Организация Объединенных Наций A/65/154

Генеральная Ассамблея

Distr.: General
20 July 2010
Russian
Original: English/Russian/Spanish

Шестьдесят пятая сессия
Пункт 94 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

Содержание

* A/65/150.

10-45844 (R) 210710 160810

I. Введение

1. В пункте 3 своей резолюции 64/25 Генеральная Ассамблея просила все государства-члены продолжать информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

a) общая оценка проблем информационной безопасности;

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

c) содержание 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 26 февраля 2010 года государствам-членам была направлена вербальная нота, в которой им предлагалось представить информацию по этому вопросу. Полученные ответы приводятся в разделе II ниже. Любые ответы, полученные дополнительно, будут опубликованы в качестве добавлений к настоящему докладу.

II. Ответы, полученные от правительств

Куба

[Подлинный текст на испанском языке]
[27 мая 2010 года]

1. Куба полностью разделяет выраженную в резолюции 64/25 обеспокоенность тем, что информационные технологии и другие средства могут быть использованы в целях, не совместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на целостность инфраструктуры государств, а также нанести ущерб безопасности в гражданской и военной сферах. Кроме того, в этой резолюции совершенно справедливо подчеркивается необходимость предотвращения использования информационных ресурсов или технологий в преступных или террористических целях.

2. Куба вновь заявляет, что враждебное использование телекоммуникаций с открытой или тайной целью подрыва правового и политического строя государств является нарушением международно признанных норм в этой сфере и неправомерной и безответственной формой применения этих средств, последствия которого могут стать причиной напряженности и нанести ущерб международному миру и безопасности, а также принципам и целям, провозглашенным в Уставе Организации Объединенных Наций.

3. Куба с обеспокоенностью отмечает, что информационно-коммуникационные системы могут быть превращены в оружие, если они будут разрабатываться и/или применяться с целью нанести ущерб инфраструктуре госу-

дарств, и впоследствии могут поставить под угрозу международный мир и безопасность.

4. В этой связи Республика Куба считает необходимым заявить, как она уже делала это на различных международных форумах, о своем осуждении агрессивной эскалации информационной войны против Кубы, которую развязало и ведет руководство Соединенных Штатов, открыто попирая международные нормы, регулирующие использование радиочастот.

5. Правительство Соединенных Штатов не компенсировало того ущерба, который оно могло нанести международному миру и безопасности путем создания опасных ситуаций, в том числе использования военных самолетов для трансляции телевизионных сигналов на Кубу без ее согласия.

6. Радиоэлектронная агрессия, развязанная в отношении Кубы с территории Соединенных Штатов, идет вразрез с принципами международного права, регулирующими отношения между государствами, а также нормами и правилами Международного союза электросвязи (МСЭ), в которых определены принципы поведения стран-членов этого специализированного учреждения системы Организации Объединенных Наций.

7. Еженедельно находящиеся на территории Соединенных Штатов станции транслируют на Кубу тысячи часов радио- и телепередач на 34 различных частотах в длинном, среднем, коротком и ультракоротком диапазоне. В марте 2010 года общая продолжительность незаконного еженедельного вещания составила 2156 часов. Некоторые из таких станций принадлежат и оказывают свои услуги организациям, связанным с известными террористическими элементами, находящимися на американской территории или действующими против Кубы с этой территории при полном согласии властей Соединенных Штатов Америки.

8. Направленные против Кубы незаконные радио- и телепередачи не содержат никакой информации; напротив, в подрывных целях они передают ложные и искаженные сведения. Ежегодно конгресс Соединенных Штатов Америки выделяет для этой цели свыше 30 млн. долл. США из федерального бюджета. С момента создания обеих вещательных станций американское правительство потратило на эти цели 659,8 млн. долл. США.

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

– основополагающими принципами Международного союза электросвязи, которые сформулированы в преамбуле к его уставу и в которых говорится 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 Шатов Америки на Кубу, носят подрывной, дестабилизирующий характер и искажают реальное положение дел в нарушение указанных принципов;

– положениями 197 и 198 устава Международного союза электросвязи, в которых говорится, что все станции, независимо от их назначения, долж-

ны устанавливаться и эксплуатироваться таким образом, чтобы не причинять вредных помех радиосвязи или радиослужбам других членов Союза;

– соглашением, подписанным в ходе 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»;

– пунктом 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;

– пунктом 42.4 статьи 42 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;

– решением Радиорегламентарного комитета, который на своем 35-м заседании в декабре 2004 года констатировал наличие вредных помех, создаваемых этими передачами для кубинских вещательных служб на частоте 213 МГц, и потребовал, чтобы администрация Соединенных Штатов Америки приняла необходимые меры для их прекращения. Кроме того, с сентября 2006 года Радиорегламентарный комитет обращается к администрации Соединенных Штатов Америки с призывами принять меры для устранения помех на частоте 509 МГц, однако никакой реакции на эти призывы до сих пор не последовало. 20 марта 2009 года на 50-м заседании Комитета было принято решение, которое получило отражение в резюме решений (документ RRB09-1/5) и в котором было вновь указано на незаконность такого вещания, а к администрации Соединенных Штатов Америки обращена просьба принять все необходимые меры с целью прекращения создания помех телевизионным службам Кубы на указанных двух частотах. 26 марта 2010 года на 53-м заседании Радиорегламентарного комитета МСЭ был вновь подтвержден его вывод о том, что вещательные станции Соединенных Штатов Америки создают вредные помехи для деятельности кубинских вещательных станций, зарегистрированных в Международном реестре радиочастот и к администрации Соединенных Штатов обращен призыв прекратить эти вредные помехи, а Управлению было поручено держать под контролем эту ситуацию и действовать в соответствии с процедурами, изложенными в Регламенте радиосвязи;

– пунктом 23.3 статьи 23 Регламента радиосвязи МСЭ, которым налагаются ограничения на телевещание за пределами национальных границ.

10. В докладе, опубликованном в январе 2009 года Главным контрольным управлением правительства Соединенных Штатов Америки (официальное ведомство этой страны), признаются нарушения международных норм и внутреннего законодательства, допущенные в программах радио- и телевещания правительства Соединенных Штатов на Кубу:

– в нем отмечается, что в 2004 и 2006 годах Международный союз электросвязи указал, что телевещание на 13-м и 20-м каналах создает вредные помехи для кубинских вещательных станций и что государственный департамент не принял никаких мер в ответ на соответствующую просьбу МСЭ. Кроме того, в докладе указывалось, что Международная конференция радиосвязи, состоявшаяся в ноябре 2007 года, приняла решение о том, что вещание, осуществляемое с борта воздушного судна, не соответствует положениям МСЭ;

– было признано, что, хотя законами Соединенных Штатов запрещается внутренняя трансляция таких передач, и радио- и телепередачи могут приниматься на территории Соединенных Штатов Америки, прежде всего в Майами, и что было зафиксировано существование вещательных станций, передающих платные политические сообщения и материалы сексуального характера. Кроме того, было отмечено, что вещание на Кубу не соответствует требованиям сбалансированности и объективности, предъявляемым к деятельности журналистов, и содержит подстрекательские и оскорбительные высказывания.

11. Куба также напоминает 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 которых трансляции, ведущиеся с борта воздушных судов Соединенных Штатов на Кубу, были признаны не соответствующими Регламенту радиосвязи. В этих заключениях, утвержденных на пленарном заседании, говорилось буквально следующее: «Радиовещательная станция, которая функционирует на борту воздушного судна и транслирует передачи исключительно на территорию другого государства без согласия последнего, не может считаться соответствующей Регламенту радиосвязи».

12. Эти заключения были приняты на пленарном заседании ВКР-07 и имеют обязательную силу для МСЭ. Таким образом, Всемирная конференция радиосвязи подтвердила решение, принятое в 1990 году Международным комитетом регистрации частот, согласно которому трансляция с борта аэростата телевизионных передач на национальную кубинскую территорию противоречит положениям Регламента.

13. Враждебная позиция правительства Соединенных Штатов Америки по отношению к Кубе выражается в сохранении на протяжении уже более 50 лет экономической, торговой и финансовой блокады, которая также затрагивает и сферу информации и телекоммуникаций:

– Куба не имеет возможности доступа ко многим веб-сайтам, обращение к которым блокируется в том случае, если запрос поступает с интернет-адреса, относящегося к кубинскому домену .cu;

– на основании решения Управления по контролю за иностранными активами были без предварительного уведомления заблокированы домены .com, имеющие отношение к Кубе;

– в силу введенных правительством Соединенных Штатов Америки законов об осуществлении экономической, торговой и финансовой блокады Куба не в состоянии пользоваться оптико-волоконными кабелями, окружающими кубинский архипелаг, и вынуждена оплачивать услуги спутниковой

связи, которая имеет ограниченную пропускную способность, что является серьезным препятствием для получения необходимых технологий и сопряжено с большими расходами;

– Интернет используется для проведения направленных против Кубы клеветнических кампаний, имеющих подрывные цели и направленных на дискредитацию страны.

14. Такая позиция вступает в противоречие с намерениями, позициями и решениями всех стран мира, изъявленными в ходе Всемирной встречи на высшем уровне по вопросам информационного общества, состоявшейся в Швейцарии и в Тунисе в 2003 и 2005 годах.

15. Эта встреча настоятельно призвала государства при строительстве информационного общества принимать необходимые положения, с тем чтобы не допускать и воздерживаться от принятия односторонних мер, идущих вразрез с международным правом и Уставом Организации Объединенных Наций, а также создающих помехи полному достижению целей социально-экономического развития населения соответствующих стран и наносящих ущерб благосостоянию их граждан.

16. Проходящие в Генеральной Ассамблее Организации Объединенных Наций дискуссии по вопросу о достижениях в сфере информации и телекоммуникаций в контексте международной безопасности весьма актуальны и с каждым днем приобретают все более своевременный и важный характер. Перечисленные выше действия Соединенных Штатов Америки, направленные против Кубы, подтверждают необходимость таких обсуждений и свидетельствуют о безотлагательной необходимости принятия мер для прекращения указанных действий.

17. Куба решительно поддерживает работу Генеральной Ассамблеи Организации Объединенных Наций в этой сфере и будет и далее прилагать максимум усилий для содействия мирному развитию информационно-коммуникационных технологий во всем мире и их применению на благо всего человечества. Кроме того, она готова сотрудничать со всеми остальными странами, в том числе и с Соединенными Штатами Америки, в деле изыскания решений, которые позволят преодолеть препятствия, мешающие достижению указанных целей.

Греция

[Подлинный текст на английском языке]
[28 июня 2010 года]

1. Вопросам информационной безопасности уделяется все большее внимание. Во всех случаях принимаются меры для противодействия современным угрозам, возникающим вследствие глобализации сетей и систем. Разрабатываются и осуществляются меры для защиты свободного распространения информации на национальном и трансграничном уровнях.

2. Отслеживаются и анализируются современные международные и многонациональные концепции. Необходимо разработать международные рекомендации для оценки существующих рисков. Кроме того, нужно заняться решением вопросов обеспечения защиты в киберпространстве. Еще одна задача за-

ключается в сохранении национальных суверенных прав на информационную безопасность в процессе глобального информационного обмена.

3. Государства-члены должны продолжать информировать Генерального секретаря о своей точке зрения и об оценках по соответствующим вопросам. В этой связи необходимо отметить следующее:

a) все вопросы обеспечения информационной безопасности имеют большое значение;

b) необходимо принимать меры для изучения и обеспечения возможностей свободного обмена информацией на национальном и трансграничном уровнях при сохранении необходимого уровня конфиденциальности, целостности и доступности информации;

c) необходимо разработать и согласовать концепции межсетевого обмена данными, которые бы предусматривали единые возможности как на национальном, так и на международном уровне. Нужно уделять особое внимание оценке рисков, возникающих в процессе межсетевого обмена данными, и разработать соответствующие международные рекомендации. Кроме того, поскольку всем странам приходится самым серьезным образом заниматься принятием мер для защиты своего киберпространства, необходимо разработать согласованные международные рекомендации по вопросам сотрудничества и в целях обеспечения эффективности и экономичности осуществляемой деятельности. Наконец важно отметить, что при разработке любой концепции нужно учитывать право стран на сохранение своего суверенитета и собственной информационной базы;

d) международное сообщество могло бы принять следующие меры для укрепления информационной безопасности на глобальном уровне:

1) детальная разработка и согласование соответствующих международных концепций;

2) разработка директивного плана создания согласованной общей инфраструктуры, который бы охватывал и вопросы базового законодательства, в целях обеспечения необходимой информационной безопасности в процессе электронной обработки различной корреспонденции и сообщений для пользователей, прошедших соответствующую сертификацию;

3) согласование концепций, которых придерживаются многонациональные объединения и группы малых государств, и их адаптация для глобальных условий. Достигнутые договоренности в отношении определения характера угроз и их негативных последствий должны предусматривать не только разработку самых современных технических средств, но и меры для их защиты от злоумышленников;

4) в дополнение к перечисленным выше мерам необходимо учитывать, что любые действия в направлении глобализации должны основываться в качестве основополагающего условия на суверенитете стран. Необходимо разработать международную концепцию для определения национальных каналов информационного обмена, а также соответствующие сценарии, отражающие желаемый уровень интеграции, и использовать такую концепцию в качестве руководства для

всех усилий, прилагаемых на национальном, межнациональном и международном уровнях.

Мексика

[Подлинный текст на испанском языке]
[18 мая 2010 года]

Общий анализ проблем в сфере информационной безопасности

1. В нашей стране банковские и финансовые учреждения, а также федеральные ведомства, занимающиеся вопросами обеспечения общественной и национальной безопасности, прилагают наибольшие усилия в сфере информационной безопасности. Для борьбы с киберпреступлениями, угрожающими общественной безопасности, в министерстве общественной безопасности существуют подразделения по борьбе с киберпреступностью и интернет-полиция.

2. С другой стороны, хотя все три ветви государственной власти прилагают отдельные усилия для борьбы с преступностью в киберпространстве, на уровне федерального правительства не существует политики обеспечения безопасности в киберпространстве, которая бы направляла стратегии борьбы с киберпреступностью в стране; необходимо укрепить законодательство в этой сфере и укрепить инструментарий судебной власти, который позволил бы ей бороться с киберпреступностью и наказывать виновных; укрепить регулирование компаний, обеспечивающих доступ к интернету, таким образом, чтобы они вели учет деятельности, осуществляемой на предоставляемой ими платформе, и предоставляли необходимые сведения в условиях возможных инцидентов. Кроме того, необходимо принять внутренние договоренности и подписать соглашения о сотрудничестве с другими странами по борьбе с преступностью и терроризмом в киберпространстве, которые угрожают национальной безопасности.

Принимаемые на национальном уровне меры для укрепления информационной безопасности и международного сотрудничества в этой сфере

3. В Мексике приняты следующие меры для обеспечения информационной безопасности:

a) криминализация некоторых киберпреступлений в следующих документах: Федеральный уголовный кодекс, Уголовный кодекс федерального округа, Уголовно-процессуальный кодекс, Закон о защите данных штата Колима, а также уголовные кодексы штатов Агуаскальентес, Синалоа, Табаско и Тамаулипас;

b) 30 апреля 2009 года в «Официальных ведомостях Федерации» был опубликован Декрет о принятии раздела XXIX-O статьи 73 Политической конституции Мексиканских Соединенных Штатов, в котором предусматривается, что конгресс Союза может принимать законы по вопросу о защите личных данных, находящихся во владении физических лиц;

c) 1 июня 2009 года был опубликован Указ о принятии второго пункта статьи 16 Конституции, в котором указывается, что любое лицо имеет право на

защиту своих личных данных, доступ к ним, внесение исправлений в такие данные и их закрытие, а также может заявлять свое несогласие в соответствии с требованиями закона с изложением мотивов исключения из принципов, регулирующих обработку данных, по соображениям национальной безопасности, общественного порядка, безопасности и общественного здравоохранения или в целях защиты прав третьих лиц;

d) в Национальном автономном университете Мексики создана Группа реагирования на инциденты, связанные с нарушением информационной безопасности, которая занимается вопросами безопасности в научной сфере, а также оказанием помощи и технической поддержки органам власти Мексики в борьбе с преступлениями, совершаемыми в киберпространстве;

e) в федеральной полиции существует подразделение интернет-полиции, которое занимается расследованием преступлений, направленных против общественной безопасности;

f) федеральное правительство публикует доклады по вопросам уязвимости киберсистем, призванные информировать высшие эшелоны федеральной власти об инцидентах, происходящих в киберпространстве на глобальном уровне, в целях подготовки и поддержки инициатив, направленных на укрепление кибербезопасности в Мексике;

g) в федеральном правительстве планируется создать национальную группу ГРИКБ[1] в целях координации усилий по борьбе с киберпреступностью в стране и за рубежом;

h) уязвимость киберсистем является одним из вопросов, рассматриваемых в Национальной программе противодействия существующим угрозам;

i) в целях предупреждения преступлений в киберпространстве проводится информационно-разъяснительная работа среди населения в целом, которая координируется государственными и частными структурами;

j) Мексика принимает участие в работе различных форумов и заключает в духе доброй воли соглашения с другими странами в целях борьбы с киберпреступлениями.

Меры, которые могло бы принять международное сообщество в целях укрепления информационной безопасности на глобальном уровне

4. Следующие меры могли бы способствовать укреплению информационной безопасности на глобальном уровне:

a) принятие или обновление в соответствующих случаях законов о защите информации в киберпространстве;

b) обучение работников судебных органов по вопросам кибербезопасности, чтобы они имели представление о характере киберпреступлений и могли назначать соответствующие наказания;

[1] ГРИКБ — Группа реагирования на инциденты, связанные с нарушением безопасности компьютерных систем.

c) создание национальных ГРИКБ в целях координации усилий по противодействию серьезным угрозам безопасности, а также в качестве центров для поддержания контактов с другими странами;

d) поддержание постоянной связи между национальными ГРИКБ в целях обеспечения координации в случае возникновения инцидентов на региональном или глобальном уровне;

e) проведение форумов для обмена мнениями и обучения сотрудников подразделений обеспечения безопасности в странах — членах международного сообщества;

f) заключение международных соглашений о сотрудничестве в борьбе с киберпреступностью в целях активизации расследований и создания единого фронта борьбы с ними.

Панама

[Подлинный текст на испанском языке]
[21 июня 2010 года]

1. В Республике Панама существуют органы по борьбе с неправомерным использованием интернета в преступных целях, в том числе для совершения террористических актов. С этой целью были созданы Совет национальной безопасности и Криминалистический отдел в Институте судебной медицины и судебно-медицинской экспертизы.

2. Совет национальной безопасности осуществляет разведывательное обеспечение деятельности по борьбе с организованной преступностью и терроризмом, в частности на случай возможных покушений на национальные блага и целостность национальной территории.

3. В Институте судебной медицины и судебно-медицинской экспертизы существует Криминалистический отдел, созданный Законом № 69 от 27 декабря 2007 года, который занимается расследованием преступлений, совершаемых в киберпространстве.

4. В Уголовном кодексе нашей страны предусматривается квалификация, а также меры наказания и пресечения использования интернета в террористических целях, и в его статье 289 указывается: «Тот, кто использует интернет для содействия подготовке или вербовке лиц в целях совершения деяний, преследующих террористические цели, наказывается тюремным заключением на срок от пяти до десяти лет».

5. Кроме того, существуют другие законодательные положения, предусматривающие наказание за использование интернета в преступных целях, и такие преступления подлежат наказанию в уголовном, гражданском и административном порядке в соответствии с главой VIII Закона № 14 от 18 мая 2007 года, главой 1 «Преступления против информационной безопасности» Закона № 51 от 22 июля 2008 года, которой регулируются электронные документы и подписи, а также оказание услуг в этой сфере и определяются другие положения, регулирующие развитие электронной торговли, а также Законом № 38 от 8 февраля 1996 года, которым предусматриваются положения, регулирующие функционирование телекоммуникаций в Республике Панама.

Катар

[Подлинный текст на английском языке]
[25 мая 2010 года]

1. Государство Катар убеждено в том, что применение информационно-коммуникационных технологий должно основываться на положениях Устава Организации Объединенных Наций и базовых принципах, регулирующих международные отношения. Кроме того, обеспечение свободного распространения информации не должно наносить ущерба суверенитету государства, а также безопасности и уважению к культурным, политическим и моральным различиям между странами.

2. Усилия, предпринимаемые на национальном уровне, основаны на необходимости обеспечения безопасности коммуникаций и постоянного совершенствования в этой сфере в соответствии с требованиями технического прогресса на национальном и международном уровнях.

3. Усилия нашей страны можно кратко охарактеризовать следующим образом:

– разработка стратегий и программ в сфере обеспечения безопасности и принятие законов, ограничивающих применение таких технологий в целях, не совместимых с требованиями обеспечения надежной защиты;

– создание механизма укрепления информационной безопасности с целью обеспечения защиты инфраструктуры, предназначенной для обработки секретной информации в Катаре;

– управление компьютерной безопасности и разведки осуществляет мониторинг правительственных сетей и всего национального интернет-сегмента с целью пресечения угроз Государству Катар в интернете;

– предупреждение инцидентов в киберпространстве и координация работы по устранению их последствий призваны обеспечить оперативное реагирование на такие ситуации и сведение к минимуму времени простоя. В Государстве Катар этими вопросами занимается Группа Катара по реагированию на чрезвычайные ситуации в киберпространстве (Q-CERT);

– большое значение придается информационно-разъяснительной работе, направленной на повышение уровня технических знаний и квалификации сотрудников организационных структур Катара;

– гражданам Катара оказывается поддержка в вопросах, связанных с интернетом;

– проводится изучение новейших технологических достижений в сфере обеспечения безопасности и надежности интернета, а также анализ создаваемых технических средств, их безопасности и функциональных особенностей;

– принимаются меры для развития международного сотрудничества в решении вопросов, связанных с интернетом. Государство Катар принимает участие в работе Форума групп оперативного реагирования и обеспечения

безопасности (FIRST) и процессе, инициированном организацией «Меридиан».

4. Наиболее важные меры, которые международное сообщество могло бы принять для укрепления информационной безопасности на национальном уровне, включают в себя следующее:

– Организация Объединенных Наций должна и далее играть главенствующую роль в обсуждении этих вопросов и предоставлять дополнительные разъяснения относительно применения проводных и беспроводных информационно-коммуникационных технологий в электронной войне, а также относительно того, обеспечивают ли существующие принципы международного права необходимую базу, которая позволяла бы определять принципы надлежащего реагирования в киберпространстве на акты агрессии;

– необходимо создать специальный международный комитет по вопросам безопасности проводной и беспроводной связи, а также подготовить всеобъемлющие исследования по этим вопросам;

– Государство Катар призывает все государства-члены создать национальные группы реагирования на чрезвычайные ситуации в киберпространстве;

– предлагается привлекать на договорной основе организации, специализирующиеся в вопросах обеспечения безопасности в сфере коммуникаций;

– необходимо повышать информированность в вопросах безопасности посредством организации симпозиумов и совещаний на местном и международном уровнях;

– необходимо укреплять сотрудничество государств с целью противодействия шпионажу и электронному пиратству;

– следует применять системы шифрования и защищенное оборудование для безопасной и конфиденциальной передачи информации и документов;

– предлагается обновлять системы защиты и регулярно проводить практикумы по обзору новейших достижений в сфере информационной безопасности.

Украина

[Подлинный текст на русском языке]
[12 мая 2010 года]

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

1. Интерес к проблемам информационной безопасности определяется все возрастающей ролью информации в различных сферах жизнедеятельности общества. С внедрением в повседневную жизнь государства и общества передовых информационных технологий, расширяются возможности воздействия информационных угроз на информационно-телекоммуникационные системы, ин-

формационные ресурсы государственных органов и коммерческих структур со стороны криминального мира и отдельных лиц, с целью совершения противоправных действий.

2. Половина зафиксированных компьютерных преступлений в мире относится к несанкционированному доступу к компьютерной информации. Растет корыстная направленность компьютерных преступлений вместе с нанесенным материальным ущербом. В настоящее время возросло количество преступлений, совершенных транснациональными хакерскими группами.

3. Компьютерная преступность характеризуется высокой латентностью, восстановление полной картины правонарушения становится невозможной по причине того, что как государственные, так и коммерческие структуры, подвергшиеся компьютерным атакам, всячески стараются скрыть такие факты, боясь потерять авторитет, не склонны афишировать нанесенный ущерб и слабую систему защиты информации. Вследствие этого случаи таких преступлений становятся достоянием гласности далеко не всегда, что говорит о необходимости развития совместных мер профилактического и предупредительного характера, которые должны быть основополагающими в системе защиты информации.

4. Компьютерные преступления, как правило, становятся лишь первым шагом в цепочке криминальных деяний, направленных на другие, традиционные виды преступления — хищения, вымогательство, мошенничество и т.д. С каждым днем преступления становятся более совершенными, изощренными и скрытными, наносящие огромный экономический и политический ущерб практически всем странам мира. Кроме того, большинство экспертов напрямую связывают информационный суверенитет государства с вопросами национальной безопасности.

5. В ходе борьбы с преступлениями в сфере информационных технологий возникают многочисленные проблемы правового характера, вызванные нематериальностью, а зачастую и недолговечностью электронных улик. Сложность разрешения проблем, характерных для кибернетической преступности, делает особенно актуальным международное сотрудничество, для чего все страны должны, в конечном счете, располагать соответствующими и совместимыми между собой правовыми, процессуальными и нормативными средствами.

6. Практика расследования компьютерных преступлений приводит к необходимости налаживания взаимодействия между правоохранительными органами различных государств.

7. В мире существует практика проведения совместных мероприятий при проведении расследований компьютерных преступлений. Служба безопасности Украины принимает активное участие в совместных операциях правоохранительных органов и специальных служб мира, проводимых в рамках борьбы с детской порнографией, мошеннических действий в сети Интернет, международным терроризмом.

8. Кроме того, необходима консолидация усилий по дальнейшему развитию сотрудничества в области обеспечения информационной безопасности, совпадающих интересов и проведения мероприятий по их защите, преимущественно на основе двусторонних и многосторонних договоров. Успешное решение проблем информационной безопасности, на наш взгляд, возможно лишь при эф-

фективном взаимодействии государственных структур различных государств, тем более что необходимая правовая база уже имеется.

9. С учетом необходимости противодействия угрозам кибернетической преступности и кибертерроризму, Служба безопасности Украины поддерживает контакты с правоохранительными органами и специальными службами иностранных государств.

10. Следует отметить, что нередко объектами нападений киберпреступников становятся сети государственных учреждений и от качественности установленных международных связей, а также оптимизации национальных законодательств под современные условия, зависит успех по розыску и наказанию преступников.

11. Принимая во внимание постоянный рост компьютерной преступности в мире, существование связи между хакерскими преступными группировками разных стран, независимости кибернетических угроз от государственных границ, следует постоянно расширять международное сотрудничество в сфере противодействия киберугрозам.

12. С целью реализации решений Всемирной встречи на высшем уровне по вопросам информационного общества (первый этап — Женева, 10–12 декабря 2003 года, второй этап — Тунис, 16–18 ноября 2005 года) в Украине был принят Закон «Про основные принципы развития информационного сообщества в Украине на 2007–2015 годы», основными приоритетами которого является интеграция в глобальное информационное пространство и развитие информационного сообщества. Данным законом предусмотрено улучшение состояния информационной безопасности в условиях использования новейших ИКТ.

13. Кроме того, разработана и принята Концепция развития телекоммуникаций в Украине, в которой предусмотрено проведение организационно-технических мероприятий, направленных на обеспечение безопасности функционирования всех элементов телекоммуникационной инфраструктуры Украины, а именно:

– создание и постепенное внедрение нормативно-правовой базы с обеспечением вопросов технической и криптографической защиты информации, гармонизированного с европейскими и международными стандартами;

– разработка современных методов защиты информации на базе технических средств для комплексного решения задач обеспечения защиты информации в телекоммуникационных сетях;

– создание системы легального перехвата информации в телекоммуникационных сетях в случаях, предусмотренных законодательством;

– создание государственного координационного центра по вопросам безопасности в информационно-телекоммуникационных сетях общественного пользования, содействие созданию государственных и негосударственных центров компетенции и реагирования на инциденты в телекоммуникационных сетях.

14. Нормативно-правовую базу защиты информации в Украине также составляют Законы Украины «Об основах национальной безопасности Украины», «Об информации», «О защите информации в информационно-телекоммуника-

ционных системах» (далее — Закон), акты Президента и Кабинета Министров Украины «Положение о технической защите информации в Украине», «Правила обеспечения защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах» (далее — Правила), «Порядок подключения к глобальным сетям передачи данных» и ряд других, а также значительное количество зарегистрированных в Министерстве юстиции нормативных актов, регламентирующих вопросы подключения информационных систем к глобальным сетям, лицензирования отдельных видов деятельности, порядок проведения оценки продукции в сфере защиты информации и другие.

15. Нормативно-правовыми актами определено, что для обработки подлежащей защите информации должны использоваться только защищенные информационно-телекоммуникационные системы (далее — ИТС), т.е. такие, в которых создана комплексная система защиты информации (далее — КСЗИ) как единая совокупность правовых и организационных мероприятий, а также программно-технических средств, способных противодействовать угрозам. При этом КСЗИ, а также используемые в ее составе средства защиты должны иметь подтверждение своего соответствия требованиям нормативных документов в области защиты информации.

16. С целью нормирования требований к КСЗИ и отдельным средствам защиты информации в Украине разработаны и введены в действие около 50 нормативных документов технического характера, устанавливающих критерии оценки защищенности информации, классификацию ИТС, порядок выполнения работ по защите, требования к отдельным средствам защиты и КСЗИ, в зависимости от класса ИТС, назначения, области применения, вида обрабатываемой информации.

17. Также, в Украине создана собственная национальная система критериев оценки защищенности информационных технологий. Система базируется на комплексе нормативных документов по защите информации в ИТС от несанкционированного доступа, которые гармонизированы с аналогичными документами стран ЕС и международными стандартами, в частности с ISO IEC 15408.

18. Кроме того, в Украине на национальном уровне создается система организационно-технических мер, направленная на противодействие осуществлению несанкционированных действий в отношении информационно-телекоммуникационных систем органов государственной власти, правоохранительных, таможенных, налоговых органов, учреждений кредитно-финансовой сферы, и других, в частности попыткам вмешательства в их работу с использованием возможностей глобальной сети Интернет.

19. В соответствии с нормами подпунктов 10, 11 Статьи 16 Закона Украины «О Государственной службе специальной связи и защиты информации Украины» с целью улучшения координации деятельности государственных органов по выявлению угроз информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах, а также устранению последствий реализации таких угроз, осуществления международного сотрудничества по этим вопросам Государственной службой специальной связи и защиты информации Украины создано и функционирует соответствующее подразделение (CERT-UA).

20. Computer emergency response team (CERT) в соответствии с мировыми тенденциями развития сети структур быстрого реагирования представляет собой команду реагирования на компьютерные чрезвычайные ситуации. Координацию деятельности таких структур на международном уровне осуществляет международная организация FIRST (Forum for Incident Response Security Teams) — форум команд реагирования на инциденты безопасности.

21. 13 июля 2009 года специализированное подразделение Государственной службы специальной связи и защиты информации Украины CERT-UA (www.cert.gov.ua) получило статус полноценного члена FIRST (Full Member).

22. В рамках своей деятельности за 2009 год CERT-UA отработано 461 сообщение от CERT-ов 30 стран мира (Австралия, Австрия, Бельгия, Венгрия, Голландия, Дания, Израиль, Индия, Испания, Италия, Канада, Китай, Корея, Литва, Малайзия, Германия, Норвегия, Пакистан, Польша, Португалия, Россия, Румыния, Саудовская Аравия, США, Тайвань, Турция, Финляндия, Франция, Эстония, Япония) о несанкционированных действиях в украинском сегменте сети Интернет (распространение вредоносного программного обеспечения, Ddos-атаки и другие попытки несанкционированных действий).

23. Необходимо добавить, что в Украине созданы нормативно-правовые основы и организована работа по обеспечению взаимодействия Госспецсвязи и правоохранительных органов, направленная на реализацию мероприятий по обеспечению безопасности государственных информационных ресурсов в ИТС и повышение эффективности системы реагирования на несанкционированные действия в отношении указанных информационных ресурсов.

24. Таким образом, сегодня в Украине обеспечена возможность выполнения работ по защите информации на всех этапах создания ИТС и КСЗИ в ИТС, независимо от вида и критичности обрабатываемой информации, вида и сложности ИТС. При этом все основные подходы к формированию требований, проектированию, разработке, оценке защищенности и обеспечению защиты информационных ресурсов в ИТС в целом совпадают с подходами, применяемыми ответственными за безопасность государственными органами стран — членов ООН и ЕС.

25. С целью проведения образовательной деятельности по подготовке специалистов в сфере информационной безопасности и компьютерной инженерии на базе Государственного университета информационно-коммуникационных технологий (ГУИКТ) создан Институт защиты информации, являющийся учебным и научным структурным подразделением Университета.

Соединенное Королевство Великобритании и Северной Ирландии

[Подлинный текст на английском языке]
[2 июня 2010 года]

1. Соединенное Королевство с удовлетворением представляет ответ на резолюцию 64/25 Генеральной Ассамблеи, озаглавленную «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

2. Мы понимаем всю актуальность этой темы и считаем, что она имеет жизненно важное значение для индивидуальных государств, их коммерческих связей и защиты их граждан, а также в более широком контексте международной безопасности. Соединенное Королевство прилагает значительные усилия для повышения безопасности киберпространства в интересах всех стран и приветствует международную деятельность в этой области, поскольку мы уверены в том, что все страны должны сотрудничать в деле повышения безопасности и надежности киберпространства.

Общая оценка положения в сфере информационной безопасности

3. Мы считаем, что безопасность киберпространства имеет важнейшее значение для сегодняшнего мира. Граждане, коммерческие организации, важнейшие элементы национальной инфраструктуры и правительства становятся все более зависимыми от интернета. Любой сбой в функционировании интернета в той или иной стране может иметь для нее последствия, а возможно и весьма значительные. К сожалению, в любой стране или за ее пределами всегда найдутся злоумышленники, которые в тех или иных целях могут попытаться воспрепятствовать функционированию интернет-услуг или манипулировать ими.

Национальные усилия по укреплению информационной безопасности и международного сотрудничества в этой сфере

4. Соединенное Королевство продолжает заниматься вопросами укрепления безопасности киберпространства как на национальном, так и на международном уровне. Что касается национального уровня, то в июне 2009 года была опубликована Национальная стратегия обеспечения кибербезопасности. Этот документ стал основой деятельности в сфере укрепления информационной безопасности на национальном уровне. Стратегией предусматривается создание двух новых учреждений: Управления по вопросам кибербезопасности и Операционного центра по вопросам кибербезопасности. Эти учреждения уже созданы и продолжают расширять свою деятельность. В правительстве Соединенного Королевства существуют три группы по реагированию на чрезвычайные ситуации в киберпространстве (CERT), которые оказывают специализированные услуги для важнейших элементов национальной инфраструктуры Соединенного Королевства, военных и иных правительственных сетей. Кроме того, наша страна ведет активную работу в этой области на международном уровне. В рамках Организации Объединенных Наций мы являемся членом Группы правительственных экспертов. Мы выступили в качестве одного из соавторов резолюции Организации Объединенных Наций по вопросу о создании глобальной культуры кибербезопасности и оценке национальных усилий по защите важнейших информационных инфраструктур. Наша страна является членом соответствующих органов Международного союза электросвязи (МСЭ). Мы участвуем в работе Организации по безопасности и сотрудничеству в Европе. При нашей полной поддержке и участии Европейский союз (ЕС) приступил к осуществлению ряда инициатив по защите важнейших элементов национальной инфраструктуры стран ЕС. Мы участвуем в совместной работе ЕС и Регионального форума АСЕАН по вопросам кибербезопасности. Мы также участвуем в ряде мероприятий в рамках НАТО по защите сетей этой организации. Соединенное Королевство уже давно является одним из ведущих государств — участников таких организаций, как «Меридиан» (www.meridian

2007.org), Форум групп оперативного реагирования и обеспечения безопасности (FIRST, www.first.org) и Европейская правительственная группа реагирования на чрезвычайные ситуации в киберпространстве (ЕГР, www.egc-group.org).

5. С текстом Национальной стратегии Соединенного Королевства по вопросам кибербезопасности можно ознакомиться на сайте кабинета министров по адресу www.cabinetoffice.gov.uk.

Возможные меры, которые могло бы принять международное сообщество для укрепления информационной безопасности на глобальном уровне

6. Мы призываем все страны создать национальные группы по реагированию на чрезвычайные ситуации в киберпространстве. Мы призываем все страны принять эффективное национальное законодательство по борьбе с киберпреступностью. Мы считаем, что, хотя электронная преступность и не является единственным видом вредоносной деятельности в киберпространстве, она получила наибольшее распространение и что сокращение масштабов противоправной деятельности отвечает интересам всех стран. Мы считаем, что Конвенция Совета Европы по борьбе с киберпреступностью представляет собой хороший инструмент для борьбы с международной электронной преступностью. Кроме того, мы считаем, что средства, разработанные МСЭ и поддержанные в Организации Объединенных Наций, обеспечивают хорошую основу для проведения государствами оценки своей готовности в плане противодействия возможным нападениям на важнейшие элементы их информационной инфраструктуры. Мы также приветствуем усилия по развитию обмена передовым опытом в сфере информационной безопасности на различных международных форумах.

Соответствующие международные концепции

7. Основная международная концепция определяется международным правом. В настоящее время, особенно на интернет-конференциях, широко обсуждаются вопросы применимости существующих положений международного права к киберпространству. Соединенное Королевство внимательно изучило этот вопрос и пришло к выводу о том, что существующие принципы международного права, как в отношении применения силы, так и в отношении вооруженных конфликтов, обеспечивают необходимую основу для определения и анализа особенностей использования киберпространства в ходе военных действий.