Организация Объединенных Наций A/62/98

Генеральная Ассамблея

Distr.: General
2 July 2007
Russian
Original: Arabic/Chinese/English/
French/Spanish

Шестьдесят вторая сессия
Пункт 95 предварительного 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/62/150.

07-40784 (R) 250707 250707

I. Введение

1. В пункте 3 своей резолюции 61/54 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) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области; c) содержание соответствующих международных концепций, направленных 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 2007 года государствам-членам была направлена вербальная нота, в которой им предлагалось сообщить Генеральному секретарю свои мнения и оценки по этому вопросу. Полученные ответы приводятся в разделе II ниже. Дополнительные полученные ответы будут изданы в качестве добавлений к настоящему докладу.

II. Ответы, полученные от правительств

Бруней-Даруссалам

[Подлинный текст на английском языке]
[25 июня 2007 года]

Бруней-Даруссалам представил следующий доклад Королевской брунейской полиции.

I. Введение

(Общая оценка вопросов информационной безопасности)

1. Информационные технологии, охватывающие все сферы развития в области информатики и телекоммуникаций, играют важную и ключевую роль во всех слоях общества. Информационные технологии меняют наш подход к накоплению, сбору, обработке, управлению и обмену информацией. Электронные операции и отчетность занимают важнейшее и центральное место во всех сферах деятельности — от торговли до здравоохранения. В основе таких преобразований лежит создание вычислительных сетей. Экспонентный рост Интернета и увеличение числа его пользователей каждый год являются примером такого перехода к сетевому обществу.

2. В результате этого информационная безопасность стала одним из важнейших компонентов информационных технологий, особенно в контексте информационного общества. Вместе с тем, это сложный вопрос, и принятие надлежащих мер часто в значительной мере зависит от вида и местонахождения аппаратных средств ИТ и соответствующей инфраструктуры.

3. Процесс создания вычислительных сетей лежит в основе многих преобразований такого рода, а они в свою очередь порождают новые опасения в сфере безопасности и защиты сетевой информации. Если не удастся изыскать надлежащего решения этих проблем, то они могут стать препятствием на пути всестороннего развития сетевого потенциала как с точки зрения количества пользователей, так и с точки зрения полезности этих сетей. Таким образом, необходимы надлежащие организационные и технические гарантии безопасности широкого спектра личной, охраняемой авторским правом, секретной или проприетарной информации.

4. Необходимо тщательно проанализировать потенциальные угрозы и проблемы в сфере безопасности в каждой конкретной ситуации, и крайне важно, чтобы все заинтересованные стороны понимали касающиеся их и подконтрольные им угрозы и факторы риска. Лишь в этом случае они смогут полностью осознать и применять надлежащие процедуры обеспечения безопасности.

5. Основное внимание в таком случае следует уделять обеспечению безопасности открытой сетевой информации, безопасности и защите сетей и надежности сетевых услуг обеспечения доступа к информации.

6. В этой связи существуют три важнейшие области: a) политика в сфере криптографии, включая стандарты и меры контроля, касающиеся обработки информации государственных органов; b) руководящие принципы обеспечения безопасности открытой информации в государственных учреждениях; и c) правовые вопросы и вопросы информационной безопасности, включая электронную торговлю, неприкосновенность информации и интеллектуальную собственность.

7. Методы обеспечения информационной безопасности, в частности основывающиеся на криптографии, приобретают все большее значение. Надлежащие меры защиты (контрмеры) должны предусматривать и предвосхищать технические, организационные и социальные преобразования, которые все чаще влекут за собой перенос ответственности за обеспечение безопасности информации на конечных пользователей. Более широкие усилия по обеспечению безопасности сетевой информации увенчаются успехом лишь в том случае, если будут решены вопросы политики в сфере криптографии. Наиболее важный шаг в деле внедрения надлежащих мер защиты сетевой информации в том или ином государственном учреждении или какой-либо организации заключается в том, чтобы высшее руководство определило общие цели организации, разработало организационную политику обеспечения безопасности, которая бы отражала эти цели, и приступила к осуществлению этой политики. Лишь высшее руководство может добиться консенсуса и выделить необходимые ресурсы для обеспечения эффективной защиты сетевой информации.

8. В настоящем документе предпринята попытка дать оценку угрозам и факторам риска, связанным с преступной деятельностью в ИТ-среде, а также указывается, какие рекомендации полиция могла бы вынести в отношении процедур обеспечения безопасности и методов предупреждения компьютерной преступности. Угрозы информационным системам могут возникать в результате преднамеренных и непреднамеренных действий и могут проистекать как из внутренних, так и из внешних источников.

II. Опасения

9. Королевская брунейская полиция обеспокоена тем, что вопросам обеспечения безопасности в контексте национального развития в рамках инициатив по созданию электронного правительства не уделяется достаточного внимания.

10. Пока Королевской брунейской полиции не предлагалось принять участие в осуществляемой в стране подготовительной деятельности по переходу к информационной эпохе. За последние три года было разработано множество законодательных актов для подготовки страны к вступлению в информационную эпоху. При этом было создано множество правительственных и регулятивных органов, которые возглавят инициативы по образованию электронного правительства.

11. Вопросам обеспечения безопасности с точки зрения подготовки правоохранительных органов не уделялось столь же активное или приоритетное внимание, как другим пунктам национальной повестки дня. Королевская брунейская полиция считает, что обеспечение безопасности играет важнейшую роль в национальных стремлениях по вступлению в информационное общество.

12. Обеспечение безопасности в информационную эпоху играет важнейшую роль. Нельзя переоценить значение безопасной и надежной инфраструктуры.

III. Инициативы Королевской брунейской полиции

(Принятые на национальном уровне меры по укреплению информационной безопасности и содействию международному сотрудничеству в этой сфере)

13. Королевская брунейская полиция является ведущим правоохранительным органом в стране и стремится оказать помощь в деле руководства деятельностью по обеспечению безопасности в информационную эпоху.

14. С этой целью многие сотрудники были командированы за рубеж для изучения преступности, затрагивающей Интернет, в частности преступлений в киберпространстве и транснациональных преступлений. На первоначальном этапе в связи с нехваткой средств не удалось добиться дальнейших успехов в деле закупки необходимых аппаратно-программных комплексов ИТ для расследования случаев проникновения в вычислительные системы. В настоящее время Королевская брунейская полиция обладает необходимым потенциалом для возбуждения расследований преступлений в киберпространстве.

15. Королевская брунейская полиция приняла меры для содействия развитию международного сотрудничества в этой сфере путем активного участия в различных форумах, занимающихся вопросами укрепления потенциала правоохранительных органов. Она имеет доступ к региональным и международным вычислительным системам правоохранительных органов, что способствует укреплению ее потенциала в деле поиска скрывающихся от правосудия преступников.

IV. Предложения и рекомендации Королевской брунейской полиции

(Возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне)

16. Королевская брунейская полиция предлагает следующие вопросы в качестве отправной точки для обсуждения тем, связанных с укреплением и совершенствованием безопасности в контексте информационного общества.

A) Представление сообщений и контроль за угрозами и факторами уязвимости:

после создания в 2004 году Брунейской группы быстрого реагирования на угрозы безопасности вычислительных систем был налажен определенный контроль. Вместе с тем такой контроль не является всеобъемлющим, поскольку эта группа никоим образом не связана с Королевской брунейской полицией, и в настоящее время не существует механизма оперативного реагирования, то есть контроля за непосредственными попытками проникновения или их перехвата и т.д.

B) Подготовка кадров и механизмы обеспечения безопасности вычислительных систем:

1) оказание поддержки в разработке учебных материалов и программ для всех пользователей киберпространства. Это позволит обеспечить обучение безопасной практике и поведению при использовании Интернета на раннем этапе;

2) вложение средств в проведение информационно-разъяснительных кампаний, в ходе которых основное внимание уделялось бы необходимости обеспечения подготовки по вопросам безопасности для системных администраторов, сетевых администраторов и старших информационных сотрудников;

3) содействие разработке и внедрению механизмов обеспечения безопасности информации в киберпространстве, механизмов, которые позволяли бы любой стороне информационной операции определять, какие меры предосторожности и ограничения они хотят применять.

C) Научно-исследовательские и опытно-конструкторские работы:

1) выделение средств для НИОКР в сферах обеспечения безопасности и безотказности систем с распределенной архитектурой и контролем;

2) разработка всеобъемлющего инструментария в поддержку деятельности сетевых администраторов по защите систем;

3) разработка методов для осуществления программ всеобъемлющего и постоянного выявления факторов риска и смягчения последствий.

D) Применение стандартов:

1) разработка и содействие внедрению стандартов защиты программного обеспечения в качестве одного из способов непосредственного стимулирования процесса повышения безопасности программного обеспечения Интернета;

2) разработка государственной политики, в соответствии с которой аппаратно-программные комплексы, установленные в государственных учреждениях, должны удовлетворять определенному ряду стандартов в области безопасности, предусматривающих оповещение пользователей о факторах уязвимости и появлении исправлений.

E) Законы и правоохранительная деятельность:

1) оказание поддержки полицейским, занимающимся борьбой с преступностью в киберпространстве, выделение надлежащих средств правоохранительным органам для поддержки подготовки кадров, обеспечение физических и кадровых ресурсов, необходимых для борьбы с киберпреступностью;

2) обеспечение учета в национальной политике потребностей правоохранительных органов в области международной координации в деле борьбы с преступлениями в киберпространстве и оказание поддержки правоохранительным органам в разработке международных соглашений, касающихся преследования «по горячим следам»;

3) обеспечение поддержки в рамках государственной политики широкого применения криптографии для защиты информации и пользователей киберпространства.

Буркина-Фасо

[Подлинный текст на французском языке]
[20 июня 2007 года]

1. Буркина-Фасо давно проявляла свое политическое стремление к развитию новых информационно-коммуникационных технологий, которые рассматриваются ею как стратегическое средство укрепления благого управления и экономического и социального развития.

2. С 1996 года она сосредоточила свои усилия на всестороннем изучении вопроса развития информационно-коммуникационных технологий. Цель заключалась в том, чтобы использовать информационные технологии в интересах общественных служб и повысить эффективность работы администрации.

3. В 1999 году в стране был разработан план создания информационно-коммуникационной инфраструктуры на 2001–2005 годы, направленный на содействие согласованию национальной политики в области телекоммуникаций, информатики и средств коммуникации.

4. В 2004 году правительство Буркина-Фасо приняло стратегию по реализации плана развития национальной информационно-коммуникационной инфраструктуры. Тем самым правительство брало на себя обязательство гарантировать распространение информационно-коммуникационных технологий во всем обществе, обеспечивать их доступность и их использование всеми слоями населения и мобилизацию их потенциала в интересах осуществления национальных стратегий развития.

5. Однако, учитывая риски, связанные с использованием информационных систем, правительство стремится разработать юридические рамки, направлен-

ные на защиту информации, обеспечение безопасности информационной системы, защиту основополагающих прав лиц, обеспечение доверия со стороны компаний и административных органов.

6. В ходе этого процесса был принят закон № 010-2004/AN от 20 апреля 2004 года о защите данных личного характера. Этот закон охраняет права и основные свободы лиц и их частную жизнь в процессе компьютерной и некомпьютерной обработки информации, содержащей данные личного характера. Во исполнение этого закона декретом 2007-283/PRES/PM/MPDH от 18 мая 2007 года была создана комиссия по вопросам информатики и свобод. Этой комиссии, имеющей независимые административные полномочия, поручено следить за тем, чтобы автоматизированная обработка информации личного характера в государственном и частном секторах осуществлялась в соответствии с законом. Будучи исполнительным органом, уполномоченным применять санкции, эта комиссия имеет право вмешиваться как на начальных, так и на последующих этапах обработки информации, путем представления предварительных мнений или заявлений и осуществления контроля и применения санкций.

7. Наконец, для удовлетворения потребностей в безопасности информационного общества были созданы органы по регулированию. В их число входят Высший совет по информации, Главное управление, на которое возложена координация программ развития информационно-коммуникационных технологий на уровне министерства почт и информационно-коммуникационных технологий.

8. Тем не менее, учитывая, что информационное общество не имеет границ, Буркина-Фасо считает крайне важным поддержание международного сотрудничества в вопросах обеспечения безопасности информационных систем. Несмотря на наличие «цифрового разрыва», страны Юга в области безопасности подвержены тем же угрозам, что и страны Севера. В этой связи сотрудничество между странами необходимо для обеспечения безопасности государств, учреждений, предприятий и отдельных лиц, а также информационных сетей и систем. Борьба с киберпреступностью может быть эффективной лишь при условии укрепления международного сотрудничества.

9. Буркина-Фасо приветствует интерес, который Организация Объединенных Наций проявляет к вопросу информационной безопасности, и считает, что сейчас сложились благоприятные условия для разработки международного документа по вопросам информационной безопасности, с одной стороны, и вопросам защиты данных личного характера, с другой стороны. В любом случае прогресс в области информатики, телеинформатики и вопросы международной безопасности должны рассматриваться сквозь призму прав человека, с тем чтобы избежать скатывания к глобальному обществу контроля, в котором доминирует рефлекс отказа от человечности во имя безопасности.

Чили

[Подлинный текст на испанском языке]
[13 июня 2007 года]

1. Чили придает большое значение информационной безопасности в контексте международной безопасности. Мы разделяем обеспокоенность междуна-

родной общественности по поводу того, что информационные технологии могут использоваться в целях, несовместимых с задачей поддержания международной стабильности и безопасности, и могут поставить под угрозу государственную инфраструктуру. Мы считаем необходимым воспрепятствовать применению информационных технологий в преступных целях.

2. В законодательной сфере были приняты меры для принятия новых законодательных и нормативных документов по вопросам обеспечения безопасности и конфиденциальности электронных документов, а также эффективности средств связи между органами государственного управления и между такими органами и гражданами.

3. Учитывая большое значение, придаваемое этому вопросу, наша страна приняла активное участие в работе обоих этапов Всемирной встречи на высшем уровне по вопросам информационного общества, которые состоялись в Женеве в декабре 2003 года и в Тунисе в ноябре 2005 года.

Китай

[Подлинный текст на китайском языке]
[15 мая 2007 года]

1. В наши дни быстрое развитие и широкое применение информационной технологии играют позитивную роль в содействии экономическому и социальному развитию и в улучшении жизни населения во всем мире. В то же время информационная безопасность стала важным фактором, влияющим на общую безопасность страны и даже на безопасность и стабильность во всем мире. Надлежащее решение этого вопроса служит общим интересам всех стран, и на международном сообществе лежит коллективная ответственность за такое решение.

2. По мнению Китая, проблема информационной безопасности включает в себя не только риски, связанные с уязвимостью и взаимозависимостью информационной инфраструктуры, но и различные политические, экономические, военные, социальные, культурные и многие другие проблемы, вызываемые злоупотреблением информационной технологией. Все эти вышеупомянутые факторы должны быть проанализированы при рассмотрении вопроса об информационной безопасности.

3. Китай считает, что использование информационной технологии должно осуществляться в соответствии с Уставом Организации Объединенных Наций и основополагающими нормами, регулирующими международные отношения. Свободный поток информации необходимо обеспечивать при условии сохранения суверенитета и безопасности каждой страны, уважения соответствующих законов каждой страны и ее исторических, культурных и политических различий. Все страны должны пользоваться своим правом регулировать свое собственное кибернетическое пространство. Учитывая несбалансированное развитие сектора телекоммуникаций в различных странах, международное сообщество должно расширять сотрудничество в области научных исследований и использования информационной технологии для обеспечения всем странам доступа к этой технологии.

4. Правительство Китая всегда придавало большое значение вопросу информационной безопасности. Оно разработало и постепенно осуществляет свою национальную стратегию в области информационной безопасности. Оно подготовило ряд законов и стандартов в области регулирования информационной безопасности и предприняло усилия по расширению контроля за случаями нарушений информационной безопасности, совершенствованию механизмов координации и управления, проведению исследований по вопросам технологий обеспечения информационной безопасности и созданию системы реагирования на угрозы безопасности информационных сетей, которая внесла важный вклад в процесс постоянного улучшения безопасности сетевой инфраструктуры Китая и основных информационных систем.

5. Китай активно участвует в международном сотрудничестве в области информационной безопасности. В июне 2006 года государства — члены Шанхайской организации сотрудничества приняли Заявление по международной информационной безопасности, в котором главы государств приняли решение создать группу экспертов государств-членов по международной информационной безопасности. Китай принял конструктивное участие в работе группы экспертов.

6. Китай считает, что Организация Объединенных Наций является надлежащим форумом для изучения путей решения проблемы информационной безопасности. С 2004 по 2005 год Группа правительственных экспертов Организации Объединенных Наций по информационной безопасности обсуждала этот вопрос во всех его аспектах и выдвинула ряд ценных предложений, которые заложили хорошую основу для дальнейшего обсуждения этой проблемы. Китай поддерживает повторное формирование группы правительственных экспертов Организации Объединенных Наций в 2009 году для проведения углубленного и всестороннего исследования угроз и проблем в области информационной безопасности во всех ее аспектах и поиска эффективных решений. Китай будет продолжать поддерживать и активно участвовать в международных усилиях, направленных на решение проблемы информационной безопасности.

Куба

[Подлинный текст на испанском языке]
[16 мая 2007 года]

1. В основе достигнутых Кубой результатов в сфере информационно-коммуникационных технологий на данный момент лежат исключительно социальные факторы, которые обусловили полный отказ от любых проявлений потребительского подхода и создали условия для подготовки специалистов нового типа, которые преданы своему делу и отвергают этические ценности, существующие в глобализованном и неолиберальном мире.

2. Значительное совершенствование технической инфраструктуры, а также существование широкомасштабной и глубокой программы подготовки кадров с самого раннего возраста являются примерами крупномасштабных усилий кубинского государства по ускоренной информатизации общества в качестве одного из путей повышения качества жизни, эффективности и конкурентоспособности страны.

3. На основе этой политики Куба обеспечивает рациональное и эффективное использование информационных ресурсов, как аппаратных комплексов, так и средств подключения, на самой широкой социальной основе. Таким образом, основное внимание уделяется таким ключевым секторам, как здравоохранение, просвещение, научные центры, культурные учреждения и предприятия, которые способствуют экономическому и социальному развитию страны.

4. Вместе с тем, препятствием на пути такого развития является жестокая и продолжительная экономическая, торговая и финансовая блокада, введенная Соединенными Штатами Америки, нынешняя администрация которых активизировала свои действия в этом направлении.

5. Подключение Кубы к Интернету произошло в 1996 году, когда правительство Соединенных Штатов предоставило ей соответствующую лицензию. Вместе с тем, в настоящее время, невзирая на то, что в непосредственной близости от кубинских берегов проходят международные оптико-волоконные линии, законы блокады препятствуют подключению к ним, в результате чего наша страна вынуждена пользоваться спутниковым каналом, который обеспечивает всего лишь 65 Мбит/с на выходе и 124 Мбит/с на входе. Подключение к оптико-волоконным линиям не только обеспечит бóльшую скорость, но и позволит существенно сократить расходы. Указанными законами предусматривается, что для любых новых подключений или изменения каналов требуется лицензия казначейства Соединенных Штатов.

6. Что касается технической инфраструктуры, то введенная Соединенными Штатами блокада в отношении Кубы не только не дает нам возможности приобретать у американских компаний аппаратные комплексы и программное обеспечение, но и вследствие своего экстерриториального характера наносит ущерб нашим коммерческим отношениям с предприятиями других государств, а также предусматривает заблокирование перегрузки программного обеспечения и информации, даже бесплатных, если номер IP имеет отношение к Кубе.

7. Интернет в качестве единой глобальной арены, безусловно, связан с определенными проблемами, причем они касаются не только вопросов управления им всем человечеством и соответственно привлечения всех стран к управлению Интернетом, но также искоренения таких получивших всемирное осуждение проблем, как распространение порнографии, подстрекательство к терроризму, расизм, мошенничество, пропаганда фашистских идеологий и любых проявлений преступности в киберпространстве.

8. Еще одна существенная проблема, которую замалчивают богатые страны, заключается в искоренении его избирательного и элитного характера, который сегодня привносит существующее в реальном мире неравенство и ограничения в киберпространстве, что влечет за собой возникновение так называемой «цифровой пропасти».

9. В мире существуют миллионы людей, которые весьма далеки от Интернета, поскольку они до сих пор не умеют ни читать, ни писать, а их главной повседневной задачей является борьба с голодом, нехваткой воды и заболеваниями. При наличии политической воли правительств, организации международного сотрудничества и выделении минимального объема тех средств, которые так называемые развитые страны в настоящее время тратят на рекламу, чрезмерное потребление и гонку вооружений, Интернет мог бы стать средством

проведения революции в сфере культуры и образования, которая способствовала бы распространению знаний в поддержку образования, культуры, сотрудничества, солидарности, а также этических и моральных ценностей, необходимых в этом столетии, что способствовало бы укреплению самых благородных устремлений человека и отказу от жестокости, эгоизма и индивидуализма.

10. С другой стороны, органы безопасности уделяют особое внимание этому вопросу и в большинстве своем используются в качестве пособников правительства. Благодаря получению огромных средств они разработали различные способы и программы развития существующих технологий или создания новых возможностей перехвата сообщений, доступа к системам и базам данных, системам, содержащим информацию об автотранспортных средствах и людях и позволяющим осуществлять контроль за ними. Эти сложные сети включают антенные системы, станции прослушивания, радары и спутники, которые действуют при поддержке шпионских подводных лодок и самолетов, имеющих доступ к суперкомпьютерам и специальному программному обеспечению.

11. Было бы весьма наивно считать, что компании, занимающиеся оказанием услуг и предоставлением технологий, в рамках их сотрудничества с указанными выше учреждениями не предоставляют информацию, которая помогает этим учреждениям в их шпионской и разведывательной деятельности. Не следует забывать о том, что согласно положениям так называемого закона «Пейтриот» Соединенных Штатов, правительство этой страны уполномочено требовать секретную или любую иную информацию от любой компании, если считается, что она может представлять интерес по соображениям национальной безопасности.

12. Исходя из того, что знания являются достоянием всего человечества, необходимо обеспечить демократизацию наличия и распределения информационного капитала, который необходимо поставить на службу мира и развития, поскольку это имеет важнейшее значение для дальнейшего развития в условиях нового тысячелетия.

Ливан

От Постоянного представительства Ливана при Организации Объединенных Наций были получены следующие письма, представляющие собой обмен сообщениями между Постоянным представительством и министерствами телекоммуникаций, внутренних дел и обороны.

[Подлинный текст на английском языке]
[4 июня 2007 года]

1. Мы сейчас в процессе принятия закона о секторе информационно-коммуникационных технологий Ливана, который находится на последнем этапе утверждения в палате депутатов. Этот закон будет охватывать вопросы безопасности и все вопросы, связанные с информационными преступлениями.

2. После вступления в силу вышеупомянутого закона министерство телекоммуникаций займется рассмотрением вопросов (b), (c) и (d) совместно с другими министерствами и компетентными ведомствами.

Министерство внутренних дел

[Подлинный текст на арабском языке]
[23 мая 2007 года]

1. В национальном плане

Обмен информацией между различными подразделениями служб безопасности осуществляется с помощью различных средств телекоммуникации (телефон, факсимильная связь и оперативные центры в различных районах). Эти средства продолжают быть объектами нарушений, таких, как перехват сообщений или прослушивание телефонных разговоров при том, что Главное управление на протяжении определенного времени занимается расширением сети «ТЕТРА», которая использовалась силами безопасности в отдельных районах Ливана и в настоящее время распространяется на всю страну. Кроме того, силы безопасности недавно были обеспечены сетью закрытой мобильной телефонной связи в соответствии с решением № 47 Совета министров от 15 сентября 2006 года.

2. В международном плане

Обмен информацией, в том числе по вопросам безопасности, между силами безопасности и различными международными органами осуществляется с помощью Отдела международной связи при Главном управлении сил безопасности, который располагает аппаратурой для передачи и получения кодируемых данных при посредничестве Отделения Интерпола в Бейруте. В настоящее время в нем используется система регулярных сообщений, действующая на основе Интернета и характеризующаяся большой скоростью распространения информации и ее конфиденциальностью, обеспечиваемой благодаря специальным сетям, функционирующим при содействии Международной организации уголовной полиции (Интерпол), на которую возложен контроль за управлением этой системой и ее совершенствованием.

- Что касается общих проблем информационной безопасности, то силы безопасности стремятся использовать эффективные технические средства в области безопасности информационных и телекоммуникационных систем. В этой области существует множество проблем, наиболее важной из которых является проблема упорядочения структуры безопасности и систем защиты данных на основе приемлемых и надлежащих критериев с целью организации, обеспечения и укрепления управления информационными системами в области безопасности и контроля за этими системами.

- Что касается вопросов (b) и (c), касающихся усилий, предпринимаемых на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области, то нами был приобретен конкретный и реальный опыт в области оценки рисков проникновения в зависимости от состояния информационной сети, которой мы располагаем. Мы добились успехов в повышении безопасности нашей сети данных на основе применения новых методов и найденных решений и конкретных мер в сфере защиты систем, оценки их устойчивости от попыток проникновения и вирусов, принятии планов, позволяющих продолжать работу в случае проникновения в системы и подготовке

компетентных сотрудников, готовых принять меры при любом возникновении угрозы.

- Что касается вопроса (d), касающегося возможных мер, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне, то мы предлагаем прежде всего разработать превентивную политику, направленную на недопущение индивидуальных посягательств, и сотрудничать на международном уровне в этой области; разработать закон о борьбе с актами саботажа и проникновения в информационные сети и предусмотреть уголовную ответственность за совершение таких актов; обмениваться накопленным государствами опытом и использовать этот опыт для достижения качественных результатов в этой области.

В этой связи следует уточнить, что Главное управление приняло с этой целью следующие меры:

a) Оно создало в рамках сил безопасности отдел по борьбе с киберпреступностью, в основные задачи которого входит, в частности, оповещение о преступлениях в информационной сфере и об угрозах безопасности цифровых данных, проведение расследований и преследование виновных в совершении таких преступлений.

b) Силы безопасности приняли участие (в лице нескольких офицеров-специалистов) в работе по разработке проекта закона о борьбе с киберпреступностью в сотрудничестве с парламентской комиссией по вопросам технологии. Проект закона ожидает утверждения парламентом.

c) Силы безопасности участвуют в деятельности Международной организации уголовной полиции (Интерпол) и оказывают помощь в работе регионального комитета Интерпола для Ближнего Востока и Северной Африки, отвечающего за борьбу с киберпреступностью. Заместитель председателя и один из членов этого комитета являются офицерами сил безопасности, специализирующимися на вопросах информатики. Кроме того, начальник отдела по борьбе с киберпреступностью обеспечивает связь с Интерполом по вопросам информационной безопасности и борьбы с киберпреступностью, в частности в тех случаях, когда она затрагивает сферу информационной безопасности. С учетом опасностей, которые угрожают — в национальном и международном планах — безопасности в целом и безопасности информационных и коммуникационных систем в частности, необходимо разработать перспективную стратегию, которая бы учитывала технический прогресс в целях защиты информации и поиска средств борьбы с любыми нарушениями. В этой связи следует отметить следующее:

1. Динамика распространения информации и критерии безопасности

Благодаря техническому прогрессу значительными темпами изменяются средства передачи и сохранения данных, однако трудности контроля за системами, инструментами и содержанием вызвали необходимость применения мер защиты на всех уровнях. Для управления информационной безопасностью были разработаны международные нормы (ISO17799).

2. Ливан и информационная безопасность

Ливану недостает множества средств в законодательной и исполнительной сфере для обеспечения информационной защиты. В стране отсутствуют какие-либо законы или административные процедуры, обязывающие государственные органы и учреждения применять международные нормы (ISO17799). Отдельные инструкции, схожие с международными нормами, применяются Центральным банком и несколькими частными банками. В стране также отсутствует законодательство, касающееся основополагающих принципов кодирования в частных коммуникационных сетях.

3. Вопрос применения

Не соблюдается циркуляр № 4/2 министерства телекоммуникаций от 19 декабря 2005 года, касающийся хранения документов, связанных с распространением данных. Нет никакого законодательства, регламентирующего работу Интернет-кафе, контроль за спутниковой связью осуществляется неэффективно.

В этой связи следует отметить, что Соединенные Штаты Америки после имевших место 11 сентября террористических нападений создали министерство национальной безопасности и утвердили систему контроля за сетями по всей стране, которая позволяет анализировать информацию и осуществлять контроль. Они также разработали строгие законы, касающиеся кодирования данных, а также входа в сети и выхода из них.

3. Средства борьбы и предупреждения

Как выяснилось, будучи сетью, регулируемой протоколом контроля передачи сообщений/протоколом Интернет, кибернетическое пространство является уязвимой и ненадежной сферой, на которую покушались и которую иногда выводили из строя преступные группы по причине того, что приоритетное внимание уделялось целям продажи и коммерциализации. Кроме того, киберпреступность характеризуется быстрой скоростью распространения и отсутствием контроля и ограничений, в то время как борьба с ней осуществляется медленным темпами, координация отсутствует, а принятые законы являются недостаточными.

Были внесены многочисленные улучшения в функционирование протоколов Интернет как в отношении пользователей, так и в отношении кодирования (в частности протокол IPv6) и проводятся серьезные исследования по выработке методов обеспечения безопасности информационных сетей, позволяющих бороться с проникновением в них и их уничтожением.

В международных соглашениях о борьбе с киберпреступностью, в частности в Будапештской конвенции, предусмотрены активизация сотрудничества между государствами, а также следующие меры:

– создание постоянно действующей коммуникационной сети, работающей параллельно с сетью Интернет и специализирующейся на киберпреступности;

– создание постоянного комитета и региональных рабочих групп для стимулирования технического сотрудничества и повышения уровня профессиональной подготовки в отделах по борьбе с киберпреступностью.

Тем не менее эта Конвенция, как представляется, не смогла обеспечить оперативную и непосредственную борьбу с вирусами, запускаемыми в сеть.

4. Предложения

- Применять и совершенствовать законодательство, касающееся информационной безопасности, и применять нормы в области обеспечения информационной безопасности;
- начать осуществление и совершенствование мер безопасности в различных компетентных службах в целях защиты информационных средств и систем;
- обеспечить функционирование специализированных служб в рамках министерства телекоммуникаций и установить связь между ними и государственными и частными службами и учреждениями в целях поиска надежных условий для работы информационных систем;
- следить за достигнутыми в мире успехами в плане, в частности, применения протоколов Интернет, таких, как IPv6, и использовать необходимые технические средства для идентификации любого лица, проникающего в сеть Интернет, и выработать систему цифровой идентификации (цифровое удостоверение);
- укрепить координацию деятельности правоохранительных служб в области информационной безопасности, выработать единые международные технические нормы для содействия применению последующих мер, осуществления контроля и координации и, насколько это возможно, привести в соответствие законодательные системы для обеспечения национальной безопасности при одновременном соблюдении требований международной безопасности.

Главное управление общественной безопасности указывает, что его сообщения по вопросам безопасности распространяются внутри страны и не направляются за ее пределы. Что касается внутренних сообщений, то при содействии специалистов отдельных дружественных служб безопасности в настоящее время совершенствуются системы защиты. Тем не менее из-за отсутствия финансовых и технических средств пока еще не было поставлено необходимое оборудование.

Министерство обороны

[Подлинный текст на арабском языке]
[1 мая 2007 года]

Министерство обороны сообщает следующее:

– Ливан обязуется не использовать информационно-коммуникационные технологии в целях, которые не совместимы с понятиями международной стабильности и безопасности;

– Ливан принимает необходимые меры на национальном уровне (совершенствование и модернизация соответствующих систем и законов) для укрепления информационной безопасности и призывает к обмену имеющимися данными между заинтересованными сторонами;

– Ливан соблюдает резолюции Организации Объединенных Наций, направленные на обеспечение безопасности и конфиденциальности информации и недопущение любого ее неправомерного использования и на запрет использования информационных источников или технологий в преступных или террористических целях.

Мексика

[Подлинный текст на испанском языке]
[22 мая 2007 года]

1. Мексика выступила в поддержку резолюции о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности, представленной Российской Федерацией в Генеральное Ассамблее Организации Объединенных Наций, и считает крайне важным способствовать более широкому обмену мнениями по этому вопросу и связанным с ним аспектам. Она считает, что можно было бы задействовать Первый комитет и другие форумы по разоружению для одновременного представления документов от экспертов и обсуждения этого вопроса.

2. Большей частью механизмы международной проверки, созданные в соответствии с международно-правовыми документами или политическими соглашениями по контролю за экспортом, используют для целей своего эффективного функционирования информационно-телекоммуникационные технологии, и именно в этой области необходимо прежде всего изучить положение вещей. С другой стороны, развитие ракетных баллистических систем и модернизация ядерных арсеналов предполагают развитие информационно-телекоммуникационных технологий, которые необходимо учитывать. Помимо этого, развитие технологий освоения космического пространства и спутниковых технологий, безусловно, имеет отношение к вопросам международной безопасности.

3. Мексика постоянно отмечала в рамках Конференции по разоружению необходимость принятия в безотлагательном порядке программы работы, одним из центральных пунктов которой стал бы вопрос о «предупреждении гонки вооружений в космическом пространстве», который, по ее мнению, связан с уязвимостью информационно-коммуникационных средств, размещаемых в космическом пространстве.

4. Мексика считает необходимым продолжить работу Группы правительственных экспертов по этой теме, которая была создана в соответствии с резолюцией 58/32 и мандат которой будет возобновлен в 2009 году. В этой связи она считает, что не следует отказываться от дальнейшего широкого обсуждения этого вопроса.