем в мире, что содействовало бы борьбе с терроризмом и торговлей секретной информацией;
- выразить озабоченность в связи с тем, что такие средства и технологии могут быть использованы для подрыва стабильности и безопасности государств;
- в военной и оборонной сфере внедрить телекоммуникационные системы, защита которых обеспечивалась бы с учетом новейших технических достижений в мире.

Рекомендации

Информационную безопасность должно обеспечивать государство в рамках политики, разработанной на основе соответствующего законодательства в

области телекоммуникаций, и регулируемой и контролируемой Управлением телекоммуникаций.

В целях обеспечения информационной безопасности на национальном уровне следовало бы осуществлять соответствующие проекты, используя новейшие технические достижения для принятия максимально эффективных мер безопасности, аналогичных тем, что используются в оперативных программах.

Китай

[Подлинный текст на китайском языке]
[24 мая 2006 года]

Информационные технологии переживают в настоящее время период бурного роста своего развития и стали важным позитивным фактором экономического и социального развития стран, а также улучшения жизни их народов. Вместе с тем в связи с разработкой и широким применением информационных технологий возникли беспрецедентные трудности в обеспечении безопасности как отдельных государств, так и международного сообщества в целом. Проблема информационной безопасности уже стала одним из основных факторов, который отражается на всеобъемлющей безопасности государств и даже глобальной безопасности и стабильности. Надлежащим решением этой проблемы, которое отвечало бы коллективным интересам всех стран, является совместная ответственность международного сообщества.

Китай считает, что проблема информационной безопасности — это не только риски, обусловленные слабостью основной информационной инфраструктуры, но и политические, экономические, военные, социальные, культурные и многие другие проблемы, которые возникают в результате несанкционированного использования информационных технологий. Поэтому при рассмотрении проблемы информационной безопасности этим двум факторам следует уделять одинаковое внимание.

Китай считает, что информационные технологии должны использоваться в соответствии с целями Устава Организации Объединенных Наций и основными принципами международных отношений; беспрепятственный поток информации следует гарантировать с учетом необходимости обеспечения национального суверенитета и безопасности и уважения существующих между странами исторических, культурных и политических различий; каждая страна имеет право на использование своего собственного киберпространства в соответствии со своим внутренним законодательством; кроме того, учитывая неравномерный уровень развития стран в области телекоммуникаций, международное сообщество должно активизировать свое сотрудничество в проведении исследований и использовании информационных технологий и сделать все для того, чтобы обеспечить, чтобы каждая страна могла воспользоваться преимуществами свободы информационных технологий.

Организация Объединенных Наций является надлежащим форумом для решения проблемы информационной безопасности. И хотя группа правительственных экспертов по информационной безопасности не сумела добиться в 2005 году существенных результатов, тем не менее эксперты разных стран провели широкий обмен мнениями и предложили множество ценных решений по целому комплексу вопросов, касающихся информационной безопасности,

заложив тем самым прочную основу для дальнейших обсуждений международным сообществом проблем информационной безопасности и их решения. Китай поддерживает идею того, чтобы Организация Объединенных Наций воссоздала в 2009 году группу правительственных экспертов для проведения тщательного и всеобъемлющего исследования, касающегося угроз и проблем в области информационной безопасности, и рассмотрела также вопрос о соответствующих программах и политики для их преодоления. Катай, как и прежде, будет поддерживать международные усилия, направленные на решение проблемы информационной безопасности, и принимать участие в этих усилиях.

Иордания

[Подлинный текст на арабском языке]
[5 июня 2006 года]

Информационная безопасность связана с концепцией национальной безопасности, и система информационной безопасности непосредственно связана с безопасностью в сфере телекоммуникаций, поскольку передача и обмен информации производится именно с использованием сетей, будь то проводных или беспроводных, телекоммуникаций. Для обеспечения защиты и укрепления информационной и телекоммуникационной безопасности необходимо:

a) разработать положения, законодательство и системы для защиты конфиденциальности, неприкосновенности и предоставления информации, а также для противодействия посягательствам на информацию и использованию информационных систем для совершения преступлений;

b) разработать национальный план в целях обеспечения информационной, телекоммуникационной и сетевой безопасности при содействии тех, кто работает в информационном и сетевом секторе. Этот план должен обеспечивать:

1) конфиденциальность и надежность: обеспечение неразглашения информации и предотвращение того, чтобы она стала достоянием лиц, не имеющих к ней допуска;

2) цельность содержания: обеспечение цельности содержания, чтобы оно не было изменено или искажено, чтобы не было уничтожено, переработано или исправлено на каком-либо этапе ее обработки или обмена ею, будь то при работе с нею внутри или в результате незаконного вмешательства;

3) обеспечить непрерывное предоставление информации или услуг: обеспечить непрерывное функционирование информационных систем и непрерывную возможность использовать информацию или предоставлять услуги информационным объектам и обеспечить, чтобы пользователь информации не лишался возможности ее использования или доступа к ней;

4) неотрекаемость от совершения действий в отношении информации причастными к этому процессу лицами: обеспечить, чтобы лица, участвующие в информационных процессах или работающие на информационных объектах, не могли отрицать свою причастность к совершению действий, поскольку имеется возможность доказать, что то или иное кон-

кретное действие было совершено тем или иным конкретным лицом в то или иное конкретное время;

с) разработать стратегию информационной безопасности, т.е. установить комплекс правил, которые должны соблюдать лица, работающие с техникой и информацией в учреждениях, обеспечивающих ввод информации и работающих с информационными системами или управляющих ими. Цель этой стратегии заключается в том, чтобы: сообщить пользователям и руководителям об их обязанностях и долге по обеспечению защиты компьютерных систем и сетей, а также защиты информации во всех ее формах на всех этапах ввода, обработки, хранения, передачи и извлечения информации.

Ливан

[Подлинный текст на арабском языке]
[21 июня 2006 года]

Отвечая на вопрос, касающийся разработок, ведущихся в области информации и телекоммуникаций в свете проблем международной безопасности, Министерство национальной обороны хотело бы заявить следующее.

В связи с проблемами информационной безопасности следует отметить, что информационные сети вооруженных сил представляют собой закрытые сети, в отношении которых ввиду отсутствия современных технологий для обеспечения защиты информации по причине дороговизны их внедрения применяются пассивные меры безопасности. Что касается телекоммуникационных сетей, то они являются частью национальной структуры гражданских коммуникаций, деятельность которой регулируется общим законодательством, и поэтому меры безопасности на нее не распространяются.

Предпринимаемые на национальном уровне усилия по укреплению информационной безопасности для обеспечения судебного преследования в связи с вопросами, касающимися информационных технологий и телекоммуникаций, существенно разнятся, поскольку последние значительно опережают законодательство. В Ливане в настоящее время действует закон № 140 от 27 октября 1999 года, касающийся защиты права на конфиденциальность переписки и условий ее перехвата на основе решения суда или административного решения в соответствии с положениями статей 2–13 указанного закона. Следует при этом отметить, что данный закон не обеспечивает основы для координации деятельности органов безопасности и деловых кругов гражданского сектора (ISP-GSM) с целью унификации мер по уголовному преследованию, расследованию и предупреждению потенциальных угроз в этой области. Это обстоятельство свидетельствует о необходимости международного сотрудничества в этой области, а также передачи технических и юридических знаний и опыта для того, чтобы восполнить пробел, существующий между законодательством и развитием технологий в Ливане.

Катар

[Подлинный текст на арабском языке]
[12 июня 2006 года]

В том что касается деятельности в области телекоммуникаций в связи с международной безопасностью, правительство Государства Катар предпринимает большие усилия для обеспечения всеобъемлющего контроля в вопросах информационной и телекоммуникационной безопасности с целью предотвращения реальных и потенциальных угроз, связанных с информационной безопасностью, разрабатывая для этого необходимое законодательство.

Недавно в Катаре создан Высший совет по коммуникациям и информационным технологиям, в структуре которого имеется юридический департамент, которому поручено разработать проект государственного закона в области электроники и представить его на рассмотрение компетентных властей, обеспечить его ратификацию и вступление в силу в нынешнем году. Цель указанного проекта закона состоит в предотвращении использования компьютерной техники или технологии в преступных или террористических целях. Указанный закон должен также обязать компетентные власти разработать определение преступных и террористических целей, чтобы государства-члены ясно понимали, о чем идет речь, чтобы они могли выполнять свои обязанности в полном объеме и попытаться выработать стандартные определения концепций, по которым еще не достигнуто международной договоренности, для того чтобы содействовать их обсуждению на международных форумах.

Объединенные Арабские Эмираты

[Подлинный текст на английском языке]
[17 июня 2006года]

Объединенные Арабские Эмираты осознают растущую угрозу киберпреступности и признают, что совершаемые в киберпространстве преступления не ограничиваются пределами традиционных государственных границ. Современные информационно-коммуникационные системы позволяют осуществлять преступную деятельность из любой точки, против любого лица, в любом месте.

Для успешной борьбы с киберпреступностью необходимы действенные меры на национальном и международном уровнях.

Объединенные Арабские Эмираты прилагают значительные усилия для укрепления информационной безопасности на национальном уровне, в том числе с помощью следующих мер:

- **Закон Объединенных Арабских Эмиратов о борьбе с киберпреступностью**

Закон о борьбе с киберпреступностью был принят и опубликован в начале 2006 года. Он включает следующие аспекты:

– преступления, связанные с доступом (несанкционированный доступ, распространение вирусов, хакинг, хищение личных данных);

– преступления в отношении данных (перехват, изменение, похищение, использование личной информации);

– преступления в отношении сетей (создание помех, изменение, разрушение);

– прочие сопутствующие преступления (пособничество совершению преступлений, незаконному обороту наркотиков, торговле людьми, отмыванию денег, совершению террористических актов).

Закон охватывает также аспекты цензуры и использования предосудительных материалов. Нарушение закона о борьбе с киберпреступностью влечет за собой тюремное заключение или штраф или и то и другое.

• **Инициатива по созданию национальной группы по борьбе с компьютерными авариями**

Управление по телекоммуникации Объединенных Арабских Эмиратов рассматривает возможность создания национальной группы по борьбе с компьютерными авариями (НГКА) для укрепления безопасности, реагирования на кибернападения, своевременного оповещения об опасности и распространения информации о киберугрозах, координации всей деятельности по борьбе с компьютерными авариями и информирования населения с помощью учебно-просветительских мероприятий в стране.

• **Кодекс поведения поставщиков Интернет-услуг**

В Объединенных Арабских Эмиратах завершается подготовка обязательного кодекса поведения для поставщиков Интернет-услуг, который должен повысить эффективность работы поставщиков Интернет-услуг и их активность для сокращения объема электронных сообщений, которые могут содержать вирусы. Ожидается, что поставщики Интернет-услуг будут активно сканировать передаваемые сообщения на предмет выявления открытых релейных сетей, автоматических сетей, прочих сетей зараженных компьютеров, используемых для рассылки сообщений-спамов. От поставщиков Интернет-услуг будут также требовать включать в договоры с пользователями положения, позволяющие им отключать пользователя, если тот преднамеренно или непреднамеренно распространяет сообщения-спамы. Невыполнение какой-либо части кодекса повлечет за собой наложение штрафа или санкций.

Кодекс поведения в Интернете призван заставить поставщиков Интернет-услуг придерживаться высоких стандартов поведения и профессиональной деятельности, принятых в сообществе поставщиков Интернет-услуг.

• **Двусторонние соглашения**

Поставщики Интернет-услуг в Объединенных Арабских Эмиратах принимают активно участие в осуществлении двусторонних соглашений с соседними странами в области борьбы со спамом и добиваются уменьшения объема спам-сообщений, передаваемых за пределы страны. Объединенные Арабские Эмираты поддерживают и поощряют международное сотрудничество в борьбе с киберпреступностью и оказывают содействие в подготовке меморандумов о взаимопонимании по вопросам обмена информацией и трансграничного сотрудничества в правоприменительной области.

• **Кампании/просветительская деятельность, направленные на повышение уровня информированности населения**

Правительство совместно с Управлением по телекоммуникации и крупными предприятиями проводит работу по повышению осведомленности населения и его информирования о преимуществах новых технологий и опасностях, связанных с киберпреступностью.

Так, недавно Управление по телекоммуникации выпустило «Руководство по безопасности беспроводной связи» и «Политику веб-хостинга». В первом из этих документов содержится подробная информация о том, как надо создавать сети беспроводной связи и какие должны приниматься меры для обеспечения их безопасной эксплуатации. Во втором документе говорится о приемлемых формах использования этих услуг, включая: политику, регулирующую использование; политику в отношении сообщений-спамов; политику в отношении случаев нарушения прав интеллектуальной собственности; и политику в отношении противозаконного содержания.

• **Значение мер технического характера в контексте международной безопасности**

Уже разработан ряд мер технического характера, направленных на обеспечение безопасности киберпространства, которые включают:

– создание инфраструктур публичных ключей (ИПК) и разработку защищенных протоколов;

– разработку высококачественного программного обеспечения, эффективных систем защиты компьютеров, антивирусных программ, систем защиты электронных прав, шифровальных систем и т.д.;

– использование «думающих» карт, биометрической идентификации, электронных подписей, ролевых технологий и т.д.

В то же время по мере того, как киберпространство становится все более комплексным, а его компоненты все более сложными, возникают все новые и непредвиденные угрозы. Поэтому необходимо активизировать деятельность по разработке технологий обеспечения безопасности и постоянно учитывать требования безопасности с самого первого этапа разработки любых будущих технологий.

• **Возможные меры по укреплению информационной безопасности на глобальном уровне**

– Международное сотрудничество является непременным условием, поскольку киберпреступность не знает границ и бороться с ней традиционными методами невозможно;

– в стране разработаны общие правовые рамки, которые обеспечат беспрепятственный обмен информацией и сотрудничество между странами. Кроме того, необходимо выработать глобальное определение киберпреступлений, учитывая то, что в разных странах определение этого понятия может быть различным;

– правоохранительные органы должны приспособиться к борьбе с преступлениями, совершаемыми в киберпространстве. Они должны научиться находить и извлекать хранящиеся в компьютерах данные, чтобы не допускать уничтожения улик.