Организация Объединенных Наций A/67/167*

Генеральная Ассамблея

Distr.: General
23 July 2012
Russian
Original: English/Russian/Spanish

Шестьдесят седьмая сессия
Пункт 90 предварительного перечня повестки дня**
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Содержание

* Переиздано по техническим причинам 8 апреля 2013 года.
** A/67/150.

12-43416* (R) 090413 090413

I. Введение

1. В пункте 3 постановляющей части своей резолюции 66/24 Генеральная Ассамблея просила все государства-члены, принимая во внимание оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/65/201), продолжать информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

a) общая оценка проблем информационной безопасности;

b) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

c) содержание концепций, упомянутых в пункте 2 резолюции;

d) возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне.

2. В соответствии с этой просьбой 16 февраля 2012 года государствам-членам была направлена вербальная нота с просьбой предоставить информацию по этому вопросу. Полученные ответы содержатся ниже в разделе II. Любые полученные дополнительные ответы будут изданы в качестве добавлений к настоящему докладу.

II. Ответы, полученные от правительств

Колумбия

[Подлинный текст на испанском языке]
[21 мая 2012 года]

Вне всякого сомнения, использование информационно-коммуникационных технологий принесло нашим странам важные изменения и преимущества. Однако успехи в области этих технологий одновременно способствовали росту применения по всему миру технологических средств в преступных целях, что указывает на необходимость принятия неотложных мер и механизмов контроля, обеспечивающих защиту государств от этих новых угроз.

Все страны разделяют обеспокоенность ростом преступного потенциала в киберпространстве, а также использованием новых технологий для создания информационных угроз, поскольку они оказывают существенное воздействие на безопасность информации как в публичной, так и в частной сфере, включая гражданское общество, что указывает на необходимость строго применять протоколы и стратегии в области безопасности, нужные для создания механизмов контроля, позволяющих защитить государство и важнейшие объекты его инфраструктуры от этих новых угроз.

В этой связи в 2005 году Колумбия разработала так называемую норму ISO-27001, задуманную в качестве системы управления, охватывающей политику, организационную структуру, процедуры, процессы и ресурсы, необходимые для осуществления управления информационной безопасностью, которая обеспечивается за счет применения таких стандартов качества, как кодекс передовых видов практики и контрольных показателей (норма ISO 17799), и которая основана на сохранении свойств конфиденциальности, неприкосновенности и доступности, смысл которых объясняется ниже:

- конфиденциальность: не допускать несанкционированного использования информации отдельными лицами или в рамках процессов;
- неприкосновенность: охранять точность и полноту всей информации, представляющей ценность для какой-либо организации;
- доступность: доступная информация, пригодная к применению по просьбе имеющих соответствующее разрешение субъектов.

Преимущества нормы ISO 27001 проявляются в следующем:

a) создание ясной и хорошо структурированной методики управления информационной безопасностью;

b) сокращение рисков утечки или кражи информации;

c) гарантированный доступ к информации для пользователей;

d) постоянное отслеживание рисков в отношении информации и соответствующих механизмов контроля за ее безопасностью;

e) возможность осуществлять внешние и внутренние ревизии, позволяющие выявлять вероятные недостатки в системах информационной безопасности;

f) гарантии выполнения законов и правил, установленных в области информационного управления;

g) повышение уровня осведомленности лиц о вопросах информационной безопасности.

Кроме того, в целях поиска оптимальных правовых и оперативных рамок для обеспечения информационной безопасности 5 января 2009 года Конгресс Республики Колумбия промульгировал закон № 1273, «которым вносятся изменения в Уголовный кодекс, создается новый предмет правовой защиты, относимый к рубрике «О защите информации и данных», и полностью сохраняются, в частности, системы, в которых применяются информационно-коммуникационные технологии».

Этот важный закон состоит из двух глав: «О покушениях на конфиденциальность, неприкосновенность и доступность информационных систем» и «Об информационных покушениях и прочих нарушениях».

Первая глава предусматривает следующее:

- *противозаконный доступ к информационной системе*: лицо, которое без разрешения или в обход договоренности получает полный или частичный доступ к какой-либо информационной системе, как защищенной, так и не защищенной с помощью каких-либо средств безопасности, или остается в

этой системе против воли того, кто обладает законным правом на его отстранение, наказывается тюремным заключением на срок от сорока восьми (48) до девяноста шести (96) месяцев и штрафом в размере от 100 до 1 000 ныне действующих законных минимальных месячных окладов;

- *незаконное воспрепятствование функционированию информационной системы или телекоммуникационной сети*: *лицо*, которое, не имея на то полномочий, противодействует или препятствует нормальному функционированию или доступу к информационной системе, к содержащимся в ней информационным данным или к телекоммуникационной сети, наказывается тюремным заключением на срок от сорока восьми (48) до девяноста шести (96) месяцев и штрафом в размере от 100 до 1000 ныне действующих законных минимальных месячных окладов, если это деяние не составляет преступления, подпадающего под более суровое наказание;

- *перехват информационных данных*: лицо, которое без предварительного судебного постановления перехватывает информационные данные в точке их происхождения или назначения либо внутри информационной системы или же перехватывает электромагнитные излучения, происходящие из передающей их информационной системы, наказывается тюремным заключением на срок от тридцати шести (36) до семидесяти двух (72) месяцев;

- *информационный ущерб*: лицо, которое, не имея на то полномочий, уничтожает, повреждает, стирает, приводит в негодность, изменяет или ликвидирует информационные данные или систему обработки информации либо ее логические части или компоненты, наказывается тюремным заключением на срок от сорока восьми (48) до девяноста шести (96) месяцев и штрафом в размере от 100 до 1000 ныне действующих законных минимальных месячных окладов;

- *использование вредоносного программного обеспечения*: лицо, которое, не имея на то полномочий, производит, приобретает, распределяет, продает, пересылает, ввозит на национальную территорию или вывозит с нее вредоносное программное обеспечение или другие компьютерные программы, имеющие вредоносное воздействие, или торгует ими, наказывается тюремным заключением на срок от сорока восьми (48) до девяноста шести (96) месяцев и штрафом в размере от 100 до 1000 ныне действующих законных минимальных месячных окладов;

- *нарушение неприкосновенности личных данных*: лицо, которое, не имея на то полномочий, в целях личной выгоды для себя или третьего лица, получает, составляет, похищает, выставляет на продажу, продает, обменивает, посылает, покупает, перехватывает, разглашает, изменяет или применяет личные коды, личные данные, содержащиеся в картотеках, архивах, базах данных или аналогичных средствах, наказывается тюремным заключением на срок от сорока восьми (48) до девяноста шести (96) месяцев и штрафом в размере от 100 до 1000 ныне действующих законных минимальных месячных окладов;

- *подделывание веб-сайтов в целях завладения персональными данными*: лицо, которое в незаконных целях и не имея на то полномочий создает, разрабатывает, продает, изготавливает, программирует или посылает электронные страницы, ссылки или диалоговые окна, или торгует ими, нака-

зывается тюремным заключением на срок от сорока восьми (48) до девяноста шести (96) месяцев и штрафом в размере от 100 до 1000 ныне действующих законных минимальных месячных окладов, если это деяние не составляет преступления, подпадающего под более суровое наказание.

Вторая глава предусматривает следующее:

- *хищение с помощью информационных и аналогичных средств*: лицо, которое в обход средств информационной безопасности совершает предусмотренное в статье 239 деяние, манипулируя информационной системой, сетевой электронной, информационно-вычислительной системой или иным аналогичным средством либо незаконно действуя от имени пользователя в существующих системах идентификации и авторизации, наказывается в соответствии с положениями статьи 240 Уголовного кодекса, а именно тюремным заключением на срок от трех (3) до восьми (8) лет;

- *несанкционированный перевод активов*: лицо, которое в целях получения выгоды и с помощью какой-либо информационной манипуляции или аналогичного способа осуществляет несанкционированный перевод каких-либо активов в ущерб какому-либо лицу, наказывается тюремным заключением на срок от сорока восьми (48) до ста двадцати (120) месяцев и штрафом в размере от 200 до 1500 ныне действующих законных минимальных месячных окладов. То же наказание применяется к лицу, которое производит или внедряет компьютерную программу, предназначенную для совершения предусмотренного в предыдущем пункте преступления либо для совершения мошенничества, или владеет такой программой, или же содействует ее использованию.

Вне всякого сомнения, закон № 1273, принятый в 2009 году, стал важнейшим шагом вперед в борьбе с информационными преступлениями в Колумбии. Вместе с тем распространение различных форм и методов организованной преступности, и в особенности киберпреступности, вынудило Колумбию разработать целостную стратегию борьбы с киберпреступностью с упором на кибероборону и кибербезопасность, в рамках которых межведомственное взаимодействие является определяющим фактором для достижения целей, предусматриваемых концепцией информационной безопасности.

В этом контексте в июле 2011 года правительство Колумбии начало внедрять национальную стратегию кибероборонны и кибербезопасности, основанную на трех главных компонентах:

- принятие надлежащих межинституциональных рамок для предупреждения, координации и пресечения возникающих угроз и рисков и вынесения рекомендаций в целях борьбы с ними;

- обеспечение специализированной подготовки в области информационной безопасности и расширение направлений исследований в сферах кибероборонны и кибербезопасности;

- укрепление законодательства в этих сферах, развитие международного сотрудничества и ускорение процесса присоединения Колумбии к различным международным документам.

В целях комплексного развития вышеупомянутых стратегических направлений Колумбия создала и задействовала следующие четыре (4) инстанции:

a) в первую очередь речь идет о так называемой Межотраслевой комиссии, которой поручено определить стратегическую концепцию информационного управления, а также установить направления политики в отношении управления технологической инфраструктурой, общественной информацией, кибербезопасностью и киберзащитой;

b) вторая инстанция — это Группа реагирования на кибернетически чрезвычайные ситуации в Колумбии, которая представляет собой орган, координирующий на национальном уровне вопросы кибербезопасности и киберозащиты;

c) в-третьих, Объединенное кибернетическое командование вооруженных сил, исполняющее функции предупреждения и устранения любых угроз и нападений кибернетического характера, затрагивающих национальные ценности и интересы;

d) и наконец, Полицейский кибернетический центр, который отвечает за вопросы кибербезопасности колумбийской территории, предоставляя информацию, поддержку и защиту в целях борьбы с киберпреступлениями.

Эти структуры обеспечат Колумбии возможность выполнять и развивать мандаты в рамках национальной стратегии кибероборонs и кибербезопасности и оказывать комплексное и эффективное противодействие этой новой форме преступности, которая стремительно развивается сегодня в мире.

Тем не менее Колумбия не остановилась на разработке своей стратегии кибероборонs и кибербезопасности. Посредством этой стратегии осуществляется ряд важных отраслевых инициатив, отвечающих потребностям в создании эффективных стратегий информационной безопасности. Ниже изложены наиболее важные из них.

Инициатива	*Руководящий орган*	*Сфера охвата*
Модель информационной безопасности для стратегии создания электронного правительства	Программа «Электронное правительство» — министерство информационных технологий и коммуникаций	Эта модель безопасности означает совокупность стратегий в поддержку достижения целей электронного правительства, таких как защита индивидуальной информации и репутация и доверие в электронном правительстве. В качестве основных элементов информационной безопасности для правительственных органов она устанавливает: a) доступность информации и услуг; b) неприкосновенность информации и данных; и c) конфиденциальность информации.
Рекомендации национальному правительству по осуществлению национальной стратегии кибербезопасности	Комиссия по регулированию телекоммуникаций	Посредством этого документа Комиссия по регулированию телекоммуникаций предоставляет национальному правительству рекомендации по созданию национальной стратегии кибербезопасности и в свою очередь обеспечивает соответствующие инструменты для сотрудничества и взаимодействия между правительством и частным сектором на всех уровнях; определяет пути борьбы с киберпреступностью; рекомендует осуществление и развитие относящихся к кибербезопасности правовых рамок, соответствующих международным параметрам; предоставляет рекомендации по разработке систем реагирования на связанные с безопасностью инциденты в сети, включая надзор, анализ и реа-

Инициатива	*Руководящий орган*	*Сфера охвата*
		гирование на эти инциденты; и предлагает направления внедрения национальной культуры кибербезопасности, повышающей уровень защиты важнейшей информационной инфраструктуры в Колумбии.
Колумбийский центр координации помощи при инцидентах, связанных с информационной безопасностью, для провайдеров интернет-услуг	Колумбийская информационно-телекоммуникационная палата	Колумбийский центр координации помощи при инцидентах, связанных с информационной безопасностью, который действует в непосредственном контакте с центрами безопасности его филиалов (крупнейших в Колумбии компаний-провайдеров интернет-услуг). Уполномочен координировать обработку и урегулирование поступающих ходатайств и заявлений по проблемам информационной безопасности.

Однако если оставить в стороне вопрос о национальном потенциале в сфере информационной безопасности, то важно упомянуть ряд мер, которые Колумбия считает целесообразным принять на международном уровне для укрепления информационной безопасности:

- укрепление коммуникационных каналов между странами, входящими в состав Организации Объединенных Наций, в целях объединения усилий по транснациональной борьбе с преступлениями, затрагивающими информацию и данные;
- определение международных и региональных документов, в которых содержится квалификация наказуемых деяний, составляющих покушения на кибербезопасность и кибероборону в каждом государстве;
- определение и структурирование протоколов о помощи при инцидентах в сфере информации с разработкой глобальных стратегий, посвященных информационной безопасности;
- укрепление имеющей превентивный характер и укладывающейся в рамки законности деятельности в отношении групп «хактивистов», особенно в университетах и колледжах, с целью сокращения участия молодежи в этих организациях, подвергающих опасности нормальное развитие цифровой инфраструктуры государств;
- стандартизированное законодательство с упором на профилактику, помощь и отслеживание деятельности, связанной с информационной безопасностью;
- технологическая конвергенция и имплементация с акцентом на освоение наилучших видов практики в сфере управления информационной безопасностью. В этом пункте важно указать, что должны существовать планы по инвестированию в новейшие технологии и оказанию поддержки проектов технологического развития со стороны государств;
- создание платформ для обмена информацией и знаниями согласно универсальным стандартам, регулирующим эту сферу.

Нормативные акты Республики Колумбия, касающиеся информационной безопасности

Закон/резолюция	*Тема*
Закон № 527 1999 года (электронная торговля)	Определяет и регламентирует доступность и использование сообщений данных, электронной торговли и цифровых подписей, а также учреждает сертифицирующие органы и предусматривает иные положения.
Закон № 599 2000 года	Вводит в действие Уголовный кодекс. Сохраняет уголовную наказуемость «незаконного нарушения коммуникаций». Создает предмет правовой защиты, относимый к рубрике «авторские права», и охватывает некоторые преступления, косвенным образом связанные с информационным преступлением, такие как выставление на продажу, продажа или покупка инструмента, пригодного для перехвата частных коммуникаций между лицами. Квалифицирует противозаконный доступ к информационной системе (статья 195). Лицо, противозаконным образом проникающее в информационную систему, охраняемую средством безопасности, или сохраняющее присутствие в ней против воли лица, имеющего право пресечь это, наказывается штрафом.
Закон № 962 2005 года	Содержит положения о рационализации административных процедур и формальностей, выполняемых государственными органами и образованиями, а также субъектами, исполняющими государственные функции или оказывающими государственные услуги. Предусматривает поощрение использования интегрированных технологических средств в целях сокращения времени и затрат на осуществление процедур подчиненными.
Закон № 1150 2007 года	Предусматривает меры по обеспечению эффективности и транспарентности закона № 80 1993 года и содержит иные общие положения о заключении договоров в отношении людских ресурсов. В частности, устанавливает возможность опубликования государственными административными органами административных актов и документов и оповещения через электронные средства, для чего предусматривается разработка электронной системы государственного заключения договоров.
Закон № 1273 2009 года	Вносит изменения в Уголовный кодекс, создает новый предмет правовой защиты «защита информации и данных» и предусматривает комплексную защиту систем, использующих информационно-коммуникационные технологии, а также содержит прочие положения.
Закон № 1341 2009 года	Определяет принципы и концепции информационного общества и рамки развития информационно-коммуникационных технологий, предусматривает создание Национального радиочастотного агентства, а также содержит прочие положения.
Резолюция 2258 2009 года Комиссии по регулированию коммуникаций	Касается безопасности сетей, провайдеров сетей и услуг в сфере телекоммуникаций. Эта резолюция вносит изменения в статьи 22 и 23 резолюции CRT 1732 2007 года и в статьи 1,8 и 2,4 резолю-

Закон/резолюция	*Тема*
	ции CRT 1740 2007 года. Эта резолюция устанавливает обязанность провайдеров сетей и/или услуг в сфере телекоммуникаций, которые предоставляют доступ в Интернет, реализовывать модели безопасности согласно свойствам и потребностям своих сетей, способствовать повышению безопасности своих сетей доступа согласно рамочным основам безопасности, определяемым Международным союзом электросвязи, с выполнением принципов конфиденциальности данных, неприкосновенности данных и доступности элементов сети, информации, услуг и приложений, а также средств идентификации, доступа и бесперебойной связи. Кроме того, устанавливает обязанности провайдеров телекоммуникационных сетей и услуг, связанные с коммуникационной неприкосновенностью и информационной безопасностью.
Циркуляр № 052 2007 года (Финансовое управление Колумбии)	Устанавливает минимальные требования по безопасности и качеству в сфере управления информацией через средства и каналы распределения продуктов и услуг для клиентов и пользователей.

Куба

[Подлинный текст на испанском языке]
[21 мая 2012 года]

Использование средств телекоммуникации во враждебных целях, с открытым или тайным намерением подорвать юридические и политические устои государств, представляет собой нарушение международно признанных норм в этой области, что может привести к возникновению трений и неблагоприятных ситуаций для международного мира и безопасности.

Куба полностью разделяет выраженную в резолюции 66/24 Генеральной Ассамблеи озабоченность тем, что информационные технологии и средства могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно отразиться на целостности инфраструктуры государств и нанести ущерб их безопасности в гражданской и военной сферах. Кроме того, в этой резолюции правомерно подчеркивается необходимость предотвратить использование информационных ресурсов и технологий в преступных или террористических целях.

В этой связи Республика Куба вновь заявляет о своем осуждении агрессивной эскалации правительством Соединенных Штатов радиотелевизионной войны, развязанной им против Кубы, которая идет вразрез с действующими международными нормами в области регулирования радиочастотного спектра. Эта агрессия осуществляется без учета того ущерба, который она может нанести международному миру и безопасности, создавая опасные ситуации, в том числе в результате использования военного самолета для трансляции телевизионных сигналов на территорию Республики Куба без ее согласия.

В течение 2011 года с территории Соединенных Штатов на 30 частотах транслировались незаконные еженедельные передачи, среднее эфирное время которых составило 2193 часа. Некоторые из этих радиостанций принадлежат

или оказывают услуги организациям, связанным с известными террористическими элементами, проживающими на территории Соединенных Штатов и действующими против Кубы. Они занимаются трансляцией программ, содержащих призывы к саботажу, политическим покушениям, убийству главы государства и другие призывы, типичные для радиотерроризма.

Эти провокационные передачи, направленные против Кубы, представляют собой нарушение следующих международных норм:

- Основополагающие принципы Международного союза электросвязи, сформулированные в преамбуле его устава. Телепрограммы, транслируемые правительством Соединенных Штатов Америки на Кубу, носят подрывной и дестабилизирующий характер и искажают реальное положение вещей, что идет вразрез с данными принципами.

- Положения CS 197 и CS 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 государств-членов.

- Документ девятого пленарного заседания Всемирной конференции радиосвязи (ноябрь 2007 года), в подпункте (g) пункта 6.1 которого говорится, что «никакая радиовещательная станция, функционирующая на борту воздушного судна и транслирующая передачи исключительно на территорию другой администрации без согласия последней, не может считаться работающей в соответствии с Регламентом радиосвязи».

- Пункт 8.3 статьи 8 Регламента радиосвязи, в котором говорится, что частотные присвоения, занесенные в регистр и получившие международное признание, должны учитываться другими администрациями при осуществлении своих собственных присвоений, с тем чтобы избежать вредных помех.

- Пункт 42.4 статьи 42 Регламента радиосвязи, гласящий, что осуществление радиовещательной службы станциями воздушных судов, находящимися в море или над морем, воспрещается.

- Решение Радиорегламентарного комитета, который на своем 35-м совещании в декабре 2004 года установил факт вредных помех, которые эти трансляции создают для работы кубинских служб на частоте 213 МГц, и потребовал от администрации Соединенных Штатов Америки принять необходимые меры для их ликвидации. Кроме того, Радиорегламентарный комитет с сентября 2006 года требует от администрации Соединенных Штатов Америки принятия мер для ликвидации помех на частоте 509 МГц, однако вплоть до сегодняшнего дня реакции на это требование не последовало. 20 марта 2009 года состоялось 50-е совещание Комитета, и в резюме своих решений (документ RRB09-1/5) он вновь подтвердил незаконность этих передач и потребовал от администрации Соединенных Штатов Америки принять все необходимые меры для ликвидации помех работе телевизионных служб Кубы на двух указанных частотах.

- Пункт 23.3 статьи 23 Регламента радиосвязи, который налагает ограничения на работу станций телевизионного вещания за пределами границ страны. В докладе, опубликованном в январе 2009 года, Счетная палата правительства Соединенных Штатов признала нарушения международных норм и внутреннего законодательства, допускаемые программой радио- и телевизионного вещания американского правительства на Кубу.

На своей сессии в 2007 году, проходившей в Женеве, Всемирная конференция радиосвязи приняла текст выводов, в котором трансляции с борта воздушных судов Соединенных Штатов на Кубу были признаны не соответствующими Регламенту радиосвязи. В этих выводах, одобренных на пленарном заседании, говорилось буквально следующее: «Радиовещательная станция, функционирующая на борту воздушного судна и транслирующая передачи исключительно на территорию другой администрации без согласия последней, не может считаться работающей в соответствии с Регламентом радиосвязи».

Эти выводы имеют обязательную юридическую силу для работы Международного союза электросвязи. Таким образом, Всемирная конференция радиосвязи подтвердила заключение, сделанное в 1990 году тогдашним Международным комитетом регистрации частот, согласно которому трансляция с борта аэростата телепередач на национальную кубинскую территорию представляет собой нарушение положений Регламента.

На 54-м совещании Радиорегламентарного комитета Международного союза электросвязи, состоявшемся в июле 2010 года, было принято следующее решение:

> Внимательно изучив доклад Директора и сообщение администрации Кубы (документ RRB10-2/3 (Add.1)), Комитет выразил сожаление по поводу продолжающихся помех работе радиовещательных станций Кубы в результате трансляций, ведущихся Соединенными Штатами, и постановил придерживаться своих решений в этой связи.
>
> Комитет также принял к сведению просьбу «Бюро в его качестве исполнительного секретариата Комитета» о том, чтобы вопрос о вредных помехах работе кубинских радиостанций, вещающих в метровом и дециметровом диапазонах, был включен в повестку дня следующей Полномочной конференции. Признав суверенное право каждой администрации поднимать любой вопрос на Полномочной конференции, Комитет подтвердил, что два представителя Радиорегламентарного комитета на Полномочной конференции 2010 года и его исполнительный секретариат готовы предоставить всю необходимую информацию и консультации, которые могут потребоваться от них на следующей Полномочной конференции.

Что касается последних событий, то в феврале 2012 года Всемирная конференция радиосвязи поручила директору Бюро радиосвязи Международного союза электросвязи обеспечить последующую деятельность и информировать следующую Конференцию, которая состоится в 2015 году, о тех помехах, которые правительство Соединенных Штатов чинит кубинским радио- и телевизионным службам своими актами радиоэлектронной агрессии.

Таким образом Конференция подтвердила правомерность своего предыдущего заключения, признающего незаконность антикубинских радио- и теле-

передач, транслируемых властями Соединенных Штатов с помощью воздушных судов.

Враждебное отношение правительства Соединенных Штатов Америки к Кубе проявляется и в сохранении на протяжении более чем 50 лет экономической, торговой и финансовой блокады, которая не обходит стороной и сферу информации и телекоммуникаций.

- Сектор информатики и коммуникаций значительно пострадал в результате воздействия блокады. В 2010–2011 годах сумма ущерба, согласно оценкам, составила порядка 7 396 394 долл. США.
- Куба по-прежнему не имеет доступа к услугам, предоставляемым большим количеством веб-сайтов, которые блокируют доступ при установлении факта соединения с IP-адресом, принадлежащим кубинскому домену ".cu".
- Со всем цинизмом и лицемерием, на которые они способны, Соединенные Штаты продолжают несправедливо обвинять Кубу в том, что она закрывает своим гражданам доступ в глобальную сеть, тогда как в реальности дело обстоит совершенно иначе: из-за блокады, введенной правительством Соединенных Штатов Америки, Куба не в состоянии подключиться к волоконно-оптическим кабелям, окружающим кубинский архипелаг, и вынуждена приобретать дорогостоящие услуги спутниковой связи.
- 6 октября 2010 года социальная сеть «Твиттер» взяла на себя полную ответственность за то, что она осуществила блокирование сообщений с помощью мобильных средств связи с Кубы в адрес своей платформы. Аналогичным образом в апреле 2011 года стало известно о том, что для Кубы ограничивается доступ к определенным средствам использования «Твиттера» под аргументом, что доступ осуществляется из страны, подпадающей под запрет.
- Начиная с февраля 2011 года финансовая компания «Синеверс» прекратила осуществление платежей в адрес кубинской телекоммуникационной компании (ЭТЕКСА) по статье «роуминг» для мобильной телефонной связи, сославшись на то, что ее банк не может осуществлять сделки с Кубой, что подразумевает утрату поступлений в размере порядка 2,6 млн. долл. США, наряду с возникновением дополнительных трудностей.

Дискуссии в Генеральной Ассамблее Организации Объединенных Наций, посвященные достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, весьма важны и актуальны. Действия, подобные вышеописанной практике правительства Соединенных Штатов Америки в отношении Кубы, подтверждают необходимость таких дискуссий и важность принятия мер с целью положить конец подобным действиям.

Куба поддержала резолюцию 66/24 Генеральной Ассамблеи и будет и далее прилагать усилия для содействия мирному глобальному развитию информационных и телекоммуникационных технологий и их применению на благо всего человечества.

Панама

[Подлинный текст на испанском языке]
[10 июля 2012 года]

Экономика XXI века во все большей степени базируется на секторе услуг, что особенно заметно в экономике развитых стран. Электронная торговля — всего лишь наиболее недавнее проявление этого сектора экономики, облегчающее коммерческие операции, сокращающее средства и время, затрачиваемые на поставки товаров и услуг по всему миру. Электронное правительство — это государственный вариант электронной торговли, позволяющий государствам быстро и эффективно рассматривать большое количество заявлений от граждан государств с помощью различных технологий (Интернета и мобильной связи).

Поскольку для поддержки электронной торговли и управления электронными сетями широко применяются информационно-коммуникационные технологии, необходимо прилагать усилия с тем, чтобы вышеупомянутые технологии соответствовали минимальным требованиям конфиденциальности, неприкосновенности и доступности, предъявляемым клиентами и гражданами государств. Вместе с тем множество прилагаемых сегодня усилий сосредоточено на технических решениях глобальных проблем, что требует рассмотрения проблемы с различных углов зрения.

По нашему мнению, развитие правовых рамок, основанных на международных стандартах, ранее принятых другими государствами и имеющих широкое международное признание, должно быть задачей номер один для государств, желающих поощрять функционирование электронной торговли и управление электронным пространством при одновременном создании враждебной среды для преступников и террористов, использующих эти средства для осуществления своей деятельности. Обеспечив благоприятные условия для функционирования электронной торговли и управления электронным пространством, рассчитывать на получение экономических благ могут лишь те страны, которые принимают меры правовой и технической защиты в этой сфере.

В то же время следует продолжать усилия, направленные на разработку технологий и стратегий защиты киберпространства государств, в котором пересекаются интересы различных стран, посредством национальных стратегий кибербезопасности, которые могут осуществляться в реально установленные сроки. Эти стратегии, способствующие международному миру, должны быть к тому же нацелены на сохранение национальной безопасности и стабильности стран.

Меры, принимаемые Панамой на национальном уровне в целях укрепления информационной безопасности и содействия международному сотрудничеству, состоят в следующем:

a) создание Национального центра реагирования на инциденты, исполнительный декрет № 709 от 26 сентября 2011 года;

b) пересмотр основополагающего закона (Уголовный кодекс) в целях включения новых уголовных деяний, связанных с киберпреступлениями, и его

последующая передача в Национальную ассамблею депутатов для утверждения (проект закона № 377);

c) обсуждение и пересмотр Уголовно-процессуального кодекса в целях приведения его в соответствие с новыми деяниями, включенными в Уголовный кодекс;

d) учреждение рабочей группы для обсуждения ответственности провайдеров Интернет-доступа в сфере информационной безопасности — группы, возглавляемой Национальным органом по правительственным инновациям и Национальным органом по коммунальным услугам. Обсуждается также применение результатов работы этой дискуссионной группы на региональном уровне (Техническая комиссия по электросвязи Центральной Америки/Международный союз электросвязи) с помощью национальных регулятивных механизмов Центральноамериканского региона;

e) Рабочая группа по управлению цифровыми доказательствами, возглавляемая министерством общественных работ при участии Национального органа по правительственным инновациям;

f) оформление заявления о технической помощи в разработке национальной стратегии кибербезопасности, направляемого в Организацию американских государств (ОАГ);

g) курсы повышения квалификации на тему «Управление инцидентами», организованные ОАГ/Координационным центром Группы реагирования на нарушения компьютерной защиты и проведенные в Панаме в апреле;

h) оценка предложения Управления Организации Объединенных Наций по наркотикам и преступности по программе укрепления возможностей Панамы в деле борьбы с киберпреступностью;

i) регулярное участие в совещаниях министров юстиции и других министров, обвинителей или генеральных прокуроров стран Северной и Южной Америки и Межамериканского комитета по борьбе с терроризмом;

j) официальное заявление о присоединении к Будапештской конвенции о киберпреступности, содержащееся в ноте от 31 января 2012 года, направленной министром иностранных дел Карлосу Аросемене, послу Панамы в Брюсселе.

Что касается мер, которые международное сообщество могло бы принять в целях укрепления безопасности информации в глобальном масштабе, то, по нашему мнению, следует учесть следующие рекомендации:

a) принятие общей правовой основы, позволяющей осуществлять сотрудничество между государствами посредством оперативного оказания взаимной правовой помощи на основе общепризнанных международных процедур;

b) разработка национальных и региональных стратегий кибербезопасности;

c) содействие нормализации обмена информацией между государствами через национальные центры реагирования на инциденты, позволяющие

обеспечить регулярное поступление информации, особенно относящейся к преследованию преступности и терроризма;

d) разработка программ информационно-разъяснительной работы относительно местных и международных норм, применимых к каждому государству.

Катар

[Подлинный текст на английском языке]
[18 мая 2012 года]

Национальные усилия Государства Катар в сфере информационной безопасности основаны на комплексном подходе, предполагающем учет как относящихся к информационной безопасности ресурсов, так и безопасности физических лиц, использующих эти ресурсы. Эта стратегия приведена в соответствие с концепцией развития Катара до 2030 года, основными составляющими которой являются развитие человеческого потенциала, социальное и экономическое развитие, а движущей силой — такие международные инициативы, как Глобальная повестка дня в области кибербезопасности Международного союза электросвязи и Основные принципы защиты информационной инфраструктуры Большой восьмерки.

В настоящее время национальная программа кибербезопасности в Катаре (Катарская группа реагирования на связанные с компьютерами чрезвычайные ситуации, Инициатива центра информационной безопасности по передаче передового опыта) — финансируемая правительством организация, действующая под эгидой Верховного совета по информационно-коммуникационным технологиям, — составляет краеугольный камень повестки дня Катара в области кибербезопасности, которая включает ведомства по защите информационной структуры и отделения по выполнению задач правительства в области ИКТ.

Катарская группа реагирования на связанные с компьютерами чрезвычайные ситуации взаимодействует с правительственными учреждениями, организациями государственного и частного сектора и с гражданами Катара, с тем чтобы обеспечить контроль за онлайновыми угрозами и сокращение рисков. В установленную практику исследования угроз входят передовая цифровая криминалистическая экспертиза, анализ вредоносного программного обеспечения и возможности систем контроля за угрозами, а также каналы усиления готовности в сфере безопасности и реагирования посредством программ практической подготовки. Ниже приводится краткое описание ее функций.

Разведывательная деятельность в связи с угрозами

Оперативный центр по обеспечению безопасности. Аналитики по вопросам безопасности с помощью разработанных силами центра инструментов (системы контроля за угрозами) будут в порядке профилактики предупреждать правительственные учреждения и ключевые организации об угрозах, связанных с инструментами удаления вирусов.

Система контроля за угрозами. Эта система является комплексным инструментом, который агрегирует и анализирует разведданные об угрозах, посту-

пающие из различных источников, с тем чтобы выявлять и смягчать воздействие зараженных компьютеров или местных веб-сайтов.

Лаборатория по анализу вредоносного программного обеспечения

Цель лаборатории состоит в том, чтобы создать потенциал для измерения и анализа связанных с вредоносным программным обеспечением угроз и предоставления защиты от них на национальном уровне. В настоящее время лаборатория занимается подготовкой подробного доклада о воздействии вредоносного программного обеспечения на зараженные машины, о видах поражаемых систем, о существующих в стране источниках вредоносного программного обеспечения и о любой Интернет-связи с командно-контрольным сервером. Она также оказывает помощь в оценке всего собранного вредоносного программного обеспечения с целью определить риск, связанный с поступающими от такого обеспечения угрозами, исходя из объема такого вредоносного обеспечения и гарантировать его обнаружение с помощью всех существующих на рынке антивирусных систем.

Государственное урегулирование инцидентов

Цель Катарской группы реагирования на связанные с компьютерами чрезвычайные ситуации — свести к минимуму число зараженных машин в Государстве Катар посредством оказания существенной поддержки обществу и ключевым отраслям. Для того чтобы достичь этой цели и обеспечить надлежащее руководство, Катар расширил свою службу реагирования на инциденты, охватив пользователей асимметричных цифровых абонентских линий через государственный портал урегулирования инцидентов. Этим обеспечиваются различные меры, руководящие принципы и базовые инструменты программного обеспечения для отслеживания и удаления вирусов из главных машин асимметричных цифровых абонентских линий.

Учебная подготовка по кибербезопасности

Катарская группа реагирования на связанные с компьютерами чрезвычайные ситуации проводит учебные мероприятия и практикумы по кибербезопасности для профессионалов в сфере информационных технологий из правительственных организаций и из других стран Совета сотрудничества стран Залива.

Информированность о кибербезопасности

Катарская группа реагирования на связанные с компьютерами чрезвычайные ситуации создает базу знаний и передовых видов практики по вопросам кибербезопасности, уделяя особое внимание корпоративным служащим.

В задачи Группы входит защита важнейших объектов инфраструктуры в связи с тем, что ряд отраслей, таких как финансы, энергетика и информационно-коммуникационные технологии, играют ключевую роль в поддержании стабильности экономики, населения и правительства Катара. В этой связи Группа стремится обеспечить защиту информационных систем, на которые опираются эти важнейшие отрасли, с помощью следующих мер:

- разработка национальных стратегий защиты, рамочных основ и методов передовой практики и повышение осведомленности заинтересованных сторон;
- создание непосредственного содействия владельцам и операторам важнейших объектов инфраструктуры в улучшении сетевых гарантий системы надзора, контроля и получения данных (SCADA);
- понимание отраслевых проблем и взаимозависимых явлений по отраслям, а также осуществление специальных отраслевых стратегий защиты;
- взаимодействие с организациями по защите отраслевой информационной инфраструктуры с целью поиска транснациональных решений;
- оценка подготовленности организаций по защите отраслевой информационной инфраструктуры в стране и оценка достигнутого прогресса.

Кроме того, программа кибербезопасности Верховного совета по информационно-коммуникационным технологиям продолжает работать совместно с законодательным органом над проектами законов и стандартов с целью постоянного повышения в стране гарантий противодействия возникающим в современном мире угроз.

Верховный совет рекомендует принять и разработать с участием международного сообщества следующие возможные меры:

- создание в течение пяти лет международных правовых рамок, согласованных на региональном уровне во всех странах;
- создание в течение трех лет групп реагирования на связанные с компьютерами чрезвычайные ситуации во всех странах, в которых в настоящее время еще нет таких групп;
- разработка в течение пяти лет национальных стратегий кибербезопасности в соответствии с принципами международного сотрудничества, в том числе в деле защиты важнейших объектов информационной инфраструктуры;
- разработка учебной программы по кибербезопасности, направленной на укрепление потенциала и повышение осведомленности среди различной клиентуры (например, правительственные органы, академические круги, частный сектор, учебные заведения);
- уделение особого внимания программам повышения осведомленности молодежи о программах онлайновой защиты.

Турция

[Подлинный текст на английском языке]
[31 мая 2012 года]

Информационно-коммуникационные технологии стремительно проникают как в ежедневную жизнь, так и в коммерческие процессы. Различные данные, имеющие важнейшее значение для физических лиц, институтов или правительств, хранятся в цифровом формате и передаются в киберпространстве. При всех преимуществах этих технологий они сопряжены с определенным

риском с точки зрения обеспечения конфиденциальности и неприкосновенности сохраняемых в цифровом формате данных и доступности информационных систем. Уязвимость информационно-коммуникационных систем, которая является следствием недоработок в их дизайне, конфигурации и функционировании, а также недостаточных технических возможностей и отсутствия подготовки или осведомленности в вопросах безопасности у служащих и пользователей, создает подходящую среду для реального возникновения этих рисков.

С тем чтобы не допускать или смягчать воздействие рисков и компенсировать факторы уязвимости, необходимо предпринимать на национальном и институциональном уровнях усилия по развитию кибербезопасности. В этой связи важной составляющей таких усилий считается укрепление административно-технического потенциала и повышение осведомленности о вопросах безопасности среди администраторов, сотрудников и пользователей в государственных и частных учреждениях.

Администраторы высокого уровня в турецком правительстве хорошо осведомлены о необходимости повышения национальной информационной безопасности. Кроме того, Информационно-коммуникационная администрация Турции уделяет конкретное внимание изучению передовых видов практики и возникающих угроз в киберпространстве, занимаясь организацией и проведением национальных учебных мероприятий по кибербезопасности, что повышает институциональный и технический потенциал по реагированию на чрезвычайные ситуации; и Администрация регулярно проводит ревизии работы операторов электронной связи с целью обеспечить наличие соответствующих стратегий, процессов, программ и механизмов контроля для надлежащего регулирования инцидентов, связанных с безопасностью электронной связи.

Существует мнение, что для укрепления безопасности глобальных информационно-коммуникационных систем важное значение имеет изучение международных концепций, касающихся глобальных угроз, конкретных факторов уязвимости информационных систем и передовых видов практики в том, что касается информационных механизмов, а также обмена специальными знаниями с другими международными организациями.

Полезными инструментами укрепления глобальной информационной безопасности могли бы стать многосторонние конвенции о сотрудничестве в деле урегулирования инцидентов с информационно-коммуникационной безопасностью в киберпространстве и о криминалистическом подходе к ним, а также об обмене информацией о базах данных по вредоносному программному обеспечению.

Украина

[Подлинный текст на русском языке]
[31 мая 2012 года]

Общая оценка проблем информационной безопасности

Стремительное внедрение информационных и коммуникационных технологий (ИКТ) во все сферы жизнедеятельности, глобализация информационных отношений обуславливают появление мировой тенденции к перемещению про-

тивоправной деятельности в виртуальное пространство. Сегодня компьютерная преступность, или иными словами — киберпреступность, для которой не существует государственных границ, угрожает не только правам и свободам граждан, но и посягает на национальные интересы и безопасность государств.

На протяжении последних лет наметилась устойчивая тенденция к увеличению проявлений компьютерных атак на важные объекты национальных инфраструктур государств, что повлекло нанесение ущерба странам в связи с искажением важной для них информации, блокированием производственных процессов на объектах промышленности, жилищно-коммунального хозяйства, транспорта, энергетического обеспечения.

Оценка ситуации в сфере киберпреступности в 2011 году в отдельных государствах, где объектами хакерских атак стали информационные системы государственных органов и институций, что в свою очередь повлекло фактическое блокирование их деятельности, свидетельствует о масштабности угроз для общества и непредсказуемости негативных последствий вследствие кибератак.

Усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области

Опыт противодействия указанным угрозам в отдельных развитых странах свидетельствует о создании общегосударственных систем по борьбе с киберпреступностью во главе с единым координационным органом. При этом обеспечивается оперативная аккумуляция сил и средств компетентных государственных и негосударственных органов для противодействия и нейтрализации угроз информационной безопасности.

Указанный аспект стал одним из определяющих при пересмотре подходов к оценке новых вызовов и угроз, в частности, в информационной сфере, осуществлении мероприятий, инициированных на высоком политическом уровне государства, по созданию единой общегосударственной системе противодействия киберпреступности, разработке проекта Закона Украины «О кибернетической безопасности», установлению и укреплению партнерского взаимодействия с иностранными спецслужбами и правоохранительными органами.

В июне 2011 года совместно с правоохранительными органами 11 государств (Соединенные Штаты Америки, Германия, Нидерланды, Великобритания, Латвия, Кипр, Франция, Литва, Румыния, Канада, Швеция) Служба безопасности Украины прекратила преступную деятельность международной хакерской группировки. Путем распространения сетью Интернет вредоносного программного обеспечения указанная группировка осуществила кражу из иностранных банковских структур более 72 млн. долл. США.

В октябре 2011 года Служба безопасности Украины организовала и провела в Ялте, Украина, ежегодные консультации экспертов Украина-Организация Североатлантического договора по вопросам кибернетической защиты, по результатам которых была поддержана позиция украинской стороны касательно необходимости дальнейшего развития системы информационной безопасности при участии государственного и частного секторов с привлечением опыта других государств.

По инициативе Службы безопасности Украины, в рамках работы 32-го заседания Совета руководителей органов безопасности и спецслужб государств — участников СНГ планируется рассмотреть вопрос о создании отдельной Комиссии по вопросам информационной безопасности.

Содержание концепций, упомянутых в пункте 2 резолюции 62/24 Генеральной Ассамблеи

Согласно законодательству Украины определены такие основные угрозы национальной безопасности, в том числе в информационной сфере:

- проявления ограничения свободы слова и доступа граждан к информации;
- компьютерная преступность и компьютерный терроризм;
- разглашение информации, которая является государственной либо другой, предусмотренной законодательством, тайной, а также конфиденциальной информации, которая является собственностью государства либо направлена на обеспечение национальных потребностей и интересов общества и государства;
- попытки манипулирования общественным сознанием, в частности путем распространения недостоверной, неполной либо предвзятой информации.

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

Основой обеспечения информационной безопасности международного сообщества является создание условий для обеспечения информационной безопасности отдельных государств и развитие их эффективного сотрудничества в этой области.

Механизмы реализации эффективного противодействия существующим и потенциальным угрозам информационной безопасности предусматривают осуществление следующих мероприятий международного сотрудничества:

- введение в практику консультативных механизмов сотрудничества в сфере кибернетической защиты с целью обмена опытом относительно законодательного обеспечения и регулирования в указанной сфере;
- налаживание системы обмена информацией о мониторинге киберпространства и системы оперативного оповещения о начале кибератак, обмена информацией о технических аспектах кибератаки, обнаружения их источников и выбора эффективных мер противодействия;
- сотрудничество в целях устранения негативных последствий кибератак, обобщения опыта, наработка технических решений и организационных рекомендаций относительно избежания кибератак;
- разработка международных правовых актов, направленных на установление единой терминологии и правил, например Кодекса поведения в Интернете и т.д.

В связи с необходимостью противодействия указанным угрозам необходимым видится организация взаимодействия с партнерскими спецслужбами и правоохранительными органами по следующим направлениям:

- отработка механизмов оперативного обмена ведомостями между спецслужбами касательно действий со стороны организованных преступных группировок, в том числе террористического характера, направленных на несанкционированное вмешательство в информационные ресурсы национальных сегментов в сети Интернет, информационные системы государственных и коммерческих учреждений;
- обмен информацией относительно преступлений, связанных с использованием несанкционированного доступа к компьютерным системам финансовых заведений, в частности про подделки банковских платежных корточек, несанкционированное вмешательство в работу банковских компьютерных систем с целью хищения конфиденциальной информации или блокирования ее работы;
- организация взаимодействия во время розыска лиц, совершающих компьютерные преступления с использованием национальных сегментов сети Интернет и документирование их противоправной деятельности;
- обмен опытом и имеющимися наработками в сфере программно-технических (судебно-кибернетических) экспертиз в процессе расследования преступлений, осуществляемых с использованием компьютерных технологий, методов и методики исследования компьютерной техники с целью документирования преступной деятельности;
- внедрение совместных учебных программ по подготовке квалифицированных кадров и проведения стажировок экспертов спецслужб;
- участие в совместных симпозиумах, семинарах и конференциях по вопросам противодействия киберпреступности.

Одним из вариантов сотрудничества в этом направлении может стать формирование систем мониторинга ресурсов национальных сегментов сети Интернет в целях своевременного выявления угроз, а также поиска оптимальных средств их нейтрализации.

С целью координации действий в части компьютерной безопасности государственных органов, операторов связи а также других субъектов национальной информационной инфраструктуры по вопросам предупреждения правонарушений в сфере использования компьютерных и информационных технологий, одним из возможных механизмов могло бы стать создание и тесное взаимодействие Национальных центров реагирования на компьютерные инциденты.

При этом среди основных задач таких национальных центров можно было бы выделить такие, как:

- сбор, анализ и накопление в соответствующих базах данных информации о современных угрозах компьютерной безопасности;
- технический мониторинг и выявления механизмов и ресурсов сети Интернет, которые функционируют с нарушением нормативно-правовых ак-

тов, регулирующих деятельность участников национального сегмента сети Интернет;

- выработка рекомендаций пользователям Интернета по обеспечению защиты интересов человека, общества и государства в информационной сфере, а также касательно предоставления консультативных услуг и технической поддержки пользователям;
- оперативный прием сообщений и предоставление экстренной помощи для прекращения хакерских атак, своевременное оповещение пользователей сети Интернет и других информационных систем, в том числе локальных и корпоративных, об угрозах компьютерной безопасности, которые возникают;
- взаимодействие и обмен информацией с аналогичными центрами в других странах.