ОРГАНИЗАЦИЯ
ОБЪЕДИНЕННЫХ НАЦИЙ

A

Генеральная Ассамблея

Distr.
GENERAL

A/54/213
10 August 1999
RUSSIAN
ORIGINAL: ENGLISH/ARABIC/
RUSSIAN/SPANISH

Пятьдесят четвертая сессия
Пункт 71 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

* A/54/150.

СОДЕРЖАНИЕ (продолжение)

I. ВВЕДЕНИЕ

1. В пунктах 2 и 3 своей резолюции 53/70 от 4 декабря 1998 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: a) общая оценка проблем информационной безопасности; b) определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов; и c) 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; и просила Генерального секретаря представить ей доклад на ее пятьдесят четвертой сессии.

2. 19 марта 1999 года Генеральный секретарь направил в адрес государств-членов вербальную ноту, в которой предложил им представить свою точку зрения во исполнение просьбы Ассамблеи. Ответы, полученные от правительств, воспроизводятся ниже.

II. ОТВЕТЫ, ПОЛУЧЕННЫЕ ОТ ПРАВИТЕЛЬСТВ

АВСТРАЛИЯ

[Подлинный текст на английском языке]
[2 июня 1999 года]

1. Австралия председательствовала в Группе экспертов Организации экономического сотрудничества и развития (ОЭСР), которая подготовила Руководящие принципы ОЭСР по обеспечению безопасности информационных систем. Австралия председательствует также в Рабочей группе ОЭСР по вопросам информационной безопасности и тайны, которая среди прочих своих обязанностей следит за необходимостью обеспечения информационной безопасности. Австралия участвует в разработке норм безопасности информационной технологии в рамках Международной организации по стандартизации (МОС). Внутри страны введены детальные процедуры обеспечения безопасности правительственной информации, и Госстандарт Австралии совместно с Госстандартом Новой Зеландии разработали на базе английского стандарта совместный стандарт управления информационной безопасностью. Правительство и промышленность Австралии занимаются в настоящее время совместной разработкой мер по охране национальной информационной инфраструктуры. В Австралии принято законодательство, обеспечивающее защиту телекоммуникационных систем от перехвата, вмешательства и других форм неправомерного использования.

2. Задача информационной безопасности, как она изложена в Руководящих принципах ОЭСР по обеспечению безопасности информационных систем и применяется на практике Австралией, заключается в следующем: "... защита интересов сторон, полагающихся на информационные системы, от причинения вреда в результате нарушения доступности, конфиденциальности и неприкосновенности".

3. По мере сближения технологий данная задача может быть распространена на телекоммуникационные системы, являющиеся частным случаем информационной системы. Любое вмешательство или неправомерное использование информационных систем отразится либо на

доступности, либо на конфиденциальности, либо на неприкосновенности. В условиях быстрого технического прогресса существует опасность выработки определений, слишком тесно привязанных к конкретным технологиям.

4. Австралия не разделяет мнения о том, что Департамент по вопросам разоружения Секретариата Организации Объединенных Наций является подходящим органом для разработки международных принципов обеспечения безопасности глобальных информационных и телекоммуникационных систем. Телекоммуникации и информационная инфраструктура оказывают влияние на вопросы торговли, экономического развития и общественного благосостояния, а также охраны правопорядка и национальной безопасности. Принципы и руководящие указания по этим вопросам уже разработаны на других форумах, таких, как ОЭСР, МОС и Международный союз электросвязи (МСЭ), с применением более широких подходов, чем подходы, предложенные в резолюции 53/70 Генеральной Ассамблеи. Кроме того, решением вопросов компьютерных преступлений занимаются такие международные органы, как Азиатский и дальневосточный институт Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями (ЮНАФЕИ) и Центр по международному предупреждению преступности. Австралия не видит смысла в том, чтобы другие органы Организации Объединенных Наций дублировали работу, которая проводится в настоящее время в мире в связи с вопросами безопасности или неправомерного использования компьютерной техники. Австралия поддержала бы предложение о развитии информационного ресурса работы, осуществляемой в рамках других форумов.

БЕЛАРУСЬ

[Подлинный текст на английском языке]
[25 мая 1999 года]

1. Республика Беларусь полностью поддерживает резолюцию 53/70 Генеральной Ассамблеи от 4 декабря 1998 года, озаглавленную "Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности". Активное применение новых информационных технологий и средств телекоммуникации открывает широчайшие возможности для ускоренного развития мировой цивилизации. В то же время, как указано в резолюции 53/70 Ассамблеи, "эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на безопасность государств".

2. Принятие резолюции 53/70 Ассамблеи является своевременным и актуальным, поскольку позволяет привлечь внимание международного сообщества к потенциальному использованию информационных технологий ведения войны и необходимости недопущения новых информационных технологий и средств, военное применение которых можно сравнить с оружием массового поражения. Кроме того, после принятия резолюции 53/70 Генеральной Ассамблеи появилась возможность конкретного рассмотрения проблемы международной информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов. Наконец, целесообразно разработать и согласовать концепцию международной информационной безопасности и международно-правовые принципы, направленные на укрепление безопасности глобальных информационных и телекоммуникационных систем и предупреждение информационного терроризма и преступности.

БРУНЕЙ-ДАРУССАЛАМ

[Подлинный текст на английском языке]
[7 июня 1999 года]

В связи с резолюцией 53/70 Генеральной Ассамблеи от 4 декабря 1998 года, озаглавленной "Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности", Постоянное представительство Брунея-Даруссалама имеет честь представить следующую точку зрения министерства обороны Брунея-Даруссалама:

> "Министерство обороны как министерство, ведающее вопросами национальной обороны, признает важность информационной безопасности в современную эпоху информационной технологии. Министерство считает важным любую форму информации, которая может быть использована и может создавать угрозу национальной безопасности при ее передаче. Однако благодаря имеющимся у него связям с информационной технологией и благодаря наличию в стране других министерств, занимающихся этим вопросом, министерство обороны будет сотрудничать с соответствующими учреждениями в осуществление положений указанной резолюции. В интересах обеспечения и создания гарантий безопасности международных коммуникаций ответственность в данном вопросе не следует считать выходящей за рамки компетенции Международного Суда".

КУБА

[Подлинный текст на испанском языке]
[28 июня 1999 года]

Общая оценка проблем информационной безопасности

1. Широкое использование информационных технологий практически во всех сферах деятельности человека, т.е. процесс "компьютеризации общества", который многие называют "информационным веком" как отражение растущей зависимости от информационных систем в мире, создает новые проблемы безопасности, требующие самого серьезного рассмотрения не только отдельными государствами, но и всем международным сообществом.

2. По этой причине Организация Объединенных Наций является подходящим форумом для обсуждения соответствующих путей и средств преодоления потенциальных угроз для международной безопасности, которые могут возникать в связи с использованием новых информационных и телекоммуникационных технологий в немирных целях.

3. Кроме того, должны приниматься меры для обеспечения доступности этих технологий в целях развития всех государств, особенно слаборазвитых государств, которые не имеют достаточных ресурсов для самостоятельной разработки таких технологий.

4. В то же время процесс глобализации в сфере информатизации и телекоммуникации уже стал реальностью, и расстояния больше не являются препятствием для обмена информацией; в то же время безопасность систем, способствующих обмену информацией, вызывает растущее беспокойство. Следует подчеркнуть, что следствием глобализации является определенный уровень стандартизации, облегчающий вмешательство в эти системы.

5. Не следует забывать о том, что речь идет о технологиях, создаваемых в развитых странах, среди которых Соединенные Штаты Америки, крупнейшая в мире гегемонистская держава, особенно в области информатизации и телекоммуникации, занимает доминирующее положение, позволяющее ей навязывать технологические стандарты, облегчающие использование информационных и телекоммуникационных систем как средство агрессии.

6. Так что у слаборазвитых стран нет другой альтернативы, кроме как принять эти технологии, чтобы выжить в новых условиях. В большинстве случаев эти страны не вполне осознают таящуюся в этом опасность и во многих случаях недостаточно широко используют меры, службы или механизмы обеспечения безопасности. Результатом является уязвимость информационных систем, которая в условиях широкого использования информационных и телекоммуникационных технологий во всех сферах общественного развития может вести к возникновению ситуаций, угрожающих международной безопасности.

7. Куба весьма признательна за предоставленную возможность рассмотреть данный пункт на Генеральной Ассамблее благодаря инициативе, приведшей к принятию консенсусом резолюции 53/70 Ассамблеи. Куба сознает важность данного пункта и будет активно участвовать в проведении оценок, предусмотренных в этой резолюции.

Определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов

8. В современном мире наблюдается беспрецедентный рост использования информационных и телекоммуникационных технологий, который, к сожалению, сделал возможным их использование во враждебных целях для проведения одними государствами агрессивной политики в отношении других государств.

9. В этой связи следует указать, что развитие и популярность глобальных сетей, особенно Интернета, имеет серьезные последствия. Несмотря на их растущее использование, информационные и телекоммуникационные системы по-прежнему функционируют на чисто кооперативной основе. Это важный момент, поскольку добровольный характер Интернета является одновременно источником его сильных и самых слабых качеств.

10. Общий свод правил, обеспечивающих эффективную и повышенную оперативную безопасность глобальных сетей, носит добровольный характер в силу того факта, что страны не приняли единообразного законодательства в отношении функционирования информационных сетей.

11. Однако, поскольку участие в таких глобальных сетях является факультативным, можно с полным основанием утверждать, что любые правила поведения, регулирующие функционирование таких сетей, должны быть составной частью соглашения об участии и что нарушение таких правил, независимо от имеющейся правовой инфраструктуры, может повлечь за собой применение санкций.

12. Безопасность информации включает защиту ее конфиденциальности (информация должна быть доступна только тем, кто имеет право на ее использование), защиту информации от несанкционированного изменения (неприкосновенность) и защиту систем от отказа в обслуживании (доступность) и несанкционированного доступа.

13. В этой связи следует рассмотреть ряд основных критериев:

a) пользователи несут ответственность за свое собственное поведение; иными словами, несанкционированный доступ к компьютеру или несанкционированное использование сети является явным нарушением правил поведения, независимо от того, насколько слабо могут быть защищены информационные системы;

b) организации, пользующиеся этими технологиями, несут ответственность за их надлежащее использование своими сотрудниками и, следовательно, должны разрабатывать с этой целью политику обеспечения безопасности, а также меры и процедуры, обеспечивающие контроль за ее соблюдением. Аналогичным образом, в каждой стране следует создать надлежащие механизмы, обеспечивающие соблюдение этих требований базирующимися на их территории организациями;

c) поставщики компьютерных услуг и сетей несут ответственность за обеспечение безопасности своих систем. Они несут также ответственность за информирование пользователей о своей политике обеспечения безопасности и о любых изменениях в такой политике;

d) продавцы и поставщики систем несут ответственность за обеспечение их надежного функционирования, предусматривающего надлежащие меры обеспечения безопасности. Продавец или поставщик должны оценивать каждую систему до ее выпуска на рынок с точки зрения мер обеспечения безопасности. К каждому товару должно прилагаться описание предусмотренных в нем мер безопасности. Продавцы и поставщики систем обязаны бесплатно устранять дефекты в соответствующих компонентах продаваемых или распространяемых ими систем;

e) пользователи, поставщики услуг и продавцы программного обеспечения и аппаратных средств должны сотрудничать друг с другом в деле обеспечения безопасности. Следует надеяться, что каждый сайт будет уведомлять другие сайты об установленных случаях несанкционированного доступа и что они будут оказывать друг другу помощь в принятии мер по борьбе с нарушениями безопасности. Такая помощь может включать отслеживание связей, выявление нарушений и оказание правовой помощи.

14. Лица, вторгающиеся в информационные сети, преследуют следующие основные цели:

a) получение, изменение или уничтожение информации. Это, несомненно, главная цель большинства нарушителей;

b) проникновение в чужие компьютеры и их использование под видом санкционированных пользователей;

c) создание плацдарма для дальнейших нарушений. Вторжение в системы может преследовать единственную цель их использования в качестве основы для новых вторжений;

d) отказ в обслуживании, т.е. отказ в предоставлении информации лицам, которые в ней нуждаются и имеют право на ее использование;

e) самореклама, что весьма выгодно в случае использования Web-серверов.

15. Неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов, особенно при использовании таких систем и ресурсов некоторыми государствами для проведения своей политики и вмешательства в дела других государств, является нарушением суверенитета и независимости соответствующих государств и создает очаги напряженности, которые могут представлять серьезную угрозу для международной безопасности.

16. Государства, постоянно добивающиеся достижения политических целей в своих национальных интересах, занимаются, с точки зрения установленных международных норм, неправомерным использованием, в частности, радио- и телевизионных станций с целью дестабилизации конституционного порядка других государств, которых они считают своими врагами.

17. Куба является примером государства, по отношению к которому проводится упомянутая в предыдущих пунктах политика. О серьезности этого вопроса можно судить по тому, что Куба в течение многих десятилетий является объектом агрессии со стороны американского радио и телевидения, являющихся составной частью целенаправленной агрессивной политики, проводимой этой самой развитой в военном, экономическом и политическом отношении державой мира, которая объявила своей целью свержение правительства Кубы.

18. С этой целью, например, до апреля 1999 года на территории Соединенных Штатов Америки работало в общей сложности 17 радиостанций, которые передавали на Кубу информацию подрывного содержания.

19. Ежедневный объем радиовещания составлял от 288,5 до 306,5 часов в диапазоне средних, коротких и ультракоротких волн; еженедельная продолжительность радиовещания составляла 2084,5 часов, а если добавить к этому еженедельный объем телевизионных трансляций, то эта цифра составит в общей сложности 2089 часов.

20. В большинстве случаев передаваемая информация подстрекала кубинских граждан к совершению актов гражданского неповиновения и к участию в подрывных и террористических акциях.

21. Куба всегда выступала за устранение разногласий между государствами на основе равенства и уважения их национального суверенитета и независимости и неоднократно делала на этот счет публичные заявления. Эта позиция остается неизменной.

Целесообразность разработки международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и преступностью

22. Развитие новых информационных технологий, несомненно, требует параллельных усилий по обеспечению прогрессивного развития международного права в этой области, включая разработку надлежащей нормативно-правовой базы, которая была бы направлена на укрепление безопасности информационных систем.

23. Задача будет не простой, если учитывать тот факт, что до сих пор сохраняются вопросы, которые потребуют разработки общепринятых определений с целью облегчения последующей кодификации новых принципов, способствующих достижению целей в области безопасности.

24. Глобальные сети уже по одному своему определению выходят далеко за рамки юрисдикции каждой страны; во многих случаях полагаться на географические границы становится невозможным. Кроме того, неодинаковый уровень развития государств, среди прочих факторов, серьезным образом затрудняет разработку унифицированных международных правил, которые были бы общеприменимы ко всем странам, совместно пользующимся этими технологиями.

25. Правда, работа начнется не на пустом месте, поскольку уже существуют общепринятые принципы и международно-правовые документы, которые согласовывались и принимались

государствами на различных многосторонних форумах по мере происходившего в последнее время научно-технического прогресса. Эти принципы и документы оказались бы весьма полезными при составлении или разработке новых международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и преступностью.

26. Среди недавних примеров таких соглашений Куба считает необходимым упомянуть следующие:

a) резолюция 110 (II) Генеральной Ассамблеи от 3 ноября 1947 года, в которой осуждается пропаганда, имеющая целью создать или усилить угрозу миру, нарушение мира или акт агрессии;

b) Международная конвенция электросвязи, принятая в Найроби в 1982 году, а также соответствующие международно-правовые документы, принятые Организацией Объединенных Наций по вопросам образования, науки и культуры и Международным союзом электросвязи;

c) Принципы использования государствами искусственных спутников Земли для международного непосредственного телевизионного вещания, принятые Генеральной Ассамблеей, в которых предусматривается, что такая деятельность должна осуществляться в соответствии с международным правом и таким образом, чтобы она была совместимой с развитием взаимопонимания и укреплением дружественных отношений и сотрудничества между государствами и народами в интересах поддержания международного мира и безопасности;

d) Конвенция о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении, в приложении к которой содержатся положения о защите конфиденциальной информации, которые могли бы также послужить полезным справочным материалом при разработке вышеупомянутых принципов.

27. Наконец, в рамках той ведущей роли, которую следует играть Организации Объединенных Наций в возможном проведении анализа по данному вопросу, Организация, по мнению Кубы, должна, в частности, признать тот факт, что каждая страна имеет право на защиту своих информационных и телекоммуникационных систем с помощью систем обеспечения безопасности, и рекомендовать государствам-членам принять законы, предусматривающие меры наказания за разработку и распространение компьютерных вирусов и других вредоносных программ. Кроме того, в рамках Организации Объединенных Наций могут быть заключены имеющие обязательную юридическую силу многосторонние соглашения, запрещающие агрессивные действия в отношении информационных и коммуникационных систем. Можно также рассмотреть идею заключения соглашений, гарантирующих использование разрабатываемых новых технологий в мирных целях и их доступность для всех государств.

ОМАН

[Подлинный текст на арабском языка]
[22 июня 1999 года]

1. Управление телекоммуникаций Султаната не отвечает за предоставление информации подписчикам, а занимается только обеспечением сетей и технологий, облегчающих доступ к информационным системам.

2. В качестве поставщика сетей и технологий Управление проводит общую оценку проблем информационной безопасности. Безусловно, существует возможность использования предоставляемых Управлением технологий несанкционированными сторонами для получения доступа к информации, и это может иметь негативные последствия.

3. В качестве поставщика телекоммуникационных услуг Управление обычно не несет ответственности за обеспечение безопасности предоставляемой подписчикам информации, которые должны сами принимать необходимые меры предосторожности для соблюдения требований безопасности в отношении получаемой ими информации. Однако Управление может ограничить доступ к информации в общественной сфере через определенные виды служб, например Интернет.

4. Что касается основных понятий, относящихся к информационной безопасности, то в действующих в Султанате правилах, и особенно правилах защиты авторского права, говорится, что информация имеет материальный и нравственный аспекты, и, следовательно, предусматривается ее правовая защита. На основе этого принципа можно определить основные понятия, относящиеся к информационной безопасности. Наиболее важными являются следующие понятия:

a) незаконный перехват информации и данных;

b) незаконное проникновение в компьютерные системы;

c) сбор данных и информации путем шпионажа и подслушивания;

d) вторжение в частную жизнь других людей или нарушение их права на конфиденциальность;

e) предоставление любого рода данных или документов, хранящихся в электронной форме;

f) уничтожение, видоизменение и переадресование данных;

g) сбор и переадресование информации;

h) утечка информации и данных;

i) противоправное вторжение в компьютерные программы путем модификации или подделки;

j) незаконное копирование программ в нарушение прав интеллектуальной собственности;

k) кража и использование сетевых адресов;

l) изменение, дополнение или изъятие информации из передаваемого первоначального сообщения до его поступления адресату;

m) сознательное заражение вирусами и преступное изменение содержания сетевой информации;

n) фактическое (физическое) уничтожение оборудования и зданий.

5. Укрепить безопасность информационных систем можно следующими путями:

a) обучение персонала технике безопасности с разъяснением существующих опасностей и путей их предотвращения;

b) контроль за доступом; т.е. выдача различного рода разрешений лицам, имеющим санкционированный доступ к информации в конкретных категориях;

c) использование опознавательных цифровых кодов (цифровые подписи, цифровые подтверждения права доступа) для передаваемых сообщений между настоящими пользователями;

d) кодирование как аппаратных средств, так и программного обеспечения;

e) использование защитных систем для недопущения распространения информации, в которую были внесены несанкционированные изменения;

f) использование антивирусов.

6. Султанат надеется на разработку международных принципов, направленных на укрепление безопасности глобальных информационных систем, особенно с учетом введения Интернета в стране, которая тем самым оказалась подверженной рискам, связанным с обеспечением информационной безопасности.

КАТАР

[Подлинный текст на английском языке]
[10 июня 1999 года]

Компетентные органы Государства Катар представили следующую информацию о своей точке зрения и оценках в отношении пунктов 2 и 3 резолюции 53/70 Генеральной Ассамблеи от 4 декабря 1998 года:

a) Общая оценка проблем информационной безопасности. Общей оценке проблем информационной безопасности могут способствовать обмен техническими знаниями и понимание опасности несанкционированного вмешательства, а также его воздействия на вопросы безопасности и финансовые вопросы;

b) Определение основных понятий, относящихся к информационной безопасности. Основными понятиями, относящимися к обеспечению безопасности, являются те меры, которые необходимо соблюдать для обеспечения путей и средств обмена информацией, а также неожиданно возникающие проблемы, как наглядно показано в таблицах 1 и 2 ниже, в которых перечислены необходимые меры по обеспечению информационной безопасности на всех этапах наряду с возникающими в этой области новыми проблемами;

c) Принципы, которые были бы направлены на укрепление безопасности коммуникационных систем. Укрепления информационной безопасности можно добиться путем совершенствования средств передачи информации, и наиболее важными с точки зрения обеспечения безопасности коммуникационных систем, с учетом связанных с этим больших финансовых издержек, являются следующие моменты:

i) использование нестандартных протоколов линии передачи данных, которые можно разработать специально для обмена определенными видами информации;

ii) использование системы кодирования, которая должна быть разработана для данной конкретной цели и не должна предусматривать использования программ, производимых в промышленных масштабах;

iii) внесение изменений с разными временны́ми параметрами и кодами.

Таблица 1

Методы обеспечения безопасности компьютерных сетей

Меры по обеспечению безопасности

Угроза	Метод обеспечения безопасности	Функция
Незаконный перехват, прочтение или изменение данных	Шифрование (стандарт шифрования данных, DES, алгоритм цифровой подписи Райвеста-Шамира-Адлемана)	Кодирование данных в целях предотвращения их изменения
Лицо, имеющее право пользоваться сетью, получает несанкционированный доступ к данным	Применение программ, обеспечивающих контроль за доступом к данным	Эти программы четко определяют полномочия пользователей и контролируют осуществление этих полномочий
Пользователь преднамеренно неправильно идентифицирует себя в целях совершения мошеннических операций	Проверка права пользователя на доступ к данным	Методика, включающая применение шифровальных программ и идентификационных карт в целях установления права как отправителя, так и получателя на доступ к соответствующей информации
Не имеющий соответствующих полномочий пользователь одной из сетей получает доступ к другой сети	Применение аппаратных и программных средств сетевой защиты	Фильтруют определенные информационные потоки в целях предотвращения несанкционированного доступа к сети или серверу
Хакеры используют "дыры" в операционной системе сервера в целях получения доступа к данным и их изменения	Специальные средства операционной системы	Устраняют "дыры" в операционной системе

Таблица 2

Проблемы в области безопасности

Изменения	Проблемы
Современная сеть:	Безопасность системы находится под угрозой, поскольку:
Охватывает гораздо большее число портативных компьютеров	Портативные компьютеры легко украсть
Имеет больше беспроводных соединений	В беспроводные каналы связи можно легче проникнуть
Более обширна с географической точки зрения	Защиту удаленных узлов сложнее обеспечить
Связывает большее число разнообразных платформ	Пользователь забывает пароль или записывает несколько паролей
Все чаще бывает связанной с сетями общего пользования, такими, как Интернет	Хакеры "атакуют" сети общего пользования
Чаще использует компьютерные системы UNIX	Операционная система UNIX является особенно уязвимой

РОССИЙСКАЯ ФЕДЕРАЦИЯ

[Подлинный текст на русском языке]
[9 июня 1999 года]

Общие положения

1. Одна из характерных особенностей современного этапа мирового научно-технического прогресса связана с глобальной информационной революцией - стремительным развитием и повсеместным внедрением новейших информационных технологий и глобальных средств телекоммуникации. Проникая во все сферы жизнедеятельности государств, информационная революция расширяет возможности развития международного сотрудничества, формирует глобальное информационное пространство, в котором информация приобретает свойства ценнейшего элемента национального достояния, его стратегического ресурса.

2. Вместе с тем становится очевидным, что наряду с положительными моментами такого процесса создается и реальная угроза использования достижений в информационной сфере в целях, не совместимых с задачами поддержания мировой стабильности и безопасности, соблюдения принципов суверенного равенства государств, мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека.

3. Увеличение за счет новейших информационных технологий военного потенциала стран ведет к изменению глобального и регионального балансов сил, возникновению напряженности между традиционными и нарождающимися центрами силы и влияния.

4. Формируется принципиально новая сфера противоборства на международной арене, создается риск нового витка гонки вооружений на основе научно-технических достижений в области информатизации и связи. При этом затрагивается как сфера национальной безопасности отдельных государств, так и общая система международной коллективной безопасности на региональных и глобальном уровнях.

5. Речь идет о создании информационного оружия, применение которого с учетом уровня информатизации общества и уязвимости критически важных структур может иметь разрушительные последствия, сравнимые с воздействием оружия массового поражения. Очевидно, что таким оружием могут воспользоваться и террористические, экстремистские или криминальные группы, а также отдельные правонарушители.

6. Таким образом, универсальность, скрытность или обезличенность, возможность широкого трансграничного применения, экономичность и общая эффективность делают информационное оружие чрезвычайно опасным средством воздействия, причем разработка и применение такого оружия практически не регулируются нормами современного международного права.

7. В этой связи возникает очевидная потребность в международно-правовом регулировании мировых процессов гражданской и военной информатизации, разработке отвечающей интересам мировой безопасности согласованной международной платформы по проблеме информационной безопасности.

Предлагаемая модель действий

80. Основой дальнейших усилий международного сообщества в этом направлении может стать принятая консенсусом резолюция 53/70 Генеральной Ассамблеи от 4 декабря 1998 года

"Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности", проект которой был инициативно внесен Российской Федерацией.

90. В дальнейшем следует вести дело к принятию Генеральной Ассамблеей резолюций по проблеме информационной безопасности, конкретизированных в части ограничения угроз как террористического или криминального, так и военного характера.

10. Необходимо продолжать совместное рассмотрение ситуации в сфере информационной безопасности с целью выявления всех имеющихся позиций и взглядов и их учета в дальнейшем общем продвижении идеи.

11. По мере определения общих подходов и тенденций вести дело к разработке международных принципов (режима, кодекса поведения государств), направленных на укрепление международной информационной безопасности, которые могли бы быть первоначально сформулированы в виде многосторонней декларации, а в перспективе закреплены в форме многостороннего международно-правового документа. Проработку этих вопросов целесообразно вести также в рамках Женевской конференции по разоружению.

12. При этом следует исходить из необходимости рассмотрения и принятия международным сообществом упомянутых принципов в комплексе, т.е. с учетом угроз военного, террористического или криминального характера и применительно как к военным, так и к гражданским сферам.

Основные угрозы в сфере международной информационной безопасности

13. К числу основных угроз в сфере международной информационной безопасности относятся:

a) создание и использование средств воздействия и нанесения ущерба информационным ресурсам и системам другого государства;

b) целенаправленное информационное воздействие на критически важные структуры другого государства;

c) информационное воздействие с целью подрыва политической и социальной системы государства, психологическая обработка населения с целью дестабилизации общества;

d) действия государств, ведущие к их доминированию и контролю в информационном пространстве, противодействие доступу к новейшим информационным технологиям, создание условий технологической зависимости в сфере информатизации в ущерб другим государствам;

e) действия международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных правонарушителей, представляющие угрозу информационным ресурсам и критически важным структурам государств;

f) разработка и принятие государствами 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;

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

h) неконтролируемое трансграничное распространение информации, противоречащее принципам и нормам международного права, а также внутреннему законодательству конкретных стран;

i) манипулирование информационными потоками, дезинформация и сокрытие информации с целью искажения психологической и духовной среды общества, эрозии традиционных культурных, нравственных, этнических и эстетических ценностей;

j) информационная экспансия, приобретение монопольного контроля над национальными информационно-телекоммуникационными инфраструктурами другого государства, включая условия их функционирования в международном информационном пространстве.

Основные задачи и цели разработки режима международной информационной безопасности

14. Существует необходимость в формировании международно-правовой основы для:

a) определения признаков и классификации информационных войн;

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

c) ограничения оборота информационного оружия;

d) запрещения разработки, распространения и применения особо опасных видов информационного оружия;

e) предотвращения угрозы возникновения информационных войн;

f) запрещения использования информационных технологий и средств во враждебных целях и, в частности, против согласованных категорий объектов;

g) признания сравнимости применения информационного оружия в отношении критически важных структур с последствиями применения оружия массового поражения;

h) создания условий равноправного и безопасного международного информационного обмена на основе баланса интересов личности, общества и государства;

i) предотвращения угроз использования информационных технологий и средств в террористических и других преступных целях;

j) предотвращения угрозы использования информационных технологий и средств для воздействия на общественное сознание с целью дестабилизации общества и государства;

k) разработки процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия;

l) создания механизма разрешения конфликтных ситуаций в сфере информационной безопасности;

m) создания международной системы сертификации технологий и средств информатизации (в том числе программно-технических) в части гарантий их информационной безопасности;

n) развития системы международного взаимодействия правоохранительных органов по предотвращению преступлений в информационной сфере;

o) создания механизма контроля выполнения условий режима международной информационной безопасности;

p) гармонизации национальных законодательств в части обеспечения информационной безопасности.

Основные понятия, относящиеся к международной информационной безопасности

15. В число основных понятий, относящихся к международной информационной безопасности, входят:

a) информационное пространство - сфера деятельности, связанная с созданием, преобразованием и использованием информации, включая индивидуальное и общественное сознание, информационно-телекоммуникационную инфраструктуру и собственно информацию;

b) информационные ресурсы - информационная инфраструктура (технические средства и системы формирования, обработки, хранения и передачи информации), включая массивы и базы данных и собственно информацию и ее потоки;

c) информационная война - противоборство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным структурам, подрыва политической и социальной систем другого государства, а также массированной психологической обработки населения и дестабилизации общества;

d) информационное оружие - средства и методы, применяемые с целью нанесения ущерба информационным ресурсам, процессам и системам другого государства, негативного информационного воздействия на оборонные, управленческие, политические, социальные, экономические и другие критически важные системы, а также массированной психологической обработки населения с целью дестабилизации общества и государства;

e) 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;

f) угроза информационной безопасности - факторы, создающие опасность основным интересам личности, общества и государства в информационном пространстве;

g) международная информационная безопасность - состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве;

h) неправомерное использование информационно-телекоммуникационных систем и информационных ресурсов - использование телекоммуникационных и информационных систем и

ресурсов без соответствующих прав или с нарушением соответствующих правил, законодательства или норм международного права;

i) несанкционированное вмешательство в информационно-телекоммуникационные системы и информационные ресурсы - вмешательство в процессы сбора, обработки, накопления, хранения, поиска, распространения и использования информации с целью нарушения нормального функционирования информационных систем или нарушение целостности, конфиденциальности и доступности информационных ресурсов;

j) 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, системы 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);

k) международный информационный терроризм - использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в террористических целях;

l) международная информационная преступность - использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в противоправных целях.

САУДОВСКАЯ АРАВИЯ

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

Во всех государствах, которые все более широко используют электронные информационные системы, многие правительственные и частные учреждения добились прогресса в области информационной технологии. Тем не менее, по мере ускорения такого прогресса возрастает и число актов, направленных на нарушение функционирования таких информационных систем, их дестабилизацию и вмешательство в них, которые предпринимаются различными образованиями в преступных и террористических целях. Эта деятельность наносит ущерб экономике и обществу и подрывает безопасность. Весьма важное значение имеет внедрение международных принципов и норм, с тем чтобы противостоять угрозам информационной безопасности и попыткам нарушения такой безопасности, а также с тем чтобы бороться с такими международными актами и в уголовном порядке наказывать виновных в них. Соответствующие международные организации должны обеспечивать, чтобы те, кто повинен в совершении таких актов, представали перед правосудием и несли наказание.

СОЕДИНЕННОЕ КОРОЛЕВСТВО ВЕЛИКОБРИТАНИИ И СЕВЕРНОЙ ИРЛАНДИИ

[Подлинный текст на английском языке]
[30 мая 1999 года]

Общие положения

1. Связь между информационными системами во всем мире в настоящее время достигла такой степени, что многие, если не все, государства стоят перед лицом потенциальной опасности того, что жизненно важные элементы их инфраструктуры подвергнутся электронному нападению со стороны преступников и террористов. Хотя опасность такого электронного нападения, вероятно, в настоящее время невелика, она будет возрастать в будущем по мере того, как государственный и частный сектора будут все более широко использовать компьютерные системы, которые будут во все большей степени связаны друг с другом. Кроме того, поскольку такие системы связаны друг с другом в международном масштабе, данная угроза имеет трансграничный характер. Поэтому попытки преступников и террористов проникнуть в наши системы со злым умыслом представляют собой проблему для всех членов Организации Объединенных Наций. В связи с этим Соединенное Королевство Великобритании и Северной Ирландии приветствует шаги, направленные на изучение соответствующих средств борьбы, как на односторонней, так и на многосторонней основе, с помощью которых мы могли бы обеспечить неприкосновенность от таких нападений основанной на информационных системах жизненно важной инфраструктуры.

Меры на национальном уровне

2. В этих целях в январе 1999 года правительство Ее Величества объявило о шагах, призванных свести к минимуму опасность электронного нападения на чрезвычайно важную национальную инфраструктуру Соединенного Королевства. Меры на национальном уровне включают:

a) обеспечение идентификации в рамках правительства всех чрезвычайно важных систем, а также обеспечение эффективного управления деятельностью по защите таких систем и соответствующей проверки;

b) разработка в сотрудничестве с частным сектором мер, которые будут соответствовать уровню опасности, и обеспечение адекватных стандартов защиты ключевых систем, охватываемых жизненно важной национальной инфраструктурой;

c) повышение уровня информированности и стандартов в области информационной безопасности в частном секторе в целом путем дальнейшей реализации уже существующих инициатив, нацеленных на внедрение и применение наилучших практических методов в этой области.

Меры на международном уровне

3. В то же время тот факт, что связь между информационными системами носит трансграничный характер, означает, что нападения на системы в других государствах могут оказать негативное воздействие и на жизненно важную национальную инфраструктуру самого Соединенного Королевства и что террористы и преступники, действующие в той или иной третьей стране, могут попытаться напасть на системы в Соединенном Королевстве. Поэтому Соединенное Королевство признает важное значение международного сотрудничества в деле борьбы с угрозой преступного нападения и рассчитывает на расширение уже проводимых в настоящее время диалогов со своими международными партнерами по данным проблемам. Эта деятельность включает в себя работу Группы "большой восьмерки" по вопросам преступности в области высоких технологий, которая касается правовой взаимопомощи, а также работу, проводимую в Совете Европы в связи с разработкой конвенции о кибернетической преступности.

4. Соединенное Королевство полагает, что Организации Объединенных Наций следует следить за ходом работы в рамках этих и других форумов в целях определения в будущем тех видов мероприятий, касающихся вопросов существа, которые она могла бы с пользой осуществлять в этой области. В их число могли бы входить разработка международных принципов в целях укрепления безопасности глобальных систем и содействия борьбе с международным информационным терроризмом и преступностью.

СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ

[Подлинный текст на английском языке]
[20 мая 1999 года]

Общий обзор проблем в области информационной безопасности и определение основных понятий

1. Соединенные Штаты Америки полагают, что информационная безопасность представляет собой широкую и сложную тему, охватывающую многие факторы и затрагивающую многие разнообразные виды деятельности отдельных лиц, групп и правительств. Хотя эта общая тема включает в себя аспекты, которые связаны с международным миром и безопасностью (работа Первого комитета), она также охватывает технические аспекты, которые касаются глобальных коммуникационных систем, равно как и нетехнические вопросы, связанные с экономическим сотрудничеством и торговлей, правами интеллектуальной собственности, соблюдением законности, сотрудничеством в борьбе с терроризмом и другими проблемами, рассматриваемыми в рамках Второго или Шестого комитета. Меры и программы правительств ни в коей степени не являются единственными надлежащими инструментами, поскольку информационная безопасность также затрагивает важные проблемы, представляющие интерес для отдельных лиц, ассоциаций, предприятий и других организаций, действующих в частном секторе.

Аспекты, касающиеся международной безопасности

2. В периоды вооруженных конфликтов государства используют различные методы, связанные с информационной безопасностью. Двумя распространенными примерами являются создание радиопомех на определенных частотах и использование электромагнитных импульсов для борьбы с противником; такие методы далеко не новы. В будущем для вооруженных сил того или иного государства важное значение будет иметь защита их собственных сетей передачи данных и других основанных на применении компьютеров систем. Кроме этого, государствам-членам необходимо располагать потенциалом для восстановления ключевых информационных систем в тех случаях, когда стихийное бедствие или имеющая катастрофические последствия чрезвычайная ситуация выводит из строя ключевые объекты коммуникации или другие сети передачи данных в государственном и частном секторах. Информационная безопасность охватывает также защиту данных, связанных с военным потенциалом и другими аспектами национальной безопасности.

Экономические, торговые и технические факторы

3. Концепция информационной безопасности предполагает необходимость в защите результатов научных исследований коммерческого характера, а также производственных технологий и других видов конфиденциальных данных (например, планы маркетинга и информация служб, работающих с клиентурой).

4. Информационная безопасность связана также с необходимостью обеспечения соблюдения международных соглашений об интеллектуальной собственности (такой, как видео- и аудиоматериалы, а также компьютерное программное обеспечение), с тем чтобы защитить ее от несанкционированного копирования и продажи. Защита информации и данных частного характера представляет собой еще один аспект информационной безопасности и связана с обеспечением безопасности информации личного и коммерческого характера, передаваемой через общественные международные сети связи или частные системы передачи данных.

5. Что касается технических аспектов, то положения, применяемые Международным союзом электросвязи, и мероприятия аналогичных национальных учреждений обеспечивают совместимость электронных сигналов, надлежащее применение электромагнитного спектра и надежность международной сети связи в целом. Эти функции выполняют также и космические спутники, которые обеспечивают оказание широкого комплекса услуг, таких, как передача речевой корреспонденции и данных, а также данных локаторов и другой информации, используемой в авиации и мореплавании, а также при проведении исследований и спасательных операций. Кроме этого, соответствующие стандарты в области проектирования и безопасности обеспечивают чрезвычайно важные гарантии производителям и пользователям электронных устройств, включая компьютеры. Все эти регулятивные и административные функции можно ассоциировать с широкой концепцией информационной безопасности.

Обеспечение соблюдения законов и сотрудничество в борьбе с терроризмом

6. Широкомасштабное применение информационных технологий породило беспрецедентно высокий уровень глобальной взаимозависимости и взаимосвязи информационных систем, в результате чего многие аспекты национальной и международной деятельности, в рамках как государственного, так и частного секторов, теоретически могут оказаться под угрозой нападения со стороны преступников или террористов.

7. Хотя степень применения информационных технологий в разных государствах может быть различной, масштабы деятельности, которая связана с применением таких средств коммуникации (экономическая, торговая, промышленная, юридическая деятельность, а также деятельность в

области образования) позволяют предположить, что потенциально все государства могут столкнуться с последствиями деятельности различных преступников. Кроме этого, следует ожидать, что применение информационных технологий будет по-прежнему расширяться, поскольку эти технологии будут играть все более важную роль для стабильного функционирования правительств, а также для поддержания ключевых глобальных коммерческих и коммуникационных систем, обеспечивающих взаимодействие между государствами.

8. Поэтому Соединенные Штаты рассматривают потенциальную опасность использования преступниками информационных технологий как проблему, представляющую интерес для всех государств, и разделяют выраженное другими странами мнение о том, что нам необходимо в одностороннем и многостороннем порядке содействовать внедрению надлежащих мер для обеспечения неприкосновенности наших ресурсов, использование которых зависит от применения информационных технологий.

9. Соединенные Штаты также полагают, что любое незаконное вмешательство или попытка нарушить или изменить любой аспект их национальных информационных систем представляют собой потенциальную опасность для основных объектов их национальной инфраструктуры, а значит и угрозу их национальным интересам. Соединенные Штаты, признавая потенциальную серьезность такой угрозы, выступили инициаторами реализации на национальном уровне долгосрочных программ в государственном и частном секторах, которые рассчитаны на обеспечение защиты чрезвычайно важных объектов их национальной инфраструктуры. Тем не менее Соединенные Штаты признают также, что в контексте все большей глобальной взаимозависимости многих этих весьма важных инфраструктур успех их усилий на национальном уровне, предпринимаемых для защиты своих информационно-коммуникационных систем, в конечном счете будет отчасти зависеть от степени обеспечения безопасности тех находящихся за пределами Соединенных Штатов систем, с которыми они связаны.

10. Поэтому Соединенные Штаты полагают, что всем государствам следует принять на национальном уровне меры, необходимые как для обеспечения охраны их национальных информационных систем, так и для обеспечения того, чтобы преступники или международные террористы, действующие на их национальной территории, которые пытаются нарушить функционирование этих систем, карались за это по всей строгости закона. Каждое государство должно принять меры для того, чтобы его информационные системы были надежны и обеспечены как можно более надежными системами защиты на случай возможных попыток со стороны преступников использовать системы в своих целях или блокировать их работу, а также обеспечить быструю восстанавливаемость информационных систем в случае сбоев в их работе.

11. Уголовное право Соединенных Штатов запрещает вмешиваться в информационные инфраструктуры Соединенных Штатов Америки. Соединенные Штаты настоятельно призывают все государства провести обзор своих соответствующих национальных законов, с тем чтобы обеспечить включение в них надлежащих положений, касающихся преследования виновных в действиях, связанных с использованием информационных систем в преступных или террористических целях. Соединенные Штаты считают необходимым внесение на постоянной основе поправок в свои законы, касающиеся компьютерных сетей, с тем чтобы совершенствовать их и приводить их в соответствие с реалиями, порождаемыми новыми проблемами.

Целесообразность разработки международных принципов

12. Как указывалось выше, информационная безопасность представляет собой широкую и сложную тему. Она имеет много измерений, которые чрезвычайно сложно переплетены между собой. Учитывая несомненную необходимость в анализе всех аспектов информационной

безопасности и в достижении четкого понимания того, как эти аспекты взаимодействуют, было бы преждевременно приступать к разработке всеобъемлющих принципов, касающихся информационной безопасности во всех ее аспектах. Вместо этого международному сообществу следует проделать значительную работу с тем, чтобы на систематической основе осмыслить пройденный этап, прежде чем двигаться дальше. В целях содействия этому государствам-членам необходимо стремиться к ознакомлению с идеями и мнениями широкого круга экспертов в наших соответствующих правительствах и странах.

13. Тем не менее уже очевидно, что международное сотрудничество имеет важное значение в деле эффективного решения новых и сложных проблем, порождаемых информационным терроризмом и преступными элементами. В настоящее время проводится несколько многосторонних мероприятий, касающихся проблем международного сотрудничества. Совет Европы изучает проект конвенции о кибернетической преступности; Группа по вопросам преступности в области высоких технологий "большой восьмерки" изучает меры по оказанию взаимопомощи в правовой области, а также смежные проблемы, связанные с преступностью в области высоких технологий; Организация американских государств также учредила группу для изучения этих проблем; Азиатский и дальневосточный институт Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями изучает смежные вопросы в рамках Организации Объединенных Наций.

14. Все эти прилагаемые в настоящее время усилия заслуживают высокой оценки, и их, несомненно, необходимо и далее активизировать, с тем чтобы они могли принести свои плоды. Было бы весьма недальновидно, если бы Генеральная Ассамблея занялась разработкой стратегий или конкретных мероприятий, которые могли бы нанести ущерб уже проводимой международным сообществом соответствующей работе или стать ей помехой.
