Организация Объединенных Наций A/59/116

Генеральная Ассамблея

Distr.: General
23 June 2004
Russian
Original: Arabic/Chinese/English/
Spanish

Пятьдесят девятая сессия
Пункт 62 первоначального перечня*
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/59/50 и Corr.1.

04-40706 (R) 210704 230704

0440706

I. Введение

1. В пункте 3 своей резолюции 58/32 о достижениях 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) определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или противоправное использование информационных и телекоммуникационных систем и информационных ресурсов; и c) содержание соответствующих международных концепций, призванных повысить безопасность глобальных информационных и телекоммуникационных систем. В пункте 4 резолюции Ассамблеи содержится просьба к Генеральному секретарю рассмотреть существующие и потенциальные угрозы в сфере информационной безопасности и возможные совместные меры по их устранению, а также провести исследование с помощью группы назначенных им на основе справедливого географического распределения правительственных экспертов, которая должна быть создана в 2004 году, а также при содействии государств-членов, способных оказать такое содействие, и представить доклад о результатах данного исследования Генеральной Ассамблее на ее шестидесятой сессии. Группа правительственных экспертов по процессам в информационно-телекоммуникационной области в контексте международной безопасности приступила к работе в июле 2004 года.

2. В вербальной ноте от 18 февраля 2004 года ко всем государствам-членам была обращена просьба информировать Генерального секретаря об их точке зрения и оценках по этому вопросу. На данный момент получено семь ответов. Эти ответы приводятся в разделе II ниже. Дополнительные ответы будут изданы в качестве дополнений к настоящему докладу.

II. Ответы, полученные от государств-членов

Аргентина

[Подлинный текст на испанском языке]
[14 мая 2004 года]

Современное положение

1. Аргентинская Республика добилась существенного прогресса в сфере обеспечения безопасности и защиты данных. В законодательной области был принят Закон № 25326 о защите личных данных, который является одним из самых современных законов такого рода в мире, а контроль за его исполнением возложен на специально созданное с этой целью управление в министерстве юстиции. Кроме того, в конгрессе страны полным ходом идет рассмотрение ряда законопроектов о преступлениях в сфере информации.

2. Также удалось добиться прогресса в разработке законодательства, касающегося электронно-цифровой подписи, которое направлено на придание законного характера и обеспечение технической защищенности электронных документов в целях гарантирования их подлинности и целостности. Аргентина яв-

ляется пионером в этой области, и к настоящему времени принимаются последние меры для создания национальной инфраструктуры открытых ключей.

3. В частности, Аргентинское государство приняло важные шаги в сфере обеспечения информационной безопасности. В этой области Национальное управление информационных технологий (НУИД) несет главную ответственность за изучение, оказание помощи и осуществление контроля в вопросах, связанных с обеспечением безопасности и защиты цифровой и электронной информации государственного сектора страны.

4. В рамках этого Управления создан Координационный отдел по чрезвычайным ситуациям в телекоммуникационных сетях государственной администрации, который занимается инцидентами в сетях государственных учреждений и главная задача которого заключается в повышении уровня безопасности в государственном секторе. В этом контексте принимаются меры в отношении зафиксированных случаев нарушения безопасности, публикуются превентивные оповещения и принимаются меры для исправления имеющихся недостатков, разрабатываются специальные средства обеспечения безопасности, проводятся соответствующие курсы для сотрудников и должностных лиц государственного сектора и разрабатывается типовая политика по обеспечению безопасности государственных учреждений.

Общая оценка проблем

5. Обеспечение информационной безопасности сопряжено с рядом серьезных проблем, которые объясняются все более сложным вследствие технического прогресса характером задач, требующих решения.

6. Основные проблемы можно разделить на три категории:

Посягательства на целостность информации как таковой

Неправомерное использование информационных ресурсов

Преступления в сфере киберпространства.

7. Что касается информации, то появление новых технологий все более осложняет задачу обеспечения соблюдения трех основных предъявляемых к ней требований: конфиденциальность, целостность и доступность. В свою очередь в числе проблем, касающихся собственно информации, есть две основные категории, которые требуют особого отношения: личная информация, которая требует особо осторожного подхода в целях сохранения неприкосновенности частной жизни, и информация, касающаяся организаций, будь то коммерческие сведения, промышленная информация или данные об организациях, или же информация о государственных учреждениях, разглашение, изменение или утрата которой может нанести ущерб в экономической, социальной, политической и других областях.

8. Другая проблема, которой, как правило, не уделяется должного внимания, заключается в неправомерном использовании информационных ресурсов. Под неправомерным использованием следует понимать использование соответствующих ресурсов для иных целей, помимо санкционированных, или же неправомерным образом, влекущим за собой злоупотребление такой информацией, ее утрату или неправомерное использование. Например, массовое распространение вирусов и других программ проникновения через Интернет и принятие

соответствующих контрмер влечет за собой весьма существенные дополнительные расходы помимо обычных оперативных затрат. Принятие превентивных мер в этой области позволит сэкономить существенные средства и усилия.

9. И наконец, новые технологии порождают новые методы доступа в целях совершения противоправных деяний — как классических преступлений, совершаемых в настоящее время при поддержке новых технологий, так и новых преступлений, порожденных техническим прогрессом.

Китай

[Подлинный текст на китайском языке]
[24 мая 2004 года]

Точка зрения Китая по вопросам информационной безопасности

1. Бурное развитие информатики и телекоммуникаций является важной особенностью научно-технического прогресса. В новых условиях, когда многократно возросли угрозы безопасности, появились нетрадиционные факторы, затрагивающие безопасность, и возрастает грозная опасность международного терроризма, обеспечение информационной безопасности стало одной из серьезных задач в сфере международной безопасности. Китай поддерживает международные усилия, направленные на обеспечение и укрепление информационной безопасности всех стран, и создание Группы правительственных экспертов Организации Объединенных Наций для обсуждения и рассмотрения вопросов информационной безопасности.

2. Китай придерживается той точки зрения, что применение информационных технологий должно осуществляться в соответствии с Уставом Организации Объединенных Наций и другими международно согласованными принципами и способствовать поддержанию и укреплению международного и регионального мира, стабильности и развития. В условиях все более широкого распространения нетрадиционных угроз безопасности государствам следует уделять особое внимание преступности и терроризму в сфере информации. С учетом неодинакового уровня развития стран в сфере телекоммуникаций международному сообществу следует также укрепить сотрудничество в деле развития и применения информационных технологий.

3. Китай придерживается той точки зрения, что в рамках Группы правительственных экспертов Организации Объединенных Наций по вопросам информационной безопасности всем сторонам следует изучить существующие и потенциальные угрозы в сфере информационной безопасности и рассмотреть конкретные пути и средства борьбы с ними. Китай будет принимать деятельное и конструктивное участие в работе Группы правительственных экспертов Организации Объединенных Наций и выражает надежду, что это принесет позитивные результаты.

Коста-Рика

[Подлинный текст на испанском языке]
[15 марта 2004 года]

1. Правительство Коста-Рики хотело бы сообщить, что 24 октября 2001 года законодательное собрание Коста-Рики приняло дополнения к Уголовному кодексу, озаглавленные «Включение в Уголовный кодекс, Закон № 4573, статей 196 бис, 217 бис и 229 бис о пресечении и наказании преступлений в сфере информации». Указанные дополнения являются самым значительным за последние годы достижением в сфере обеспечения информационной безопасности в Коста-Рике.

2. Эти дополнения предусматривают классификацию трех видов преступлений в сфере информации (перехват электронных сообщений, мошенничество в сфере информации и изменение данных и подрывная деятельность в сфере информации), что является важным достижением для Коста-Рики в этой области и отвечает существующим требованиям для обеспечения информационной безопасности.

Ниже приводится текст указанных дополнений (см. приложение).

Приложение

Включение в Уголовный кодекс, Закон № 4573, статей 196 бис, 217 бис и 229 бис о пресечении и наказании преступлений в сфере информации

8148

Законодательное собрание Республики Коста-Рики постановляет: включение в Уголовный кодекс, Закон № 4573, статей 196 бис, 217 бис и 229 бис о пресечении и наказании преступлений в сфере информации

Единственная статья — включить в Уголовный кодекс, Закон № 4573 от 4 мая 1970 года, статьи 196 бис, 217 бис и 229 бис следующего содержания:

Статья 196 бис — перехват электронных сообщений

Наказывается тюремным заключением на срок от шести месяцев до двух лет тот, кто в целях раскрытия тайны или нарушения неприкосновенности личной жизни другого лица, без его согласия осуществляет присвоение, доступ, модификацию, изменение, сокрытие, перехват, вмешательство, использование, распространение или пересылку не по назначению сообщений, данных и изображений, содержащихся на электронных, информационных, магнитных и сетевых носителях. Наказание составляет тюремное заключение на срок от одного до трех лет, если действия, описанные в предыдущем пункте, осуществляются лицами, отвечающими за сохранность электронных, информационных, магнитных и сетевых носителей.

Статья 217 бис — мошенничество в сфере информации

Наказывается тюремным заключением на срок от одного до десяти лет тот, кто с намерением приобрести или получить в собственное пользование или в интересах третьего лица включает в процессе обработки или на этапе получения результатов данных в вычислительной системе программными средствами подложные или неполные данные, совершает неправомерное использование данных или любые другие действия, влияющие на процесс обработки данных в системе.

Статья 229 бис — изменение данных и подрывная деятельность в сфере информации

Наказывается тюремным заключением на срок от одного до четырех лет тот, кто любым способом без разрешения осуществляет доступ, стирание, уничтожение, изменение или приведение в негодность данных, содержащихся в компьютере.

Если в результате указанных действий нарушается функционирование или приводится в негодность компьютерная программа, база данных или информационная система, то наказание составляет от трех до шести лет тюремного заключения. Если такая компьютерная программа, база данных или информационная система содержит данные государственного характера, то наказание составляет тюремное заключение на срок до восьми лет.

Куба

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

Точка зрения Республики Куба в соответствии с положениями пункта 3 резолюции 58/32, озаглавленной «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности»

1. В подпунктах (a) и (b) пункта 3 резолюции 58/32 от 8 декабря 2003 года, касающейся достижений 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) определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство и противоправное использование информационных и телекоммуникационных систем и информационных ресурсов; и c) содержание соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем.

2. Куба считает, что использование телекоммуникаций с враждебными намерениями с явной или скрытой целью изменить правовую и политическую систему государств является нарушением международно признанных норм в этой области и негативным и безответственным использованием этих средств, последствия которого могут повлечь за собой возникновение напряженных ситуаций, ставящих под угрозу международный мир и безопасность, что является прямым нарушением целей и принципов Устава Организации Объединенных Наций.

3. В восьмом пункте преамбулы резолюции 58/32 вновь подтверждена озабоченность Генеральной Ассамблеи тем, что «эти технологии и средства потенциально могут быть использованы в целях, не совместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на целостность инфраструктуры государств, нарушая их безопасность применительно как к гражданской, так и к военной сферам». Куба полностью разделяет эту озабоченность.

4. Информационно-телекоммуникационные системы могут стать оружием, если они разрабатываются и/или применяются с целью нанесения ущерба инфраструктуре какого-либо государства.

5. Куба вновь заявляет, что все государства обязаны уважать существующие международные нормы в этой сфере. Доступ к информационным или телекоммуникационным системам другого государства должен осуществляться с соблюдением международных соглашений о сотрудничестве на базе принципа согласия соответствующего государства. Формы и масштабы обмена должны определяться на основе уважения законодательства того государства, к системе которого открывается доступ.

6. Международному миру и безопасности может быть нанесен ущерб в результате агрессии со стороны того или иного государства против информаци-

онных или телекоммуникационных систем других государств. К сожалению, эти методы уже практикуются в качестве инструмента враждебной политики.

7. Куба на протяжении почти 20 лет является объектом такой агрессии, осуществляемой при содействии и с согласия правительства Соединенных Штатов. Начиная с 1985 и 1990 годов, когда американское правительство незаконно создало станции радио- и телевещания, соответственно, нормальная работа кубинского радио и телевидения была нарушена в результате создаваемых помех и вмешательства.

8. Еженедельно из Соединенных Штатов на Кубу транслируются радио- и телевизионные программы объемом 2227,5 часов, которые направлены на подрыв нашего конституционного строя. Только для этих целей выделено 29 частот, на которых работают 18 станций вещания в диапазоне СВ, КВ, ЧМ и телевещания.

9. В целом на этих частотах ежесуточно осуществляется трансляция объемом 312–315 часов, которая представляет собой передачи, содержащие политические измышления, которые не имеют ничего общего со свободным обменом информацией и идеями, поскольку их материалы содержат вымышленные измышления, сфабрикованные путем обмана, лжи и искажения действительности, а также сведения, направленные на подрыв конституционного порядка страны.

10. Из 18 станций, которые принимают участие в радиоэлектронной и телевизионной агрессии против Кубы, 15 принадлежат организациям, которые поддерживают связи или принадлежат известным террористам, проживающим, функционирующим и действующим на американской территории при полной осведомленности и согласии федеральных властей Соединенных Штатов.

11. Из этих станций 12 работают исключительно против Кубы. Из них самой печально известной является телевидение и радио Марти. Они принадлежат правительству Соединенных Штатов, которое ежегодно выделяет 35 млн. долл. США на эту радиоэлектронную войну против Кубы.

12. В мае 2004 года правительство Соединенных Штатов выступило с новой опасной провокацией, объявив, что оно будет использовать воздушную платформу самолета управления ЕС-130 и выделит дополнительные средства для приобретения и модернизации воздушной платформы, используемой для вещания на Кубу так называемого радио и телевидения Марти.

13. Эти незаконные трансляции на Кубу содержат искаженные сведения о действительном положении в нашей стране, способствуют незаконной эмиграции, которая происходит в опасных условиях, подстрекают к неподчинению и гражданскому неповиновению, насилию и активизации террористических действий, а также подрыву институционального устройства и правопорядка, созданного в соответствии с Конституцией Республики Куба, получившей поддержку свыше 96 процентов граждан.

14. Применение информации с явной целью подрыва внутреннего строя государств, нанесения ущерба суверенитету и оказания влияния и осуществления актов вмешательства в их внутренние дела является незаконным в соответствии с международным правом и представляет собой нарушение права народов на самоопределение.

15. Эти передачи являются не только нарушением суверенитета Кубы, но и представляют собой вопиющее нарушение норм, установленных Международным комитетом регистрации частот Международного союза электросвязи, в частности правила 23.3 его Регламента радиосвязи, в котором запрещается вести телевизионные передачи за пределами национальных границ, и таким образом являются нарушением международного права.

16. Эти телевизионные передачи также являются нарушением положений преамбулы Устава Международного союза электросвязи, поскольку они представляют собой деятельность, которая не способствует обеспечению мирных связей, международному сотрудничеству и экономическому и социальному развитию народов с помощью эффективно действующей электросвязи.

17. Куба считает необходимым вновь обратить внимание на следующие аспекты, которые имеют непосредственное отношение к использованию в полном объеме телекоммуникаций в качестве инструмента укрепления международного мира и безопасности:

a) все государства обязаны воздерживаться от применения односторонних мер принудительного характера, противоречащих международному праву, которые ограничивают доступ затрагиваемого государства к технологиям и международным информационно-коммуникационным сетям;

b) системы сертификации и возможные санкции в отношении какого-либо государства в вопросах доступа к телекоммуникационным технологиям или иным, тесно связанным с ними технологиям с точки зрения угрозы международному миру и безопасности, должны быть многосторонними по своему характеру и разрабатываться на основе моделей, согласованных международным сообществом;

c) необходимо укрепить международное сотрудничество в этой области, задействовав все необходимые ресурсы для оказания помощи развивающимся странам в укреплении и расширении их телекоммуникационных систем;

d) необходимо в срочном порядке принять законодательные и иные меры как на национальном, так и на международном уровнях, чтобы не допустить неоправданной концентрации в руках частных лиц собственности и средств контроля над средствами телекоммуникаций, а также других средств информации и связи, поскольку они препятствуют необходимой диверсификации источников информации и могут быть использованы в качестве средства подрыва мира и подстрекательства к войне;

e) необходимо создать многостороннюю, межправительственную, демократическую и прозрачную систему управления и контроля за Интернетом и другими международными сетями информации и коммуникаций. Важнейшее значение имеет межправительственный характер такой системы контроля;

f) системы контроля и наблюдения за средствами телекоммуникаций и другими формами международной связи должны быть многосторонними и прозрачными по своему характеру и предусматривать четко установленную ответственность и процедуры общественного контроля, чтобы положить конец нарушениям суверенитета и безопасности многих государств и даже вмешательству в частную жизнь граждан со стороны глобальных систем шпионажа,

созданных некоторыми промышленно развитыми странами, в частности Соединенными Штатами;

g) необходимо обеспечить эффективные гарантии уважения культурного многообразия и ликвидации всех форм дискриминации или пропаганды ненависти в информационных материалах, распространяемых в рамках телекоммуникационных систем на международном уровне.

Грузия

[Подлинный текст на английском языке]
[18 мая 2004 года]

Изменения в информационно-телекоммукационной области в Грузии в контексте международной безопасности

1. Нынешняя ситуация в области информационной безопасности в телекоммуникационных системах Грузии

1.1. В настоящее время система информационной безопасности Грузии находится на этапе разработки.

1.2. В разработке концепции национальной системы информационной безопасности принимают участие министерство инфраструктуры и развития Грузии и Национальная комиссия Грузии по связи (НКГС).

1.3. Этой работой занимается инициативная группа, не имеющая адресного финансирования.

2. Ход работы

В состав инициативной рабочей группы входят следующие члены:

- министерство инфраструктуры и развития Грузии — департамент политики в сфере телекоммуникаций и информационных технологий;
- Национальная комиссия Грузии по связи (НКГС) — технический департамент.

3. Основные принципы политики национальной системы информационной безопасности Грузии заключаются в следующем:

3.1. Общие положения концепции информационной безопасности определяются Программой информатизации Грузии. Эта программа находится на этапе разработки.

3.2. Стратегия информационной безопасности для корпоративных, правительственных и общественных информационных систем и надлежащая инфраструктура телекоммуникаций основываются на стандартах национальной системы информационной безопасности.

3.3. Система стандартов информационной безопасности Грузии основывается на согласованных международных стандартах Международной организации по стандартизации (ИСО), Международного союза электросвязи (МСЭ) и Европейского института по стандартам телекоммуникаций (ЕИТС).

3.4. На корпоративном уровне политика информационной безопасности осуществляется на основании методологических рекомендаций и норм в сочетании с добровольной сертификацией в соответствии со стандартом ISO 17799.

4. Участие Грузии в глобальном информационном сообществе должно обеспечивать следующие возможности:

4.1. Создание единого информационного пространства и инфраструктур с участием Грузии в международных процессах, включая разработку международной системы информационной безопасности.

4.2. Глобализация защитных функций на основе международных информационных стандартов, согласующихся с участием Грузии во Всемирной торговой организации (ВТО), Организации Объединенных Наций и других международных сообществах.

4.3. Вхождение в глобальную постиндустриальную экономику на основе принципов сотрудничества и информационную доступность в целях преодоления информационного разрыва между Грузией и международным сообществом.

4.4. Повышение информационной безопасности Грузии.

5. Основные задачи министерства инфраструктуры и развития Грузии в сфере информационной безопасности

5.1. Определение недостатков телекоммуникационных стандартов, мониторинг и изучение результатов деятельности международных организаций по стандартизации, систем сертификации качества, экологической и информационной безопасности.

5.2. Координация международных и местных программ и стратегии развития коммуникаций с требованиями международных организаций, а также сотрудничество с международными инициативами и региональными проектами безопасности.

6. Укрепление национальной информационной безопасности Грузии

6.1. Для успешной реализации информационной программы и системы информационной безопасности необходимы адресное финансирование и международная поддержка.

6.2. Помощь международных организаций считается важной в решении следующих задач:

- исследований в сфере телекоммуникационной инфраструктуры и ее перевода на сети нового поколения;
- анализ условий и сопоставимости системы стандартов национальной информационной безопасности;
- разработка программ и методов обеспечения информационной безопасности различного уровня для экономической и социальной деятельности.

7. Сотрудничество с международными организациями:

- МСЭ и Региональное коммуникационное сообщество;
- Организация Объединенных Наций; и
- Экономическая и социальная комиссия для Азии и Тихого океана, Конференция Организации Объединенных Наций по торговле и развитию и Всемирная торговая организация.

8. Проекты, семинары и другие мероприятия

8.1. МСЭ — проект системы защиты от несанкционированного доступа для министерства инфраструктуры и развития Грузии.

Организаторы: БРЭ, МСЭ, «Утимако», правительство Болгарии, Департамент телекоммуникации и информационных технологий.

8.2. Учебные практикумы по вопросам развития инфраструктуры финансирования торговли Грузии:

- проблемы создания корпоративной системы при поддержке новых информационно-коммуникационных технологий;
- электронная торговля, разработка ИКТ и финансирование торговли, разработка системы финансирования электронной торговли, электронной банковской системы и системы электронных платежей;
- обсуждение проблем, включая развитие национальной торгово-финансовой инфраструктуры.

Ливан

[Подлинный текст на арабском языке]
[27 мая 2004 года]

В связи с развитием и применением информационных технологий и средств коммуникации Ливан обеспокоен тем, что они могут быть использованы для целей, не совместимых с интересами международной стабильности и безопасности, и считает необходимым воспрепятствовать применению таких информационных технологий и средств коммуникации в преступных и террористических целях. Он будет принимать соответствующие меры и сотрудничать в осуществлении резолюций Организации Объединенных Наций, направленных на защиту безопасности и конфиденциальности информации и предупреждение ее неправомерного использования любыми способами.

Соединенное Королевство Великобритании и Северной Ирландии

[Подлинный текст на английском языке]
[14 мая 2004 года]

1. Соединенное Королевство приветствует участие сообщества Организации Объединенных Наций в рассмотрении последствий нашей растущей зависимости от информационно-коммуникационных систем, включая нашу уязвимость от связанных с этим угроз. Информационная безопасность имеет важнейшее значение для развития глобальной экономики, что получило признание в принципах и плане действий, принятых на Всемирной встрече на высшем уровне по вопросам информационного общества по окончании его первого этапа.

2. Принятые принципы предусматривают «создание глобальной культуры кибербезопасности, развитие и внедрение которой должны осуществляться на основе сотрудничества со всеми участниками и международными органами экспертов» и для этой цели «осуществляться в условиях более широкого международного сотрудничества». Соединенное Королевство твердо убеждено в том, что наилучшим путем достижения целей государств в области безопасности является укрепление глобальной культуры кибербезопасности, как это указано в принципах Всемирной встречи на высшем уровне и принципах по защите важнейших информационных инфраструктур Группы 8, а также принципах, определенных в резолюции 58/199 Генеральной Ассамблеи.

3. Соединенное Королевство не считает, что в данном случае необходим многосторонний инструмент, который будет ограничивать развитие или использование некоторых гражданских и/или военных технологий. Что касается военного применения информационных технологий, то в таком инструменте нет необходимости. Законы и обычаи войны, в частности принципы необходимости и пропорциональности, регулируют применение таких технологий. Кроме того, такой подход может воспрепятствовать свободе информационных потоков, которая в ходе ВСИС получила признание в качестве одного из ключевых принципов информационного общества.

Основные положения и концепции

4. Мы должны понимать, что опасность для сетей и информационных систем является следствием угрозы и уязвимости. Эта опасность постоянно меняется, однако ясно, что за последние годы ее формула усложнилась. Государственные субъекты представляют собой лишь незначительную часть угрозы для информационных систем. В последние годы бóльшие опасения вызывает деятельность террористов, организованных преступников и «хакеров», которые пытаются получить неправомерный доступ к системам и нанести ущерб функционированию сетей. В целях укрепления глобальной кибербезопасности нам необходимо обеспечить, чтобы нападения на информационные системы и сети пресекались уголовным правом. Наилучшей моделью для уголовного преследования преступности в киберпространстве является Конвенция Совета Европы о киберпреступности.

5. Вместе с тем анализ угрозы является лишь одним из аспектов кибербезопасности. Соединенное Королевство считает, что защита сетей и информаци-

онных систем в значительной мере зависит от источника угрозы. Таким образом, для устранения факторов уязвимости необходимо задействовать международное сотрудничество. Факторы уязвимости могут носить технический характер (программное обеспечение или используемые протоколы), но также и обуславливаться ошибками пользователей, когда они, поддаваясь обману и попадаясь на уловки «хакеров», разглашают информацию, касающуюся безопасности. Изменение киберкультуры, то есть путей разработки, развертывания и применения сетей и информационных систем, является нашей главной задачей. В «Руководстве по безопасности информационных систем и сетей — к культуре безопасности», разработанном Организацией экономического сотрудничества (ОЭСР), содержатся прочные основы для инициирования таких культурных изменений.

Осуществление соответствующих концепций: подход Соединенного Королевства

6. В 2003 году Соединенное Королевство приняло национальную стратегию информационной безопасности, в которой рассматриваются вопросы защиты важнейших информационных систем и защищенность сетей. Основное внимание в ней уделяется защите государственных информационных массивов и систем, однако также признается важность сотрудничества с частным сектором и четко указывается на значение элемента информационно-пропагандистской работы как с предпринимательскими кругами, так и с отдельными гражданами. В ней также признается важность партнерства с другими странами в деле повышения безопасности киберпространства.

7. В правительстве были созданы новые структуры для осуществления этой стратегии при активном участии министерств внутренних дел, промышленности и обороны с назначением ответственных координационных центров в каждом министерстве. В поддержку этой стратегии также принимаются меры для укрепления технического потенциала государственных экспертов по прогнозированию и устранению проблем в области информационной безопасности. В этой стратегии также признается важность информационно-разъяснительной работы и новаторского подхода, а в июне 2004 года планируется опубликовать крупное исследование по долгосрочным подходам к вопросам кибербезопасности.

8. Стратегия Соединенного Королевства предусматривает три ключевые инициативы. В 1999 году Соединенное Королевство создало Национальный координационный центр по вопросам безопасности инфраструктуры, который представляет собой межведомственную инициативу и в настоящее время пользуется хорошей международной репутацией в вопросах защиты важнейших инфраструктур. Центр способствует информационному обмену между заинтересованными сообществами, выступает в качестве координатора для оперативного оповещения о возможных опасностях на базе международных контактов и играет ведущую роль в деле выявления и исправления уязвимых мест в используемых протоколах.

9. Соединенное Королевство также сыграло роль в разработке стандартов в области управления информационной безопасностью, включая руководящие принципы в отношении управления информационной безопасностью (ISO/IEC 17799), которые первоначально являлись стандартом, принятым в Ве-

ликобритании, а в настоящее время получают все более широкое признание в качестве важнейшего стандарта в этой области. Такие стандарты предусматривают подход к обеспечению информационной безопасности на основе оценки факторов уязвимости или риска, что позволяет организациям уделять основное внимание вопросам управления информационной безопасностью.

10. Для борьбы с преступностью в киберпространстве Соединенное Королевство разрабатывает соответствующую стратегию, которая основывается на Конвенции Совета Европы и законодательстве Европейского союза. Кроме того, в Соединенном Королевстве правоохранительные органы изменили свою деятельность с учетом меняющегося характера киберпреступности путем создания национального органа — Национальной группы по борьбе с преступностью в сфере современных технологий, а также специальных подразделений в местных органах полиции.

Осуществление соответствующих концепций: потенциал для международного сотрудничества

11. В ходе Всемирной встречи на высшем уровне по вопросам информационного общества была подчеркнута важность международного сотрудничества в деле максимального укрепления потенциала информационного сообщества. Резолюция 58/32 Генеральной Ассамблеи обеспечивает возможность для создания культуры кибербезопасности, которая будет обеспечивать защиту интересов правительств, предпринимательских кругов и отдельных граждан благодаря сведению к минимуму риска нарушения работы систем и защите свободного обмена информацией. В Руководящих принципах ОЭСР содержится модель передовых принципов, которые могут способствовать укреплению такой культуры и должны лежать в основе нашего подхода к кибербезопасности.

12. Соединенное Королевство приветствует тот факт, что сообщество Организации Объединенных Наций занялось вопросом информационной безопасности, и считает, что Организация Объединенных Наций может способствовать созданию культуры кибербезопасности путем уделения особого внимания следующим вопросам:

- изучение наиболее рациональной практики и обмен соответствующей информацией;
- разработка типового подхода к пресечению преступности в киберпространстве на базе Конвенции Совета Европы;
- укрепление оперативного сотрудничества между национальными органами в деле выявления опасностей и факторов уязвимости и проведение расследований и наказание виновных;
- разработка более согласованного подхода к устранению факторов уязвимости в информационных системах.