Организация Объединенных Наций A/64/129/Add.1

Генеральная Ассамблея

Distr.: General
9 September 2009
Russian
Original: French/Spanish

Шестьдесят четвертая сессия
Пункт 91 предварительной повестки дня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Добавление**

Содержание

* A/64/150 и Corr.1.

** Информация, содержащаяся в настоящем документе, была получена после представления основного доклада.

09-50577 (R) 180909 240909

II. Ответы, полученные от правительств

Куба

[Подлинный текст на испанском языке]
[2 июля 2009 года]

Позиция в отношении резолюции 63/37 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»

1. Куба полностью разделяет выраженную в резолюции 63/37 озабоченность тем, что информационные технологии и средства 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. Кроме того, в резолюции вполне правомерно подчеркивается необходимость предотвратить использование информационных ресурсов или технологий в преступных или террористических целях.

2. Куба подтверждает, что злонамеренное использование телекоммуникаций с открытой или тайной целью подрыва юридического и политического строя государств является нарушением международно признанных норм в этой области и ненадлежащей и безответственной формой применения этих средств, которая может повлечь за собой напряженность и неблагоприятные последствия для международного мира и безопасности и нанести ущерб принципам и целям, провозглашенным в Уставе Организации Объединенных Наций.

3. Куба с обеспокоенностью обращает внимание на то, что информационные и телекоммуникационные системы могут быть превращены в оружие, если они будут разрабатываться и/или применяться с целью причинить ущерб инфраструктуре государств, и, как следствие, могут поставить под угрозу международный мир и безопасность.

4. В этой связи Республика Куба считает необходимым вновь заявить, как она уже это делала на различных международных форумах, о своем осуждении агрессивной эскалации радио- и телевизионной войны против Кубы, которую вели и продолжают вести правящие верхушки Соединенных Штатов, открыто нарушая международные нормы, регулирующие использование сектора радиочастот.

5. Правящие верхушки Соединенных Штатов не возместили того ущерба, который они могли нанести международному миру и безопасности, создавая опасные ситуации, в том числе путем использования военного самолета для трансляции телевизионных сигналов на Кубу без ее согласия. Куба считает такое поведение неподобающим для постоянного члена Совета Безопасности Организации Объединенных Наций.

6. Радиоэлектронная агрессия против Кубы с территории Соединенных Штатов идет вразрез с принципами международного права, регулирующими отношения между государствами, и нормами и правилами Международного союза электросвязи, в которых определены принципы поведения стран-членов

этого специализированного учреждения системы Организации Объединенных Наций.

7. В конце мая 2009 года общая продолжительность незаконного еженедельного вещания с территории Соединенных Штатов на Кубу на 30 частотах составляла 1924 часа. Некоторые из используемых для этого радиостанций принадлежат либо оказывают свои услуги организациям, связанным с известными террористическими элементами, проживающими и действующими против Кубы на американской территории. Они занимаются трансляцией программ, в которых содержатся призывы к подрывным действиям, покушениям на политических деятелей, убийству главы государства и другие призывы, характерные для радиотерроризма.

8. Эти провокационные передачи, направленные против Кубы, вступают в противоречие со следующими международными нормами:

- Основополагающие принципы Международного союза электросвязи, сформулированные в преамбуле к его уставу, о возрастающем значении электросвязи для сохранения мира, экономического и социального развития всех государств с целью обеспечения мирных связей, международного сотрудничества и экономического и социального развития народов с помощью эффективно действующей электросвязи. Телевизионные программы, транслируемые правительством Соединенных Штатов на Кубу, носят подрывной и дестабилизирующий характер и искажают реальное положение дел, вступая в противоречие с указанными принципами.

- Положения 197 и 198 устава Международного союза электросвязи, в которых говорится, что все станции, независимо от их назначения, должны устанавливаться и эксплуатироваться таким образом, чтобы не причинять вредных помех радиосвязи или радиослужбам других членов Союза.

- Соглашение, подписанное на девятой пленарной сессии Всемирной конференции радиосвязи (ВКР) в ноябре 2007 года, в пункте 6.1(g) которого говорится, что «никакая радиопередающая станция, функционирующая на борту воздушного судна и транслирующая передачи исключительно на территорию другого государства без согласия последнего, не может считаться функционирующей в соответствии с Регламентом радиосвязи».

- Пункт 8.3 статьи 8 Регламента радиосвязи Международного союза электросвязи, в котором говорится, что частоты, которые были присвоены и выделены с ведома международного сообщества, должны приниматься во внимание другими администрациями при осуществлении собственных частотных присвоений во избежание вредных помех.

- Пункт 42.4 статьи 2 Регламента радиосвязи Международного союза электросвязи, в котором радиостанциям на борту воздушных судов, находящихся в море или над морем, запрещается осуществлять какое бы то ни было радиовещание.

- Решение Радиорегламентарного комитета, который на своем 35-м собрании в декабре 2004 года констатировал факт вредных помех, которые эти передачи создавали для кубинских радиослужб на частоте 213 МГц, и потребовал, чтобы администрация Соединенных Штатов Америки приняла необходимые меры для их прекращения. Кроме того, Ра-

диорегламентарный комитет с сентября 2006 года обращается к администрации Соединенных Штатов Америки с призывами принять меры для устранения помех на частоте 509 МГц, но никакой реакции на эти призывы до сих пор не последовало. 20 марта 2009 года состоялось 50-е собрание Комитета, и в резюме решений (документ RRB09-1/5) он вновь заявил о незаконности этого вещания и просил администрацию Соединенных Штатов Америки принять все необходимые меры с целью прекратить создание двух вышеупомянутых помех телевизионным службам Кубы.

- Пункт 23.3 статьи 23 Регламента радиосвязи Международного союза электросвязи, в котором налагаются ограничения на телевещание за пределами национальных территорий. В докладе, опубликованном в январе 2009 года Главным контрольным управлением правительства Соединенных Штатов (официальным американским ведомством), признаются нарушения международных норм и норм внутреннего законодательства, допущенные в программе радио- и телевещания американского правительства на Кубу.

9. Куба напоминает также о том, что на сессии Всемирной конференции радиосвязи (ВКР-07), которая состоялась в Женеве, Швейцария, 22 октября — 16 ноября 2007 года, был принят текст заключений, в котором были признаны не соответствующими Регламенту радиосвязи трансляции, ведущиеся с воздушных судов Соединенных Штатов на Кубу. В заключениях, утвержденных на пленарном заседании, говорилось буквально следующее: «Радиопередающая станция, которая функционирует на борту воздушного судна и транслирует передачи исключительно на территорию другого государства без согласия последнего, не может считаться соответствующей Регламенту радиосвязи». Эти заключения были приняты на пленарном заседании ВКР-07 и имеют юридическую силу для деятельности Международного союза электросвязи. Таким образом Всемирная конференция радиосвязи подтвердила решение, принятое в 1990 году тогдашним Международным комитетом регистрации частот, согласно которому трансляция с борта аэростата телевизионных программ на национальную кубинскую территорию противоречит действующим правилам.

10. Враждебная позиция правительства Соединенных Штатов Америки по отношению к Кубе выражается в сохранении на протяжении уже почти 50 лет экономической, торговой и финансовой блокады, которая затрагивает и сферу информации и телекоммуникаций, о чем свидетельствуют, в частности, следующие примеры:

- Кубе недоступны услуги, предоставляемые большим количеством вебсайтов, и причиной отказа является установление того, что запрос имел место с Интернет-адреса, относящегося к кубинскому домену .cu.

- На основании недавнего решения Управления по контролю за иностранными активами (ОФАК) без предварительного уведомления были заблокированы доменные имена .com, связанные с Кубой.

- Весьма показательно, сделанное в мае 2009 года технологическим консорциумом «Майкрософт» публичное заявление о приостановлении чат-сервиса “Windows Live Messenger IM” в отношении Кубы и других стран «в силу обязанности соблюдать американское законодательство». При со-

единении с этим сервисом появляется надпись: «Компания «Майкрософт» отключила сервис “Windows Live Messenger IM” для пользователей из стран, в отношении которых действует эмбарго Соединенных Штатов, и поэтому сервис “Windows Live” больше не предоставляется в вашей стране».

- Доступ с домена .cu закрыт и на другие веб-сайты: Cisco Systems (http://tools cisco com/RPF/register do) — технологии связи, маршрутизаторы для Интернет-серверов, включая оборудование для цифрового видео; SolidWorks (http://wwwsolldworks com/sw/termsofuse html) — автоматизированные системы дизайна; и Symantec (http://www symantec com/about/profile/pollcies/legal) — антивирусное программное обеспечение.

- Соединенные Штаты цинично и лицемерно обвиняют Кубу в том, что та якобы препятствует доступу их граждан во всемирную сеть, тогда как в реальности дело обстоит совершенно иначе: из-за блокады, которую установили по отношению к ней Соединенные Штаты, Куба не может подсоединиться к линиям волоконно-оптической связи, окружающим кубинский архипелаг, и вынуждена платить за дорогостоящие услуги спутниковой связи.

- По состоянию на декабрь 2008 года кубинское телекоммуникационное предприятие “La Empresa de Telecomunicaciones de Cuba S.A.” (ETECSA) понесло убытки в размере 53 769,8 долл. США, в первую очередь из-за невозможности закупить специализированное оборудование на американском рынке. В результате ему приходится прибегать к услугам посредников, которые взвинчивают цены на продукты, необходимые для функционирования этого предприятия.

11. Подобная позиция Соединенных Штатов вступает в противоречие с духом, волеизъявлением и решениями, которые были приняты странами всего мира в Швейцарии и Тунисе в рамках Всемирной встречи на высшем уровне по вопросам информационного общества. Участники Встречи настоятельно призвали государства при строительстве информационного общества ввести необходимые нормативные положения с тем, чтобы не допускать и воздерживаться от принятия односторонних мер, идущих вразрез с международным правом и Уставом Организации Объединенных Наций, которые создают помехи полному достижению целей социально-экономического развития населения соответствующих стран и наносят ущерб благополучию их граждан.

12. Двенадцатая сессия Комиссии по науке и технике в целях развития, состоявшаяся в Женеве 25–29 мая 2009 года, на которой обсуждались успехи в осуществлении решений Всемирной встречи на высшем уровне по вопросам информационного общества и последующей деятельности в связи с ней, стала важным форумом, на котором Куба вновь заявила о своем осуждении политики блокады, проводимой по отношению к ней правительством Соединенных Штатов, и, в частности, применения односторонних принудительных мер в отношении развития коммуникационных технологий и доступа к информации, а также агрессивной политики в отношении кубинского радиочастотного спектра, что идет вразрез с решениями, принятыми на двух этапах упомянутой встречи.

13. Ведущиеся в Генеральной Ассамблее Организации Объединенных Наций дискуссии по вопросу о достижении в сфере информатизации и телекоммуникаций в контексте международной безопасности весьма актуальны, и их актуальность и важность возрастают с каждым днем. Действия Соединенных Штатов Америки против Кубы, подобные описанным выше, свидетельствуют о необходимости таких обсуждений, равно как и о важности принятия мер к тому, чтобы положить конец таким проявлениям государственного терроризма.

14. Куба решительно поддерживает деятельность Генеральной Ассамблеи Организации Объединенных Наций в этой области, и по этой причине она присоединилась к 178 государствам-членам, проголосовавшим за принятие резолюции 63/37, что резко контрастирует с позицией, уже неоднократно занимавшейся Соединенными Штатами Америки — единственной страной, проголосовавшей против этой резолюции.

15. Куба будет и в дальнейшем прилагать максимум усилий для содействия мирному глобальному развитию информационных и телекоммуникационных технологий и их применению на благо всего человечества, и она готова совместно со всеми остальными странами, в том числе Соединенными Штатами Америки, заняться поиском путей преодоления препятствий, которые мешают достижению этих целей.

Мали

[Подлинный текст на французском языке]
[9 июля 2009 года]

Мнения и замечания, касающиеся осуществления резолюции о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности

Общие проблемы в области информационной безопасности

1. Основными формами атак на информационные системы являются отказ в работе серверов, направленный на прекращение функционирования информационной системы, и вторжение в систему с целью использования информации не по назначению.

2. Угрозами, стоящими перед государственными системами или чувствительными предприятиями, являются угрозы или инциденты, которые затрагивают целостность системы, конфиденциальность или доступность основной информационной инфраструктуры.

3. В качестве примеров можно привести следующие:

- угрозы со стороны иностранного правительства, террористической группы или экстремистов, обусловленные политическими мотивами;
- угрозы, связанные со шпионажем, саботажем, иностранным вмешательством или насилием политического характера (терроризмом).

4. Использование информационных технологий выступает в качестве альтернативы более традиционным методам, таким, как уничтожение, создание

помех с помощью электромагнитных волн, физическое проникновение или контроль за внутренними источниками информации.

5. Информационные атаки могут быть направлены как против частных лиц, так и против предприятий или государственных учреждений. Что касается атак, направленных на подрыв обороны или национальной безопасности, то они особенно угрожают государственным службам, операторам, обеспечивающим жизненно важные функции, и предприятиям, связанным со стратегическими или чувствительными вопросами. Тем не менее, эти атаки не приводят к одинаковым последствиям в зависимости от того, направлены ли они против объектов или служб, доступных широкой публике, операционных систем или непосредственно против лиц, обладающих конфиденциальной информацией.

6. Особенно сложной задачей является выявление источника информационной атаки. Применяемая процедура чаще всего связана с проверкой цепочки использовавшихся для этого компьютеров, которые могут быть расположены в различных странах. Прослеживание всего пути до начала цепочки задействованного компьютерного оборудования означает проведение чрезвычайно долгих расследований, зависящих от международного сотрудничества между судебными органами. Методы сокрытия разнообразны: от использования компьютеров втайне от их владельцев до использования публичных и анонимных компьютеров, например, расположенных в Интернет-кафе.

7. Большинство государственных служб и наблюдателей указывают, что за этими атаками стоят группы информационных пиратов, применяющих все более сложные методы.

Усилия на национальном уровне и международное сотрудничество по укреплению информационной безопасности

a) В национальном плане

8. В настоящее время Мали не располагает действующими законами в области информационной безопасности.

9. Создание нормативно-правовых рамок является одним из приоритетных направлений национального стратегического плана развития информационно-коммуникационных технологий, принятого правительством в июне 2005 года.

10. Правительство Мали получило от Международной ассоциации развития кредит (4033 MLI) для финансирования проекта поддержки развития и намерено использовать часть этого кредита для проведения консультаций с целью оказания технической помощи в разработке нормативно-правовых рамок применения информационно-коммуникационных технологий Мали.

11. Выбор консультантов заемщиками Всемирного банка определялся просьбой сообщить о заинтересованности (№ 001/2009/SPM/UCP-PAC) в соответствии с кругом ведения, разработанным в мае 2008 года Агентством по информационно-коммуникационным технологиям.

12. В этих нормативно-правовых рамках предусмотрено разработать тексты законов о свободах, деловой практике, электронной торговле, интеллектуальной собственности, безопасности и конфиденциальности данных, преступлениях и деликтах в киберпространстве, свободном доступе к открытой информации и информации, представляющей собой достояние человечества.

b) Международное сотрудничество по укреплению информационной безопасности

13. Информационные атаки совершаются через границы и могут быть одновременно направлены против нескольких государств. Наблюдение за сетями и реагирование в случае инцидентов требует международного сотрудничества и помощи. В целом защита информационных систем от незаконных видов деятельности в настоящее время представляет собой совместную задачу многих государств.

14. Кроме того, Мали выступает за региональный подход к регулированию сектора телекоммуникаций, в связи с чем страна ратифицировала директивы Западноафриканского экономического и валютного союза (ЮЕМОА) в 2006 году и дополнительные акты ЭКОВАС в 2007 году.

15. Международный союз электросвязи работает над созданием международных рамок обеспечения кибербезопасности (Глобальная программа кибербезопасности), к которым Мали проявляет особый интерес. Эти меры по обеспечению кибербезопасности привели к созданию группы экспертов высокого уровня, на которую возложена задача подготовки долгосрочной стратегии, включающей правовые меры, технические меры по исправлению недостатков программного обеспечения, а также меры по предупреждению и выявлению информационных атак и устранения последствий кризиса.

Содержание международных принципов укрепления безопасности в области телеинформатики

16. Информационная безопасность на международном уровне должна основываться на существующем международном праве (jus ad bellum), в котором определяются меры по устранению угроз международному миру и безопасности, и на международном гуманитарном праве (jus in bello), которое касается методов и средств ведения войны, защиты государств, не являющихся сторонами конфликта, а также лиц и имущества, которые затронуты или могут быть затронуты конфликтом.

17. Основополагающим документом международного права в вопросах поддержания международного мира и безопасности является Устав Организации Объединенных Наций.

18. Все специалисты международного права признают, что содержащиеся в нем положения предусматривают универсальный механизм безопасности для сохранения международного мира и безопасности. В то время как информационно-коммуникационные технологии отныне разрабатываются и используются как средства разрушения (иными словами как «информационное оружие»), а международное сообщество пока не определилось с местом информационной безопасности в существующем международном праве, положения Устава Организации Объединенных Наций могут быть истолкованы таким образом, чтобы обеспечить международным участникам широкое поле деятельности для использования информационно-коммуникационных технологий для агрессивных действий и урегулирования международных конфликтов и споров.

19. Такая удивительная ситуация вытекает из того факта, что враждебные действия в области информации пока конкретно не рассматриваются в между-

народном праве в том же плане, что и враждебные действия с применением обычных вооружений, даже если сегодняшнее взаимодействие в мире и его зависимость от информационно-коммуникационных технологий означает, что подобного рода атака будет столь же и даже более разрушительной, что и атака с применением обычных вооружений. Трудности усугубляются отсутствием общепринятых толкований таких понятий, как «акт агрессии» (статья 1), «сила» (статья 2, пункт 4) и «вооруженное нападение» (статья 51) применительно к информационной безопасности.

20. Акт агрессии определяется в резолюции 3314 (XXIX) Генеральной Ассамблеи от 14 декабря 1974 года.

21. Даже если эта резолюция и не была принята консенсусом, ее положения дают Совету Безопасности и всем членам международного сообщества ориентиры в отношении критериев определения акта агрессии.

22. Применение информационного оружия может быть истолковано как акт агрессии, если государство, являющееся жертвой, имеет основания полагать, что атака была совершена вооруженными силами другого государства и была направлена на нарушение функционирования военных установок, уничтожение оборонного и экономического потенциала или нарушение суверенитета государства на конкретной территории.

Меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне

23. Для укрепления информационной безопасности на глобальном уровне и противодействия угрозе использования информационно-коммуникационных технологий во враждебных целях международное сообщество должно сосредоточить свои усилия на ряде областей, включая следующие:

a) Оказание содействия государствам в информировании и обеспечении ответственности различных участников (административных органов, предприятий и пользователей) в вопросах безопасности информационных систем. В этом контексте важная роль отводится координации политики государств в области обеспечения безопасности продукции на производственном и технологическом уровне. Значительное внимание должно также уделяться сотрудничеству между государствами и частным сектором;

b) Укрепление потенциала государств путем предоставления в их распоряжение необходимых людских ресурсов и технических знаний и специалистов для наблюдения и, таким образом, выявления необычных потоков, через которые осуществляются кибератаки;

c) Изменение круга ведения различных международных учреждений, занимающихся вопросами безопасности информационных систем, предоставив каждому из них конкретные функции;

d) Установление показателей в области информационной безопасности для оказания помощи странам в совершенствовании управления инфраструктурой информационно-коммуникационных технологий. Эти показатели могут касаться следующих аспектов:

• восстановления данных в критической ситуации

- использования стандартов (норм)
- контроля за деятельностью (установление целевых показателей)
- электронного перевода
- сотрудничества с Интерполом
- платформы доступа.

Заключение

24. Как представляется, проблемы информационной безопасности и использования информационно-коммуникационных технологий во враждебных целях вызывают все большее беспокойство. Эти технологии, безусловно, предоставляют многочисленные преимущества, однако и могут привести к катастрофам с непредсказуемыми последствиями, учитывая их неуклонное развитие.

25. Возникшие в результате развития этих технологий правовые вопросы до настоящего времени не нашли удовлетворительного решения по причине различных нормативных положений, которые часто не подходят для этих целей.

26. Таким образом, государствам надлежит обеспечить согласованную разработку этих инструментов, чтобы гарантировать лучшие условия для вступления в более безопасное информационное общество.

Испания

[Подлинный текст на испанском языке]
[8 июля 2009 года]

Позиция Испании по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности

Введение

1. Информационная безопасность — одна из ключевых сторон жизни информационного общества. Технический прогресс способствует постоянному и ускоренному расширению возможностей для обработки и хранения информации в самых разных форматах; с другой стороны, в сфере коммуникации происходит резкое увеличение пропускной способности существующих каналов, что открывает возможности для передачи и получения огромных объемов информации практически в реальном режиме времени и без необходимости наличия особенно сложных технических устройств.

2. Подобный технический прогресс не только ведет к повышению доступности информации любого типа, но и способствует большей доступности и более широкому использованию этой информации с противоправными целями, в особенности использованию телекоммуникационных и информационных систем с враждебными и преступными целями и даже для совершения террористических актов или актов агрессии в отношении государств или транснациональных структур.

3. В последние годы наблюдается растущая тенденция к использованию сети Интернет преступными организациями и, в частности, террористическими группами, которые пользуются в основном двумя ее отличительными особенностями: глобальным характером этой сети и надежными гарантиями анонимности, которые она может дать.

4. В этой связи необходимо найти «золотую середину» между эволюцией общества и информационных технологий и параллельным развитием таких национальных и международных норм, которые были бы актуальными, современными, учитывали новые технические реалии и могли бы использоваться для решения задач, связанных с необходимостью защиты информации от противоправного использования без ограничения прав и свобод личности.

Ненадлежащее использование сети Интернет в террористических целях

5. Сегодня основные угрозы, связанные с использованием сети Интернет террористическими организациями, состоят в следующем:

a) Использование сети Интернет как оружия, т.е. использование Интернета как средства для осуществления атак против информационных систем ключевых инфраструктурных объектов либо против самой инфраструктуры сети Интернет. Подобного рода атаки — весьма частое явление в сфере общеуголовной преступности, но та атака, которой подверглась Эстония в 2007 году, показала, что атаки подобного рода могут быть направлены и против информационной инфраструктуры того или иного государства. Прямое отношение к такой угрозе имеет резкое увеличение в последние два года числа новых вредоносных программ, а также «бот-сетей», или сетей компьютеров — «зомби», которые используются для осуществления атак на информационные системы.

b) Использование сети Интернет как средства для решения других задач, в первую очередь в следующих:

- Коммуникационные функции. Интернет заменяет собой другие виды связи, которыми пользуются преступные организации, включая стационарные и мобильные телефоны. Наиболее часто используемыми средствами коммуникации в Интернете являются электронная почта, программы мгновенного обмена сообщениями и форумы.

- Пропаганда и распространение материалов, связанных с террористической деятельностью. Сегодня в сети существуют тысячи веб-сайтов, которые посвящены террористической деятельности или занимаются пропагандой насилия, причем эта тенденция усилилась с появлением такого средства общения, как блоги. Что же касается способов помешать подобному использованию Интернета террористическими организациями, то дело это достаточно сложное, поскольку эти сайты способны легко менять свои адреса. Речь здесь идет о транснациональном явлении, так как страны, где находится сервер с данной страницей, и страны, откуда осуществляется ее администрирование, могут быть разными и, более того, отличными от той страны, где действует соответствующая террористическая организация.

- Акции по вербовке. Периодически Интернет используется для организации акций по вербовке сторонников, особенно при помощи форумов и программ мгновенного обмена сообщениями.

- Финансирование. Интернет также открывает возможности для проведения террористическими организациями акций по сбору финансовых средств. Особый интерес представляет возможность участия террористических организаций в актах мошенничества при помощи Интернета как способа получения финансовых средств.

- Распространение учебных пособий. Через Интернет террористические организации рассылают пособия по методам террористической деятельности, изготовлению взрывчатых веществ или обращению с оружием.

- Сбор информации для совершения терактов. Интернет представляет собой крайне важный источник информации, которая во многих случаях используется террористическими организациями для сбора данных об объектах их покушений.

Меры, принимаемые на национальном уровне для противодействия использованию сети Интернет террористическими организациями

Законодательные меры

6. Если говорить о мерах, принимаемых различными государствами, то в последние годы, и особенно в 2007 году, Испания проделала огромную работу в этой связи, включив в систему внутреннего права целый ряд законов, имеющих отношение к информационной безопасности и свободному осуществлению прав и свобод, провозглашенных во Всеобщей декларации прав человека и Конституции Испании. Была разработана обширная нормативно-правовая база, включающая в себя как чисто национальные аспекты, так и директивы Европейского союза и направленная на решение этих задач путем применения новых требований к информационной безопасности, в которых предусматривается, что для обеспечения достаточного уровня защиты важное значение, помимо сохранения конфиденциальности информации, в большинстве случаев приобретает сохранение ее целостности и доступности. Среди принятых законов можно отметить следующие (в хронологическом порядке):

- Органический закон 5/1992 от 29 октября о порядке автоматизированной обработки личных данных, в основе которого лежит идея создания предохранительных механизмов, которые предупреждали бы нарушения конфиденциальности при обработке информации, и положения, принятые в его развитие.

- Органический закон 15/1999 от 13 декабря о защите личных данных, призванный гарантировать и защищать — в части, касающейся обращения с личными данными, — публичные свободы и основополагающие права физических лиц, в особенности их достоинство и право на неприкосновенность частной и семейной жизни, и положения, принятые в его развитие.

- Королевский декрет-закон 14/1999 от 17 сентября об электронной подписи, принятый в целях скорейшего внедрения новых технологий обеспечения безопасности электронных сообщений в практику работы предприятий и государственных учреждений и в жизнь рядовых граждан. На основании этого декрета в испанскую систему публичного права включена директива 1999/93/CE Европарламента и Совета Европы от 13 декабря 1999 года, устанавливающая общеевропейские нормы использования

электронной подписи. На основании закона 59/2003 от 19 декабря об электронной подписи в эти нормы были внесены коррективы с учетом опыта, накопленного со времени вступления упомянутого декрета в силу.

- Закон 11/2002 от 6 мая о порядке функционирования Национального разведывательного центра (НРЦ), а в дальнейшем — королевский декрет 421/2004 от 12 марта о порядке функционирования Национального криптологического центра, в которых НРЦ было поручено, в частности, координировать действия различных государственных учреждений, пользующихся цифровыми средствами и методами, гарантировать безопасность информационных технологий в этой области и следить за соблюдением норм, касающихся защиты секретной информации.

- Закон 34/2002 от 11 июля об услугах информационного общества и электронной торговле. Имеет целью включение в испанскую систему внутреннего права директивы 2000/31/CE от 8 июня, касающейся определенных аспектов услуг информационного общества, в частности электронной торговли на внутреннем рынке (директива об электронной торговле). Кроме того, в него частично включена директива 98/27/CE Европарламента и Совета Европы от 19 мая о судебных запретах в области защиты интересов потребителей, в которой регулируется порядок наложения судебных запретов на действия, представляющие собой нарушение данного закона.

- Закон 32/2003 от 13 ноября: общий закон о телекоммуникации, регулирующий использование сетей и предоставление услуг по передаче электронных сообщений.

- Закон 59/2003 от 19 декабря об электронной подписи, уже упоминавшийся выше.

- Закон 11/2007 от 22 июня об электронном доступе граждан к государственным службам, который регламентирует коммуникацию между гражданами и государственными учреждениями путем использования существующих электронных, информационных и телематических методов и средств.

- Органический закон 10/2007 от 8 октября о создании полицейской базы данных с идентификационными данными, полученными при помощи анализа дезоксирибонуклеиновой кислоты (ДНК). Он предусматривает создание базы данных, в которую будут впервые включены файлы по сотрудникам государственных сил и органов безопасности, содержащие идентификационные данные, полученные путем анализа ДНК, который проводится в рамках уголовного расследования, при опознании трупов либо выяснении участи пропавших без вести.

- Закон 25/2007 от 18 октября о сохранении данных, касающихся электронных сообщений и публичных коммуникационных сетей, который имеет конкретное отношение к ведущимся в этой сфере расследованиям.

- Королевский декрет 1720/2007 от 21 декабря, принятый в развитие положений Органического закона 15/1999 от 13 декабря о защите личных данных.

- Закон 56/2007 от 28 декабря о мерах, способствующих развитию информационного общества.
- Определение состава следующих киберпреступлений, связанных с деятельностью террористических организаций в сети Интернет:
  - информационный саботаж, статья 264 Уголовного кодекса;
  - угрозы, статья 169 и последующие статьи Уголовного кодекса;
  - апологетика и героизация терроризма, статья 578 Уголовного кодекса.

Другие меры

- Создание специализированных полицейских подразделений для борьбы с использованием сети Интернет преступными группами.
- Участие в проекте Европола “Check the Web” («Проверка сети Интернет»).
- Создание центра быстрого реагирования для повышения безопасности информационных систем в государственных учреждениях.
- Создание национального центра защиты ключевых объектов инфраструктуры.

Меры, которые могут быть приняты международным сообществом для укрепления информационной безопасности в общемировом масштабе

- Использование сети Интернет террористическими организациями — это явление транснационального характера, которое зачастую требует проведения совместных расследований в разных странах. Таким образом, расследование и предупреждение террористической деятельности в сети Интернет во многом зависит от наличия международных соглашений и других инструментов международного сотрудничества. В этой связи важно обеспечивать согласование законодательных норм, которое позволило бы эффективнее бороться с присутствием в сети этих преступных групп. Еще одним важным аспектом является международное сотрудничество в полицейской сфере, поскольку при подобного рода расследованиях решающую роль играет оперативность в деле сбора трудноуловимых электронных доказательств.
- Привлечение частного сектора к борьбе с киберпреступностью. Участие частного сектора имеет важное значение по той причине, что он занимается оказанием большинства Интернет-услуг. Частный сектор тратит немало времени на борьбу с угрозами в сети Интернет, и его знания и опыт могут оказаться чрезвычайно полезными в этой связи.
- Разъяснение конечным пользователям важности обеспечения безопасности их информационных систем. Лучшее понимание этих проблем будет способствовать сокращению числа компьютеров, используемых кибер-

преступниками для своих операций, особенно связанных с использованием «бот-сетей».

- Что касается мер, которые могут быть приняты международным сообществом для укрепления информационной безопасности в глобальном масштабе, то представляется целесообразным подписать межгосударственное соглашение (наподобие Конвенции СОЛАС или аналогичного документа), в котором государства обязались бы унифицировать законодательные нормы для судебного преследования лиц, совершающих преступления в сети, стремясь, по возможности, не допустить того, чтобы в результате анонимности, отсутствия законодательных норм и наличия экономических интересов Интернет превратился в инкубатор преступности и терроризма. При этом нельзя забывать об уважении свободы информации и беспрепятственного доступа к ней.

- Активизация процессов судебного и полицейского сотрудничества на международном уровне, в соответствии с действующим в каждой стране законодательством, для оперативного и эффективного судебного преследования лиц, совершающих уголовные преступления, с учетом распределенного характера сети Интернет и трудноуловимости данных о сетевых операциях.

7. В заключение следует отметить, что международное сообщество должно принимать такие меры по защите информации, которые оно сочтет необходимыми, исходя из общего стратегического видения этой проблемы и, по возможности, создав единый руководящий орган, который установил бы общие нормы и процедуры для всех стран, разработал полный и сбалансированный комплекс конкретных мер защиты и дал возможность согласовать стратегии и действия различных национальных и международных организаций, участвующих в этой работе.