Организация Объединенных Наций A/68/156

Генеральная Ассамблея

Distr.: General
16 July 2013
Russian
Original: English/Russian/Spanish

Шестьдесят восьмая сессия
Пункт 94 первоначального перечня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Содержание

* A/68/50.

13-39737 (R) 020813 120813

I. Введение

1. 3 декабря 2012 года Генеральная Ассамблея приняла резолюцию 67/27, озаглавленную «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». В пункте 3 данной резолюции 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 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 данной резолюции;

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

2. Во исполнение данной просьбы 22 февраля 2013 года государствам-членам была направлена вербальная нота с просьбой представить информацию по данному вопросу. В разделе II ниже содержатся полученные ответы. Любые дополнительные ответы, которые будут получены, будут опубликованы в качестве дополнений к настоящему докладу.

II. Ответы, полученные от правительств

Куба

[Подлинный текст на испанском языке]
[20 мая 2013 года]

Враждебное использование телекоммуникаций в открытых или скрытых целях, заключающихся в подрыве юридического и политического строя государств, является нарушением международно признанных норм в этой области, ибо последствия таких действий могут вызвать напряженность и создать негативные проблемы, затрагивающие международный мир и безопасность.

Куба в полной мере разделяет озабоченность, выраженную в резолюции 67/27 в отношении применения информационных технологий и средств в целях, которые могут повлиять на международную стабильность и безопасность, целостность инфраструктуры государств, нарушая их безопасность в гражданской и военной сферах. Кроме того, в данной резолюции сделан надлежащий упор на необходимость воспрепятствовать применению информационных ресурсов и технологий в преступных или террористических целях.

В этой связи Куба вновь заявляет об осуждении агрессивной эскалации осуществляемой правительством Соединенных Штатов радиотелевизионной войны против Кубы в нарушение международных норм, действующих в области регулирования радиоэлектронного спектра. Эта агрессия наносит ущерб международному миру и безопасности, создавая опасные ситуации, в том числе путем использования военного самолета для передачи радиотелевизионных сигналов в направлении нашей страны без согласия Республики Куба.

Осуществление радиопередач с борта воздушных судов является нарушением правила 42.4 Регламента радиосвязи Международного союза электросвязи (МСЭ), которое запрещает использование радиовещания с воздушных судов, находящихся в морском пространстве или над ним.

В 2012 году Соединенные Штаты осуществили 192 полета, с помощью которых, помимо осуществления незаконной передачи телевизионных сигналов с воздушных судов в направлении кубинской территории, также осуществлялась одновременно незаконная передача сигналов на частотах FM. Эти действия привели к негативному воздействию на работу телевизионных кубинских радиостанций, которые зарегистрированы в Генеральном регистре Управления радиокоммуникаций Международного союза электросвязи.

В течение каждой недели радиостанции, находящиеся на территории Соединенных Штатов, передают в направлении Кубы в среднем 2400 часов радиотелевизионного вещания, осуществляемого на незаконной основе, используя 30 различных частот в диапазоне средних частот, коротких частот, FM и телевизионных частот. Некоторые из этих радиостанций принадлежат или используются организациями, связанными с широко известными террористическими элементами, которые действуют против Кубы с американской территории и ведут передачу программ, в которых содержатся призывы к осуществлению актов саботажа, политических покушений, массовых убийств и других мер, связанных с радиотерроризмом.

Ведение незаконных радио- и телевизионных передач в направлении Кубы имеет своей целью поощрение незаконной эмиграции, подстрекательство к насилию, нарушение конституционного порядка и совершение террористических акций. Куба вновь заявляет, что использование информации в целях подрыва законного строя других стран, нарушения их суверенитета и вмешательства в их внутренние дела является незаконным.

Такие провокационные передачи, ведущиеся в направлении Кубы, нарушают действующие международные нормы, регулирующие использование радиоэлектронного спектра в рамках Международной конвенции электросвязи, причем правительство Соединенных Штатов Америки является одной из сторон, подписавших эту Конвенцию.

Куба поддерживает резолюцию 67/27 и будет и впредь вносить свой вклад в мирное глобальное развитие информационных и телекоммуникационных технологий и их использование на благо всего человечества.

Испания

[Подлинный текст на испанском языке]
[29 мая 2013 года]

1. Введение

Защищенность информации является ключевым элементом информационного общества. Технологический прогресс содействовал постоянному развитию и расширению возможностей в области сбора и хранения информации в многочисленных форматах; с другой стороны, в области коммуникаций имело место весьма существенное расширение имеющихся полос, что открывает возможности для передачи и получения огромного количества информации практически в реальном времени и без необходимости обладания исключительно сложной инфраструктурой.

Такой технологический прогресс наряду с улучшением доступа к информации всевозможного типа содействует также их применению и использованию в незаконных целях, включая использование систем телекоммуникаций и информации во враждебных, преступных и даже террористических и агрессивных целях против государств или транснациональных субъектов.

В последние годы была выявлена все более усиливающаяся тенденция к использованию сети Интернет преступными организациями, в частности террористическими группами, которые в основном используют две из ее основных характеристик: глобальный характер и большие гарантии анонимности, которые может обеспечить Интернет.

В этой связи необходимо обеспечить сбалансированность между эволюцией общества и информационных технологий и одновременной эволюцией национальных и международных, современных, обновленных и адаптированных к новым технологическим условиям норм, которые будут содействовать созданию возможностей для ответа на вызовы, которые связаны с необходимостью защиты информации, с тем чтобы не допустить ее незаконного использования, не допуская при этом ограничения прав и свобод отдельных граждан.

2. Противоправное использование сети Интернет в террористических целях

В настоящее время основными угрозами, которые связаны с использованием сети Интернет террористическими организациями, являются следующие:

а) использование сети Интернет в качестве оружия, иначе говоря, использование сети Интернет в качестве средства для организации нападений на информационные системы, имеющие важное значение для инфраструктуры, а также на саму инфраструктуру сети Интернет. Нападения такого рода осуществляются относительно часто в чисто преступных целях, однако нападение, которому подверглась Эстония в 2007 году, наглядно показало, что объекты информационной инфраструктуры государства также могут быть доведены до состояния коллапса в результате атаки такого типа. С такими угрозами непосредственно связано все более возрастающее использование новых форм вредонос-

ного программного обеспечения, которые возникли в последние годы, и так называемых «ботнетс» или компьютерных систем «зомби», которые используются для осуществления нападений на информационные системы;

b) использование сети Интернет в качестве средства для осуществления другой деятельности, в основном следующего типа:

- **Деятельность в области коммуникации.** Использование сети Интернет приходит на смену коммуникационных средств, используемых преступными организациями, как, например, стационарные средства телефонной связи или мобильная телефонная связь. Средствами, которые в наибольшей степени используются для осуществления связи через посредство сети Интернет в надежных и анонимных условиях, являются электронная почта, сообщения SMS и Интернет-форумы.

- **Распространение пропаганды и материалов, связанных с деятельностью террористических организаций.** В настоящее время существуют тысячи веб-сайтов, которые имеют отношение к деятельности террористов или которые связаны с подстрекательством к совершению актов насилия, что наглядно подтверждается все большим распространением явления веб 2.0 и социальных сетей. Что касается методов, которые позволили бы воспрепятствовать использованию сети Интернет террористическими организациями, то речь идет о довольно сложной задаче, поскольку такие сайты довольно легко осуществляют миграцию. Речь идет о транснациональном явлении, поскольку страны, в которых находится сервис сети, на котором размещается веб-страница и осуществляется ее обслуживание, могут быть разными и, кроме того, могут находиться в другой стране, не имеющей никакого отношения к стране, в которой действует террористическая организация, что создает правовой вакуум, если не существует необходимых двусторонних соглашений с такими странами.

- **Деятельность в целях вербовки.** В различных случаях сеть Интернет используется в качестве средства для осуществления вербовки, прежде всего с помощью форумов и программ SMS сообщений.

- **Финансирование.** Сеть Интернет также создает возможности для того, чтобы террористические организации осуществляли деятельность, направленную на сбор финансовых средств. В частности, представляется вполне реальным, что террористические организации принимают участие в совершении мошеннических действий, вымогательства и отмывания денег с помощью сети Интернет как средства для получения финансовых средств.

- **Распространение учебных пособий.** С помощью Интернет террористические организации распространяют пособия о технике террористической деятельности, изготовления взрывчатых веществ и использования вооружений.

- **Сбор информации для совершения преступных действий.** Сеть Интернет также является очень важным источником информации, который во многих случаях используется террористическими организациями для получения данных об объектах своих акций, будь то против физических или юридических лиц или объектов инфраструктуры.

3. Меры, принимаемые на национальном уровне для борьбы с использованием сети Интернет террористическими организациями

3.1. Законодательные меры

Что касается мер, которые принимают различные государства, то Испания прилагала большие усилия в течение последних лет, и в частности в 2007 году, включила в свою юридическую систему ряд законов, которые связаны с безопасностью информации и свободой осуществления прав и свобод, признанных во Всеобщей декларации прав человека и в Конституции Испании. Были осуществлены крупномасштабные законодательные и нормативные действия, включая принятие мер как чисто национального характера, так и директив Европейского союза, направленных на достижение этих целей путем применения новых критериев информационной безопасности, которые являются необходимыми для обеспечения разумной степени защиты, а также для сохранения конфиденциальности информации, что является основополагающей задачей в большинстве случаев, с целью сохранения ее целостности и наличия. Среди них следует отметить:

- Органический закон № 5/1992 от 29 октября 1992 года о регулировании автоматизированного режима сбора данных личного характера, в основу которого положена необходимость создания предохранительных механизмов, которые будут препятствовать нарушению частной жизни в результате использования информации и положения по осуществлению этого закона.

- Органический закон № 15/1999 от 13 декабря 1999 года о защите данных личного характера, цель которого состоит в том, чтобы гарантировать и обеспечить защиту личных данных, публичных свобод и основополагающих прав физических лиц, и в частности их чести и личной и семейной жизни, и положения по осуществлению этого закона.

- Королевский указ-закон № 14/1999 от 17 сентября 1999 года об электронных подписях, который был принят с целью содействия скорейшему внедрению новых технологий и обеспечения безопасности электронных сообщений, связанных с деятельностью предприятий, граждан и государственных административных органов, который инкорпорирует в испанское законодательство положения директивы № 1999/93/CE Европейского парламента и Совета Европы от 13 декабря 1999 года, в соответствии с которым устанавливаются общие рамки для электронных подписей. Закон № 59/2003 от 19 декабря 2003 года об электронных подписях уточняет эти положения путем инкорпорации новых положений с учетом накопленного опыта в период после его вступления в силу.

- Закон № 11/2002 от 6 мая 2002 года о регулировании деятельности Национального разведывательного центра (НРЦ) и впоследствии Королевский указ № 421/2004 от 12 марта 2004 года, в соответствии с которым обеспечивается регулирование деятельности Национального криптологического центра; с помощью этих законодательных актов Национальному разведывательному центру, в частности, рекомендуется осуществлять координацию деятельности различных административных органов, которые используют цифровые средства и процедуры, с тем чтобы гарантировать

безопасность информационных технологий в этой области и обеспечить соблюдение норм, касающихся защиты закрытой информации.

- Закон № 34/2002 от 11 июля 2002 года об услугах информационного общества и электронной торговле. Этот закон имеет своей целью инкорпорирование в испанское законодательство положений директивы № 2000/31/CE Совета Европы от 8 июня 2000 года, которые касаются определенных аспектов услуг информационного общества, в частности электронной торговли на внутреннем рынке (Директива об электронной торговле). Кроме того, этот закон инкорпорирует положения Директивы № 98/27/CE, Европейского парламента и Совета Европы от 19 мая 1998 года, касающиеся мер по обеспечению защиты интересов потребителей с помощью регулирования — в соответствии с его положениями — действий санкций в отношении поведения, которое является нарушением положений настоящего закона.

- Закон № 32/2003 от 3 ноября 2003 года о телекоммуникациях, который регулирует использование сетей и предоставление электронных коммуникационных услуг.

- Закон № 59/2003 от 19 декабря 2003 года об электронных подписях, упомянутый выше.

- Закон № 11/2007 от 22 июня 2007 года об электронном доступе граждан к государственным службам, который регулирует сферу коммуникаций путем использования и применения электронных, информационных и телематических технологий и средств, доступных для граждан и государственных административных органов.

- Органический закон № 10/2007 от 8 октября 2007 года, регулирующий базы полицейских данных, касающиеся различных показателей, с целью использования результатов анализа дезоксирибонуклеиновой кислоты (ДНК), что позволяет создать базу данных, в рамках которой обеспечивается ведение файлов в вооруженных силах и органах государственной безопасности и сбор идентификационных данных, полученных с помощью анализа ДНК, которые использовались в ходе уголовных следственных мероприятий или в рамках процедур идентификации останков умерших лиц или сверки данных о пропавших без вести лиц.

- Закон № 25/2007 от 18 октября 2007 года о сохранении данных, касающихся электронной связи и государственных коммуникационных сетей, что позволяет оказывать позитивное воздействие на проведение расследований в этой области.

- Королевский указ № 1720/2007 от 21 декабря 2007 года, в соответствии с которым утверждается регламент, разработанный на основе Органического закона № 15/1999 от 13 декабря 1999 года о защите данных личного характера.

- Закон № 56/2007 от 28 декабря 2007 года о мерах по стимулированию создания информационного общества.

- Уголовная кодификация следующих кибернетических преступлений, связанных с деятельностью террористических организаций в сети Интернет:
  - информационный саботаж, статья 264 Уголовного кодекса
  - угрозы, статья 169 и последующие статьи Уголовного кодекса
  - подстрекательство и пропаганда терроризма, статья 578 Уголовного кодекса

3.2. Другие меры

- Создание полицейских групп по борьбе с использованием сети Интернет уголовными сообществами.
- Участие в реализации проекта “Check the Web” («Проверка электронной сети»), подготовленного Полицейской службой Европейского союза (Европол).
- Организация по безопасности и сотрудничеству в Европе (ОБСЕ) создала неофициальную рабочую группу для разработки мер укрепления доверия с целью уменьшения опасности возникновения конфликтов в результате использования информационных и коммуникационных технологий. Эта рабочая группа имеет своей целью сокращение возможностей осуществления кибернетических нападений и, кроме того, обеспечивает взаимную безопасность на основе международного сотрудничества, поощрения транспарентности и открытости и сокращения опасности возникновения недоразумений, которые могут привести к эскалации конфликтов. Все это осуществляется на основе мер укрепления доверия в политической и военной областях в целях использования информационных и коммуникационных технологий.
- Национальная система безопасности. Эта система имеет своей целью разработку политики национальной безопасности в сфере использования электронных средств. Эта система основывается на основополагающих принципах и минимальных требованиях, которые позволяют обеспечить адекватную защиту информации. В ее работе принимают участие представители всех органов власти. Ее юридической основой является Королевский декрет, в соответствии с которым претворяется в жизнь статья 42 Закона № 11/2007. Фактически, стратегия безопасности Испании благодаря определению угроз и рисков, которые в наибольшей степени затрагивают безопасность нашей страны, а также обеспечению их поддержки мер реагирования, рассматривает кибернетическое пространство как одну из многочисленных областей, в которых необходимо осуществлять деятельность. Данный анализ обеспечивает основы для разработки стратегических направлений в сферах реагирования и наращивания потенциала и проведения организационных реформ.
- Национальный криптологический центр при Национальном разведывательном центре ежедневно вносит свой веский вклад в борьбу с кибернетическими преступлениями. В этой связи следует подчеркнуть деятельность Национального криптологического центра и его группы по реагированию на чрезвычайные ситуации в киберпространстве (CERT), которая оказывает поддержку и обеспечивает потенциал по реагированию на ин-

циденты, касающиеся информационной безопасности. Этот центр, созданный правительством Испании в начале 2007 года, принимает участие в работе основных международных форумов, в ходе которых осуществляется обмен мнениями, идеями и информацией по вопросам кибернетической безопасности.

- Создание Национального центра по защите основных объектов инфраструктуры.

- Министерство обороны осуществляет различные мероприятия в области кибероборонны. Следует отметить участие — через посредство Генерального штаба министерства обороны Передового центра кибернетической обороны — в работе Организации Североатлантического договора (НАТО) в Таллинне, Эстония, работу которого Испания совместно финансирует с другими государствами с момента его создания. В этом Центре работают два испанских эксперта. Международное значение данного центра в борьбе против кибертерроризма постоянно возрастает, что подтверждается недавним визитом Его Королевского Высочества, в ходе которого он подчеркнул обязательства Испании по реализации международных инициатив в области кибербезопасности.

- С другой стороны, НАТО осуществляет весьма активную деятельность в области кибернетической обороны и разработала концепцию, в соответствии с которой определяется политика, и создала агентство по руководству деятельностью в области кибероборонны НАТО.

Директива по вопросам национальной обороны 2012 года. В ее рамках осуществлен анализ глобальных угроз, которым мы должны противостоять, и в первую очередь кибернетические акции рассматриваются как одна из основных опасностей, которые могут быть устранены только с помощью объединения сил, в данном случае на основе деятельности НАТО и Европейского союза. Тем не менее необходимо заручиться поддержкой других стран и групп стран, которые как косвенно, так и непосредственно также заинтересованы в противодействии таким явлениям.

Иначе говоря, данная директива определяет рамки деятельности, включая участие в поощрении комплексного взаимодействия в области кибербезопасности на основе принципов, которые определяются в соответствии с национальной стратегией кибербезопасности.

Политическая директива по вопросам обороны, одобренная в течение 2012 года, также содержит упоминание о кибернетическом пространстве как новой сфере международного взаимодействия. В ней определяется необходимость укрепления систем сбора информации и ведения разведывательной деятельности с целью поддержки ее операций, а также систем управления и контроля для уменьшения опасности совершения кибернетических преступлений.

Начальник Генерального штаба министерства обороны в январе 2011 года опубликовал свою концепцию военной кибероборонны, которая предусматривает определение, функционирование и использование необходимых военных средств, которые позволят гарантировать эффективное использование кибернетического пространства в ходе военных операций.

4. Меры, которые следует принять международному сообществу для укрепления информационной безопасности в международном масштабе

Усиление взаимозависимости информационных систем и усиление взаимосвязи критических объектов инфраструктуры привели к тому, что безопасность в кибернетическом пространстве является основополагающим элементом функционирования современного государства. Соответственно, кибернетическая безопасность должна стать неотъемлемой частью планирования национальной безопасности.

В настоящее время не существует каких-либо гарантий создания международно-правовых рамок, которые будут реагировать на угрозы, касающиеся безопасности в этой сфере, поэтому без ущерба для национального суверенитета в области кибернетической безопасности необходимо разработать многосторонние соглашения по вопросам сотрудничества в этой области, аналогичные Международной конвенции по охране человеческой жизни на море или же другим конвенциям, в рамках которых государства берут на себя обязательство унифицировать свои законодательные акты, с тем чтобы обеспечить преследование и наказание преступлений в сети Интернет, с тем чтобы по мере возможностей исключить возможность использования анонимных средств, отсутствие законодательства или экономические интересы, в результате которых сеть Интернет превращается в идеальную питательную среду для преступности и терроризма.

Необходимо привлечь частный сектор, в частности поставщиков интернет-услуг, к борьбе против кибернетической преступности. Сотрудничество частного сектора имеет основополагающее значение, поскольку большинство услуг, предоставляемых в рамках Интернета, находится в руках частного сектора. Частный сектор тратит большие средства и много времени на борьбу с угрозами, существующими в сети Интернет, и его знания и опыт могут оказаться весьма ценными.

Группа по реагированию на чрезвычайные ситуации в киберпространстве является основополагающим элементом в области кибербезопасности. Создание специальных групп по реагированию на чрезвычайные ситуации в киберпространстве и дальнейшее повышение квалификации ее членов с учетом последних тенденций являются первыми шагами, которые правительства должны принять, с тем чтобы гарантировать кибернетическую безопасность. Кроме того, в рамках сил правопорядка необходимо создать специализированные подразделения по расследованию преступлений, совершаемых с использованием сети Интернет.

Кибербезопасность является глобальным вызовом, и поэтому международное сотрудничество, направленное на ее совершенствование, имеет основополагающее значение и должно получать поддержку как на политическом, так и на оперативном уровне. Взаимодействие между группами кибернетического реагирования различных государств должно иметь гибкий характер, с тем чтобы содействовать обмену информацией о кибернетических преступлениях в течение самого короткого возможного срока. Также необходимо осуществлять обмен извлеченными уроками и передовым национальным и международным опытом.

Среди других мер следует отметить:

- Формирование и повышение осведомленности граждан с самого раннего возраста относительно необходимости уделения внимания безопасности используемых информационных систем. Осуществление различных форм кибернетических преступлений часто объясняется тем, что многие пользователи Интернета не принимают необходимых предосторожностей для того, чтобы обеспечить безопасность и неприкосновенность своих электронных средств. Поэтому просвещение пользователей имеет важное значение. Повышение осведомленности об этой проблеме позволит сократить число компьютеров, используемых киберпреступниками для осуществления их деятельности, в частности деятельности, связанной с «ботнетс».

- Совершенствование процедур судебного и полицейского взаимодействия на международной арене, с тем чтобы обеспечить эффективное и оперативное уголовное преследование преступных деяний, учитывая характер деятельности сети Интернет и нестабильный характер регистрации соединений с учетом законодательства каждой отдельной страны.

- Организация форумов, семинаров и международных конференций. Они должны иметь своей целью повышение осведомленности экспертов и обмен знаниями о различных формах кибернетических преступлений, новых тенденциях при совершении киберпреступлений, анализ уязвимых сторон и воздействие потенциальных атак, а также обмен извлеченными уроками и передовым опытом и поощрение систематической профессиональной подготовки сотрудников сил правопорядка в области расследования кибернетических преступлений.

- Координация усилий других специализированных организаций в конкретных областях кибернетической безопасности, в том числе в рамках Совета Европы и НАТО. Это позволит избежать ненужного дублирования усилий.

- Разработка пособий или сборников данных о передовом опыте с целью повышения кибернетической безопасности в сотрудничестве с частным сектором и гражданским обществом.

В заключение следует отметить, что международное сообщество должно принять меры по защите информации, которые оно считает необходимыми, исходя из единого стратегического видения и, по возможности, формированию единой концепции деятельности с целью разработки соответствующих норм и общих принципов для всех стран, что позволит обеспечить сбалансированное и полное осуществление конкретных мер в области защиты и позволит согласовать политику и действия различных международных и национальных организаций, связанных с этой деятельностью.

Украина

[Подлинный текст на русском языке]
[31 мая 2013 года]

1. Общая оценка проблем информационной безопасности

Проблематика информационной безопасности, а также обеспечение безопасности телекоммуникаций и противодействие киберпреступности является одним из ключевых направлений обеспечения национальной безопасности Украины, что, в свою очередь, способствует укреплению международной безопасности в условиях глобализации.

Мировые процессы глобализации, формирование информационного сообщества, внедрение новых информационных технологий усиливают важность такой составляющей национальной безопасности государства, как информационная безопасность, которая характеризует состояние защищенности национальных интересов в информационной сфере от внешних и внутренних угроз.

Соответственно, к угрозам информационной безопасности на международном уровне можно отнести следующие:

- неправомерное использование информационных ресурсов;
- несанкционированные действия, которые носят деструктивный характер, в автоматизированных системах, в том числе системах управления объектами национальной критической инфраструктуры;
- использование киберпространства, а также мероприятий, информационно-компьютерных технологий и средств, связанных с нарушением основных прав и свобод человека, или для достижения террористических, экстремистских и других преступных намерений вплоть до применения актов агрессии;
- использование информационной инфраструктуры для распространения информации, которая разжигает вражду и ненависть в обществе или отдельной стране;
- распространение информации, которая противоречит действующему национальному законодательству, а также нормам и принципам морали;
- использование киберпространства с целью дестабилизации общества, подрыва экономической, политической и социальной системы другого государства или дезинформация, направленная на искажение культурных, этических и эстетических ценностей;
- противодействие доступу к новейшим технологиям, создание условий для технологической зависимости в сфере информатизации в целях получения преимущества и контроля за киберпространством других государств.

В информационной сфере следует выделить следующие проблемные вопросы, проявляющиеся в условиях глобализации. К ним относятся: информационно-психологическое воздействие индивидуальной и массовой направленности, ограничение доступа потребителей к услугам, основанным на информационно-телекоммуникационных технологиях, киберпреступность.

Согласно оценкам украинских экспертов, повышению уровня вероятности реализации указанных выше угроз способствуют такие факторы:

- недостаточный (низкий) уровень компьютерной грамотности большинства пользователей информационных ресурсов и услуг киберпространства;
- отсутствие единого международного понятийного аппарата, связанного с информационной безопасностью;
- различные подходы в национальном законодательстве, связанные с мерами по защите информации, направленными на создание и модернизацию (восстановление) информационной инфраструктуры;
- разные уровни информатизации и обеспечения безопасности информации в других странах;
- потенциальная опасность, связанная с подключением к информационно-телекоммуникационным системам средств с деструктивными возможностями;
- отсутствие определенности в идентификации источников несанкционированных действий в киберпространстве.

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

В Украине ключевыми государственными органами по вопросам информационной безопасности и ее составляющих определены Министерство внутренних дел Украины, Служба безопасности Украины, а также Государственная служба специальной связи и защиты информации Украины (Госспецсвязь). Указанные государственные органы проводят активную работу относительно урегулирования различных сфер обеспечения информационной безопасности. При этом особое внимание уделяется вопросу нормативно-правового обеспечения кибернетической составляющей (кибербезопасности).

На сегодняшний день в Украине действуют нижеследующие нормы законодательства, которые регулируют общественные отношения в сфере информационной безопасности.

В соответствии со статьей 17 Конституции Украины, обеспечение информационной безопасности наряду с защитой суверенитета и территориальной целостности Украины, обеспечением ее экономичной безопасности является важнейшей функцией государства.

Согласно статье 3 Закона Украины «Об информации», обеспечение информационной безопасности Украины относится к основным направлениям государственной информационной политики.

Информационная безопасность в общей системе национальной безопасности Украины занимает особое место, поскольку информационные отношения и процессы являются составляющими любых процессов, происходящих в обществе и государстве. При этом информационной безопасностью государства

считается состояние информационного пространства (среды), которое состоит из совокупности информационной инфраструктуры, информационных технологий, информационных ресурсов и информационных отношений субъектов, которое гарантирует его развитие и использование в интересах личности, общества и государства.

Основные цели обеспечения информационной безопасности определяются приоритетами национальной безопасности, что соответствует интересам общественного развития. Такими целями являются:

- обеспечение национального информационного суверенитета Украины в условиях глобализации информационных процессов и стремления других стран к информационному доминированию;
- формирование информационной среды, ориентированной на духовное и интеллектуальное развитие личности и общества в целом;
- поддержка достаточного объема информационных ресурсов Украины, которые обеспечивают стойкое функционирование и развитие личности, общества и государства;
- обеспечение защиты информации физических, юридических лиц и государства от внешних и внутренних информационных угроз, в том числе борьба с компьютерными преступлениями;
- обеспечение законности и реализация прав субъектов информационных отношений Украины в сфере создания и использования национальных информационных ресурсов, информационных технологий и информационной инфраструктуры.

С целью укрепления информационной безопасности осуществляется формирование нормативно-правовой базы, системы подготовки профессиональных кадров, а также координация работы органов государственной власти, отвечающих за информационную безопасность, в том числе их эффективное взаимодействие с Командой реагирования на компьютерные чрезвычайные события Украины (CERT-UA), аккредитованной международной организацией «Форум команд реагирования на компьютерные инциденты» (FIRST).

В соответствии с украинским законодательством CERT-UA функционирует в составе Госспецсвязи и осуществляет координацию деятельности предприятий, учреждений и организаций, независимо от форм собственности, направленной на предупреждение, анализ и ликвидацию последствий несанкционированных действий по отношению к государственным информационным ресурсам в информационно-телекоммуникационных системах.

Кроме того, CERT-UA осуществляет взаимодействие с компетентными зарубежными и международными органами и организациями, а наличие у Команды CERT-UA обязательств перед иностранными коллегами (полноправное членство в FIRST, членство в Международном многостороннем партнерстве против киберугроз Международного союза электросвязи ITU-IMPACT) способствует развитию международного сотрудничества в сфере информационной безопасности.

В соответствии с Законом Украины «О внесении изменений в Закон Украины “О ратификации Конвенции о киберпреступности”» органом, на который возложены полномочия по созданию и функционированию круглосуточной контактной сети для предоставления неотложной помощи при расследовании преступлений, связанных с компьютерными системами и данными, преследовании лиц, которые обвиняются в совершении таких преступлений, а также сбору доказательств в электронной форме, является министерство внутренних дел.

На сегодняшний день в структуре министерства внутренних дел функционирует соответствующее подразделение — отдел организации круглосуточной контактной сети по реагированию на киберпреступления Управления борьбы с киберпреступностью, на который и возложена реализация соответствующих задач и функций, в том числе:

– противодействие «Ddos-Атакам»;

– борьба с криминальными правонарушениями, совершаемых с использованием платежных карточек или их реквизитов;

– борьба с несанкционированными вмешательствами в работу систем дистанционного банковского обслуживания «клиент-банк»;

– противодействие распространению противоправного контента (нарушающего авторские права) в сети Интернет;

– противодействие распространению в сети Интернет продукции порнографического характера, в том числе изготовленной с участием детей;

– противодействие правонарушениям в сфере телекоммуникаций;

– противодействие правонарушениям в сфере несанкционированного доступа к спутниковым сетям передачи данных;

– противодействие финансовым и другим видам мошенничества в сети Интернет;

– противодействие криминальным и другим правонарушениям в сфере электронной коммерции;

– организация работы круглосуточной контактной сети из реагирования на киберпреступления.

На сегодняшний день продолжается работа по актуализации национального законодательства в сфере информационной безопасности с целью создания гармонизированной с международными нормами нормативно-правовой базы Украины.

В настоящее время в Украине в соответствии с Указом Президента Украины от 10 декабря 2010 года № 1119 «О решении Совета национальной безопасности и обороны Украины от 17 ноября 2010 года „О вызовах и угрозах национальной безопасности Украины в 2011 году“» осуществляется разработка законопроекта «О кибернетичной безопасности Украины».

Перспективными направлениями национальной политики в соответствии с действующими нормативно-правовыми актами являются следующие:

1) *Указами Президента Украины:* от 10 декабря 2010 года № 1119 «О решении Совета национальной безопасности и обороны Украины от 17 ноября 2010 года “О вызовах и угрозах национальной безопасности Украины в 2011 году”» (п. 4); от 8 июня 2012 года № 388 «О решении Совета национальной безопасности и обороны Украины от 25 мая 2012 года “О мероприятиях по усилению борьбы с терроризмом в Украине”» (п. 1); от 8 июня 2012 года № 389 «О решении Совета национальной безопасности и обороны Украины от 8 июня 2012 года “О новой редакции Стратегии национальной безопасности Украины” (п.п. 3.1.1, 3.3, 4.3), от 8 июня 2012 года № 390 “О решении Совета национальной безопасности и обороны Украины от 8 июня 2012 года “О новой редакции Военной доктрины Украины”» (п.п. 7, 19), предусмотрены такие задачи:

– создание национальной системы кибербезопасности;

– создание единой общегосударственной системы противодействия киберпреступности;

– разработка и утверждение перечня объектов, критически важных для обеспечения национальной безопасности и обороны Украины, а также имеющих первоочередное значение в плане защиты от кибернетических атак;

– разработка и внесение на рассмотрение Парламента Украины проекта Закона Украины «О кибернетической безопасности Украины»;

– определение киберпреступности в качестве одного из основных факторов, угрожающих международной стабильности и национальной безопасности Украины;

– утверждение в качестве стратегической цели и основной задачи политики национальной безопасности разработки национальных стандартов и технических регламентов применения информационно-коммуникационных технологий, их гармонизации с соответствующими стандартами стран — членов ЕС;

– определение термина «кибертерроризм»;

– создание в Украине эффективного механизма реагирования на новейшие вызовы национальной безопасности (явления и тенденции, которые могут в определенных условиях трансформироваться в угрозы национальным интересам), связанные с использованием информационных технологий в условиях глобализации, особенно «киберугрозы»;

– расценивание «кибернетических атак» на объекты ядерной, химической промышленности, оборонно-промышленного комплекса и другие потенциально опасные объекты как проявление применения военной силы против Украины, которое создает условия для возникновения военного конфликта;

2) *нормативно-правовые акты Кабинета Министров Украины*: Распоряжение от 22 августа 2012 года № 720-р «Об утверждении плана мероприятий по выполнению Годовой национальной программы сотрудни-

чества Украина — НАТО на 2012 год», а также Поручение от 15 июня 2012 года № 24066/1/1-12 к вышеуказанному Решению Совета национальной безопасности и обороны Украины (далее — СНБО), введенного в действие Указом Президента Украины от 8 июня 2012 года № 388, — также направлены на обеспечение подготовки законодательного акта по вопросам обеспечения кибербезопасности;

3) Парламентом Украины рассматриваются *проекты Закона Украины «О внесении изменений в некоторые законы Украины относительно обеспечения кибернетической безопасности Украины»*. Указанными законопроектами, среди прочего, предусмотрено введение в национальное законодательство таких понятий, как «кибернетическая безопасность государства», «объекты критической инфраструктуры», «объекты критической информационной инфраструктуры», а также «кибернетическое пространство (киберпространство)», а также определение основных угроз национальной безопасности кибернетического характера, основных направлений государственной политики и функции субъектов обеспечения национальной безопасности в этой сфере.

3. Внедрение международных концепций, направленных на усиление безопасности глобальных информационных и телекоммуникационных систем

В Украине создана нормативно-правовая база по вопросам защиты информации в информационно-телекоммуникационных системах, которая является гармонизированной (по принципам и подходам к строительству защиты) с международным стандартом ISO 15408 (Общие критерии оценки безопасности информационных технологий) (Common Criteria for Information Technology Security Evaluation).

В связи с тем, что компьютерная преступность переросла национальные границы и стала интернациональным явлением, Украина последовательно проводит политику сотрудничества с правоохранительными органами других стран.

Также следует отметить, что Украина в процессе реализации проектов и программ Организации по безопасности и сотрудничеству в Европе, Парламентской Ассамблеи Совета Европы, Совета Европы, Программы НАТО «Партнерство во имя мира», а также в рамках двухсторонних договоренностей прилагает усилия для обеспечения международной информационной безопасности.

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

Транснациональный характер компьютерной преступности дает основание считать, что настало время разработки международных принципов, направленных на укрепление безопасности информационно-телекоммуникационных сетей, общей интернациональной политики безопасности, совер-

шенствованию форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности.

Одним из основополагающих направлений обеспечения глобальной информационной безопасности является подготовка и принятие международно-правовых актов, направленных на устранение терминологической неопределенности в сфере информационной безопасности. При этом важным элементом является определение международно-правового статуса киберпространства, а также нормативно-правовое закрепление юрисдикции государств в отношении национальных составляющих этого пространства (по аналогии с воздушным, водным пространством государств) и последующим урегулированием вопросов, связанных с кибервойной, киберагрессией и т.д.

Ключевым направлением нормотворческой деятельности в данной сфере является также внедрение унифицированного понятия киберпреступности, а также четкой систематизации соответствующих деяний.

Другие возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне, могут включать гармонизацию нормативно-правовой базы в сфере защиты информации, разработку согласованных критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности, взаимное признание сертификатов продукции в сфере защиты информации, расширение взаимодействия при решении научно-техничных и правовых вопросов обеспечения безопасности информации. При этом укрепление взаимодействия правоохранительных органов государств по предотвращению и пресечению компьютерных преступлений, применению юридической ответственности является необходимым условием успешного взаимодействия на данном направлении.

Соединенное Королевство Великобритании и Северной Ирландии

[Подлинный текст на английском языке]
[16 мая 2013 года]

Соединенное Королевство Великобритании и Северной Ирландии приветствует возможность ответить на просьбу, содержащуюся в резолюции 67/27 Генеральной Ассамблеи, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

Общая оценка проблем информационной безопасности

В настоящем документе Соединенное Королевство будет использовать термин «кибербезопасность» и соответствующие концепции с особым упором на усилия, направленные на сохранение конфиденциальности, доступности и целостности информации в кибернетическом пространстве. Термин «информационная безопасность» часто используется деловыми кругами и нормативными организациями для определения одного и того же понятия, и именно этот термин также используется Соединенным Королевством с учетом этого конкретного значения. Существуют определенные возможности для недопонимания в плане использования термина «информационная безопасность» в том смысле,

что он используется некоторыми странами и организациями как часть их доктрины, в рамках которой информация как таковая рассматривается как угроза и, соответственно, для ее защиты требуются дополнительные меры. Соединенное Королевство не признает приемлемость термина «информационная безопасность», когда он используется в этом контексте, поскольку его можно также использовать в рамках усилий по легитимизации дальнейшего контроля за свободой слова сверх тех мер контроля, которые определены во Всеобщей декларации прав человека и Международном пакте о международных и политических правах.

Кибернетическое пространство является сферой, предоставляющей большие возможности, однако оно также является и сферой для реальных и потенциальных угроз. В настоящее время более 2 миллиардов человек имеют доступ к кибернетическому пространству через посредство сети Интернет, причем их число продолжает расти по мере того, как создание мобильных технологий позволяет развивающимся странам в полной мере пользоваться ее огромными выгодами при более низких издержках. Сеть Интернет обеспечивает локомотив для экономического роста, открывает доступ к образованию, укрепляет взаимодействие и взаимопонимание между людьми, разрушает культурные и географические барьеры, позволяет предоставлять услуги в интерактивном режиме и укрепляет демократию путем повышения отчетности правительств перед их гражданами с использованием новых и динамических средств. Например:

- базирующаяся в Интернете деятельность уже обеспечивает 8 процентов валового внутреннего продукта Соединенного Королевства. Обеспечение того, чтобы предприниматели и покупатели чувствовали себя безопасно в процессе осуществления деятельности в кибернетическом пространстве, имеет решающее значение для экономического роста;

- в 2011 году Соединенное Королевство создало службу электронных петиций, что позволяет любому человеку открыть или подписать петицию по вопросу, ответственность за который несет правительство. Все петиции, собравшие 100 000 подписей или более, подлежат рассмотрению в парламенте. В течение первого года осуществления этой инициативы было открыто для подписания более 15 600 петиций, из которых 10 превысили пороговый лимит в 100 000 подписей. Все эти петиции были либо обсуждены, либо планируются к обсуждению в рамках парламентских дебатов.

Соединенное Королевство, как и многие другие страны, использует кибернетическое пространство во многих областях, имеющих критически важное значение для таких национальных служб, как энергетика, финансы и транспорт. Существенные срывы в работе этих служб, будь то по не зависящим от человека причинам или в результате преднамеренной атаки, могут причинить серьезный экономический ущерб или потерю жизни.

Ландшафт террористических угроз имеет сложный и динамический характер. Системы управления правительства Соединенного Королевства, а также предпринимателей и частных лиц часто подвергаются попыткам проникновения на ежедневной основе. Среди причин следует указать как политический, так и промышленный шпионаж, кибернетическую преступность, намерение срыва или контроля за деятельностью сетей или отказ в получении обслуживания. Среди субъектов, которые создают угрозы, следует отметить государства, субъектов, действующих от имени государств, негосударственных субъектов и

организованные преступные сообщества, а также индивидуальных лиц. Взаимосвязанный характер кибернетического пространства означает, что совершение деструктивной деятельности в отношении одной системы может привести к непреднамеренным и непредсказуемым последствиям в других системах. Попытки противодействия этим угрозам затрудняются в результате того, что иногда трудно определить конкретный источник кибернетической угрозы, поэтому виновные лица часто скрываются, используя личные данные других лиц, недостаточное понимание адекватного поведения государств в кибернетическом пространстве, отсутствие защищенности кибернетической инфраструктуры в некоторых странах и отсутствие согласованного международного подхода к вопросам обнаружения, преследования и наказания киберпреступников.

Все элементы общества должны играть определенную роль и выполнять обязанности по борьбе с такими угрозами. Правительства должны возглавить международные усилия по повышению понимания относительно приемлемого государственного поведения и относительно борьбы с киберпреступностью. Однако, учитывая, что большинство объектов инфраструктуры в кибернетическом пространстве принадлежит или эксплуатируется частными компаниями, их участие в рассмотрении данных вопросов имеет критически важное значение. Соединенное Королевство считает, что укрепление кибернетической безопасности не должно осуществляться в ущерб экономическим и социальным выгодам, которые обеспечивает кибернетическое пространство. Особенно важно обеспечить, чтобы усилия по повышению кибернетической безопасности не использовались в неблагоприятных целях для установления дальнейших ограничений на свободу слова сверх тех ограничений, которые предусматриваются в международных соглашениях. В этой связи особенно важную роль играют организации гражданского общества.

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

Национальные подходы

Стратегия Соединенного Королевства в области национальной безопасности, опубликованная в 2010 году, рассматривает кибернетические преступления как одну из четырех угроз «уровня 1» наряду с международными военными кризисами, крупными авариями или национальными стихийными бедствиями или террористическими нападениями. В ноябре 2011 года Соединенное Королевство опубликовало обновленную стратегию в области кибернетической безопасности, в которой определяется концепция, предусматривающая получение огромных экономических и социальных выгод в результате использования динамичного, активного и безопасного кибернетического пространства, в котором наши действия, основывающиеся на наших ключевых ценностях свободы, справедливости, транспарентности и верховенства права, содействуют повышению благополучия, укреплению национальной безопасности и консолидации общества. Реализация этой стратегии обеспечивается с учетом четырех целей:

- борьба с киберпреступностью и превращение киберпространства в наиболее безопасное место в мире для осуществления предпринимательской деятельности;
- обеспечение большей защищенности перед лицом кибернетических преступлений и повышение возможностей по защите наших интересов в кибернетическом пространстве;
- оказание помощи в деле формирования открытого, устойчивого и динамичного кибернетического пространства, которое граждане Соединенного Королевства могли бы использовать безопасно и которое будет содействовать созданию открытого общества;
- обеспечение передового уровня знаний, навыков и потенциала, необходимых для достижения всех наших целей в области кибернетической безопасности.

В целях обоснования потребностей, необходимых для достижения этих целей, правительство Соединенного Королевства выделило 650 млн. фунтов стерлингов в рамках дополнительных расходов, которые будут использоваться в реализации рассчитанной на четыре года программы, предназначенной для трансформации реагирования на кибернетические угрозы.

Соединенное Королевство осуществило инвестиции в создание новых уникальных возможностей по защите своих основных сетей и служб и углублению своего понимания возникающих угроз. В свою очередь углубление знаний позволило лучше обеспечить приоритизацию непосредственных усилий в области кибернетической защиты. Под эгидой министерства обороны Соединенного Королевства в стране было создано включающее три службы подразделение с целью разработки новой тактики, методики и планов по использованию военных возможностей в деле реагирования на современные угрозы. Правительство тесно взаимодействует с жертвами преступной кибернетической деятельности, и результаты этой деятельности позволяют ему обеспечивать консультации для отраслей промышленности с целью повышения их потенциала по принятию мер в области кибернетической безопасности. Что касается собственных сетей, то Соединенное Королевство создало новую модель безопасности для обмена опытом деятельности служб, включая более современную аутентификацию сотрудников, обеспечение более строгого соблюдения существующих положений и повышение защищенности сетей.

Правительство Соединенного Королевства осуществило большие инвестиции в укрепление потенциала органов правопорядка и прокуратуры по предотвращению, пресечению и расследованию кибернетических преступлений и привлечению виновных лиц к ответственности. Численность персонала центрального управления полиции по борьбе с электронной преступностью была увеличена в три раза, и в настоящее время созданы три региональные группы кибернетического патрулирования, которые проводят подготовку по борьбе с киберпреступностью для регулярных сотрудников полиции. В конце 2013 года Агентство по борьбе с серьезной организованной преступностью будет объединено с Центральным управлением полиции по борьбе с электронной преступностью с целью создания национального управления по борьбе с кибернетической преступностью при Национальном агентстве по борьбе с преступностью, что является еще одним шагом с целью укрепления потенциала право-

применительных органов Соединенного Королевства в области борьбы с киберпреступностью.

Промышленные предприятия Соединенного Королевства являются самой крупной жертвой киберпреступности, включая широко распространенные случаи кражи интеллектуальной собственности. Правительство взаимодействует с промышленными и научными кругами с целью повышения осведомленности о необходимости борьбы с кибернетическими угрозами, и в 2012 году правительство подготовило пособие для руководителей отраслей промышленности, в котором излагаются положения, касающиеся того, как старшие руководящие сотрудники должны применять стратегию для защиты их наиболее ценных информационных активов. Правительство также успешно завершило экспериментальную инициативу по обмену информацией с целью создания надежной окружающей среды для организаций в целях обмена информацией о существующих угрозах и разрешения возникших проблем. В этой инициативе принимает участие порядка 160 компаний, действующих в областях обороны, финансов, фармацевтики, энергетики и телекоммуникаций.

Совместно с промышленными кругами правительство Соединенного Королевства осуществляет активную деятельность по повышению осведомленности об угрозах представителей индустриальной и государственной сфер, с тем чтобы они могли принимать зачастую довольно простые меры по обеспечению своей защиты и повышению безопасности кибернетической продукции и услуг. Эти инициативы включают инициативы под названием «Неделя обеспечения безопасности Интернета» (“Gen Safe Online Week”) (осуществляется совместно с Европейским союзом и Канадой), целью которой является проведение интерактивных кампаний по борьбе с мошенничеством через посредство Национального управления по борьбе с мошенничеством и в рамках кампании «Дьявол кроется в деталях» (“Devils in your details”), которая была осуществлена в 2012 году.

Соединенное Королевство осуществляет инвестиции в повышение квалификации и проведение научных исследований, с тем чтобы страна обладала потенциалом по своевременному реагированию на эту проблему в будущем. Первые восемь университетов Соединенного Королевства, которые провели исследования по вопросам кибербезопасности, получили статус передовых научных центров в области исследований по вопросам кибернетической безопасности. Осуществляется подготовка интерактивных учебных материалов для учащихся, и было начато осуществление инициативы по совершенствованию технических навыков с целью выявления и развития талантливых учащихся в школах и университетах. С тем чтобы обеспечить получение надлежащих навыков и образования лицами, работающими в области кибербезопасности, была учреждена система или сертификация сотрудников, работающих в области информационной безопасности, которая будет содействовать тому, чтобы органы правительства и отрасли промышленности нанимали на соответствующие должности специалистов в области кибербезопасности, которые обладают надлежащими навыками.

Международные подходы

Соединенное Королевство находится на передовом рубеже международных усилий по повышению транспарентности, предсказуемости и стабильно-

сти кибернетического пространства. В ноябре 2011 года Соединенное Королевство провело первую международную конференцию по кибернетической безопасности, в которой приняли участие представители более чем 60 стран и организаций предпринимателей и гражданского общества с целью обсуждения путей расширения экономических и социальных выгод от сотрудничества в кибернетическом пространстве в целях пресечения кибернетической преступности, обеспечения безопасного и надежного доступа к сети Интернет и поддержания международной безопасности. Инициативы, разработанные в ходе этого мероприятия, были впоследствии рассмотрены на конференции 2012 года, состоявшейся в Будапеште. Кроме того, уже планируется проведение конференции 2013 года, которая должна состояться в Сеуле.

Соединенное Королевство является активным членом Группы правительственных экспертов по достижениям в сфере информации и телекоммуникаций в контексте международной безопасности, а также неформальной рабочей группы Организации по безопасности и сотрудничеству в Европе (ОБСЕ) по укреплению мер доверия в кибернетическом пространстве.

В октябре 2012 года Соединенное Королевство приступило к осуществлению инициативы по созданию центра глобальной кибернетической безопасности, который будет финансироваться в размере 2 млн. фунтов стерлингов в год и будет реализовывать различные многосторонние и двусторонние инициативы. Центр будет предоставлять независимые консультативные услуги и информацию другим странам по вопросам создания более надежных и более защищенных национальных объектов инфраструктуры и будет служить в качестве координационного центра для проведения передовых исследований и международного сотрудничества по этому важному вопросу.

В целях содействия международным усилиям по борьбе с международной киберпреступностью Соединенное Королевство продолжает пропагандировать Конвенцию о кибербезопасности и ее принципы в качестве наиболее эффективного инструмента в этой области. Агентство по серьезной организованной преступности во взаимодействии с международными партнерами продолжает играть руководящую роль в международной деятельности по глобальным правоприменительным вопросам, касающимся Корпорации по присвоению имен и номеров в Интернете.

Соответствующие международные концепции, направленные на укрепление безопасности глобальных информационных и телекоммуникационных систем

Основополагающая концепция заключается в применении международного права и существующих норм поведения, которые регулируют отношения между государствами. Соединенное Королевство твердо убеждено в том, что эти принципы в равной мере применяются и к кибернетическому пространству, и считает, что конкретное заявление государств о том, что в своей деятельности в кибернетическом пространстве они будут руководствоваться этими законами и нормами, создаст основы для более мирного, предсказуемого и безопасного кибернетического пространства.

В этой связи кибернетическое пространство связано с определенными проблемами, например трудности в получении достоверных сведений об источнике деятельности, оценка намерений и роль неправительственных субъек-

тов. Соединенное Королевство выступает за проведение международных дискуссий по вопросу о том, как применять международное право и нормы государственного поведения в этом контексте.

Соединенное Королевство не считает, что попытки заключить всеобъемлющие международные договоры, кодексы поведения или аналогичные документы внесут позитивный вклад в повышение кибербезопасности в обозримом будущем. Сложный и всеобъемлющий характер любого имеющего обязательный характер соглашения в отношении всех вопросов, касающихся киберпространства, которое развивается со скоростью «сети», означает, что оно не будет эффективным и не получит всеобъемлющую поддержку в течение многих лет, возможно десятилетий, без осуществления напряженной работы по разработке норм поведения и мер укрепления доверия, с тем чтобы сформировать необходимое взаимопонимание и доверие среди стран, подписавших такое соглашение, и обеспечить, чтобы их можно было бы надлежащим образом привлекать к ответственности в целях обеспечения соблюдения ими взятых на себя обязательств. Опыт заключения таких соглашений по другим темам свидетельствует о том, что они могут иметь большое значение и быть эффективными только в случае успешного завершения дипломатических усилий по разработке совместных взаимопониманий и подходов, а не в качестве отправной точки. Соединенное Королевство считает, что усилия международного сообщества должны быть сосредоточены на разработке общего понимания международных норм и правил, а не на ведении переговоров по заключению обязательных соглашений, которые приведут только к частичному или преждевременному применению подхода к этой сфере, которая в настоящее время еще не сформировалась достаточным образом, чтобы обеспечить ее поддержку.

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

Трансграничный характер киберпространства делает особенно императивной необходимость того, чтобы государства заключили двусторонние, региональные и многосторонние меры в области сотрудничества для разработки общих мер реагирования на общие угрозы. По мнению Соединенного Королевства, меры, которые могли бы внести существенный вклад в этой области на данном этапе, заключаются в следующем:

a) проведение дальнейших дискуссий между государствами по разработке нормативных основ приемлемого государственного поведения на основе существующих принципов международного права и норм международного обычного права;

b) разработка мер укрепления доверия, применимых к киберпространству, которые будут направлены на повышение транспарентности и предсказуемости государственного поведения, и тем самым приведут к сокращению риска возникновения недопонимания или непреднамеренной эскалации инцидентов;

c) создание компьютерных групп чрезвычайного реагирования государствами в качестве координационного форума для решения проблем и обмена информацией при условии обеспечения необходимых уведомлений о ключевых координаторах и надежных механизмах коммуникации в случае кризиса;

d) проведение совместных учений для апробирования совместных процедур регулирования конфликтов и процедур в области коммуникации;

e) разработка согласованных правовых подходов к решению проблемы киберпреступности;

f) активизация диалога с представителями деловых кругов и гражданского общества для обеспечения скоординированных и приоритизированных подходов к этой сфере, которая в значительной мере находится в собственности частного сектора и регулируется им;

g) принятие государствами, имеющими более значительный потенциал в области кибербезопасности, обязательств по оказанию поддержки в наращивании такого потенциала другими государствами.