Организация Объединенных Наций A/71/172

Генеральная Ассамблея

Distr.: General
19 July 2016
Russian
Original: Arabic/English/French/
Russian/Spanish

Семьдесят первая сессия
Пункт 94 предварительной повестки дня*

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Содержание

* A/71/150.

16-12486 (R) 110816 150816

I. Введение

1. 23 декабря 2015 года Генеральная Ассамблея приняла резолюцию 70/237, озаглавленную «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». В пункте 4 этой резолюции Ассамблея просила все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/70/174), 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 3 резолюции;

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

2. Во исполнение этой просьбы 15 февраля 2015 года всем государствам-членам была направлена вербальная нота с предложением предоставить информацию по данной теме. Ответы, полученные на момент составления настоящего доклада, приводятся в разделе II. Все остальные полученные ответы будут опубликованы в качестве добавлений к настоящему докладу. С полным текстом всех сообщений можно ознакомиться по адресу: www.un.org/disarmament/topics/informationsecurity.

II. Ответы, полученные от правительств

Албания

[Подлинный текст на английском языке]
[15 апреля 2016 года]

Приоритетная задача Албании в области обеспечения безопасности и защиты конфиденциальной информации заключается в выполнении положений заключенного между правительством Республики Албания и Европейским союзом соглашения о процедурах обеспечения безопасности при обмене конфиденциальной информацией и ее защиты. Это соглашение было подписано 3 марта 2016 года в Тиране, и ожидается, что в ближайшее время оно будет ратифицировано Народным собранием Республики Албания.

В контексте разработки и принятия надлежащих мер, а также с целью укрепления информационной безопасности и поощрения международного сотрудничества в этой области в Албании был проведен пересмотр нормативно-правовой базы.

– Решение Совета министров № 188 от 4 марта 2015 года «Об утверждении правил обеспечения безопасности персонала»

– Решение Совета министров № 189 от 4 марта 2015 года «Об обеспечении физической сохранности конфиденциальной информации с пометкой „государственная тайна“, „информация НАТО“»

– Решение Совета министров № 190 от 4 марта 2015 года «О внесении некоторых изменений и дополнений в решение Совета министров № 81 „Об определении критериев и процедур уничтожения конфиденциальной информации“»

– Решение Совета министров № 701 от 22 октября 2014 года «Об утверждении правил обеспечения сохранности конфиденциальной информации в промышленной сфере»

Нормативно-правовая база Албании, касающаяся физической безопасности конфиденциальной информации, была усовершенствована. С учетом различных уровней конфиденциальной информации были пересмотрены и перераспределены так называемые «зоны безопасности».

После принятия нового решения о безопасности персонала постепенно увеличились масштабы институционального сотрудничества, контроля и наблюдения за деятельностью государственных учреждений. Государственные учреждения приступили к пересмотру списков должностных обязанностей и выпуску соответствующих сертификатов в области безопасности в зависимости от сферы ответственности.

Что касается обеспечения безопасности в промышленной сфере, то Албания уделила пристальное внимание обзору политики в области информационной безопасности, а также обзору практики в контексте решения Совета министров № 701 от 22 октября 2014 года.

Еще одна важная задача, которой мы уделяем пристальное внимание, заключается в составлении проекта нового закона об обращении с конфиденциальной информацией, который станет эффективным и современным правовым инструментом, отвечающим высоким европейским стандартам. Обзор национального законодательства в этой области проводится с учетом нормативно-правовой базы Европейского союза, и в частности решения Совета 2013/488/EU о правилах безопасности и защиты конфиденциальной информации в Европейском союзе.

Австралия

[Подлинный текст на английском языке]
[31 мая 2016 года]

Австралия рада возможности представить в ответ на просьбу, изложенную в резолюции 70/237 Генеральной Ассамблеи, свое мнение о положении дел в области информатизации и телекоммуникаций в контексте международной безопасности. Соответствующая информация представляется в дополнение к сведениям, представленным Австралией в 2014 году в связи с резолюцией 68/243 и в 2011 году в связи с резолюцией 65/41.

Кибербезопасность так же неразрывно связана с новаторской деятельностью, как и с национальной безопасностью. Это фундамент инноваций, роста и процветания. Кибербезопасность представляет собой сферу глобальных воз-

можностей, в которой участвуют и из которой извлекают выгоду правительства, частный сектор и общество.

Мировое сообщество должно уделить вопросу кибербезопасности самое пристальное внимание. Чтобы создать надежную интерактивную среду, все участники процесса — правительство, субъекты предпринимательства и частные лица — должны работать сообща. Это нужно не только для того, чтобы защитить важнейшую информацию, но и для того, чтобы обеспечить условия для процветания новаторства; расширения возможностей для развития индустрии технологий; и удовлетворения растущих глобальных потребностей в более эффективных решениях в области кибербезопасности, в оборудовании и в квалифицированном персонале.

Австралия считает, что высокий уровень кибербезопасности — это непременное условие обеспечения роста и процветания в мировой экономике. В 2015 году Австралия пересмотрела свой подход кибербезопасности и 21 апреля 2016 года приступила к осуществлению своей новой стратегии в области кибербезопасности.

По мнению Австралии, приоритетная задача международного сообщества заключается в определении того, как нормы международного права применяются к поведению государств в киберпространстве, особенно в неконфликтных ситуациях. По-прежнему существует необходимость проделать дальнейшую работу для углубления понимания того, как основные принципы, такие как суверенитет и юрисдикция, действуют в киберпространстве, принимая во внимание общий интерес человечества в сохранении глобальной природы Интернета. Существуют также возможности для дальнейшей доработки норм добровольного характера, изложенных в докладе Группы правительственных экспертов 2015 года, в отношении защиты критически важной инфраструктуры, деятельности групп реагирования на нарушения компьютерной защиты, обязанности государств оказывать помощь и сотрудничества в области борьбы с киберпреступлениями и предотвращения распространения вредоносных инструментов и технологий. Важно сделать так, чтобы работа над формулированием мер по укреплению доверия перешла на следующий этап: от поощрения транспарентности к принятию мер на основе сотрудничества.

Канада

[Подлинный текст на английском языке]
[27 мая 2016 года]

По вопросу о кибербезопасности Канада желает заявить следующее:

- Свободное, открытое и безопасное киберпространство имеет решающее значение для мировой безопасности, экономического процветания и поощрения прав человека, демократии и инклюзивности.
- Любой подход к противостоянию киберугрозам должен основываться на уважении к правам человека и основным свободам.
- Существующие нормы международного права применяются к использованию информационно-коммуникационных технологий государствами.

- Поощрение норм мирного времени способствует поддержанию среды, в которой ответственное поведение лежит в основе деятельности государств, способствует сохранению партнерских отношений и обеспечивает стабильное киберпространство.
- Практические меры укрепления доверия являются испытанным методом снижения напряженности и риска вооруженного конфликта.

Что касается мер, принимаемых на национальном уровне, то со времени обнародования правительством Канады в 2010 году его стратегии в области кибербезопасности, оно продолжает работу над содействием обеспечению безопасности канадских киберсистем и защиты деятельности канадцев в Интернете. За это время Канада также приступила к осуществлению информационной кампании под названием «Защити себя в киберпространстве». Недавно правительство обязалось провести обзор существующих мер по обеспечению защиты граждан и критических объектов инфраструктуры от киберугроз.

Что касается мер, принимаемых на международном уровне, то Канада активно участвует в следующих видах связанной с кибербезопаностью деятельности:

- Канада намеревается и впредь содействовать разработке норм мирного времени, касающихся поведения государств в киберпространстве, включая выполнение рекомендаций, вынесенных Группой правительственных экспертов Организации Объединенных Наций в 2012–2013 и 2014–2015 годах. Канада будет участвовать в работе Группы в 2015–2016 году.
- В июле 2015 года Канада ратифицировала Будапештскую конвенцию. Канада призывает другие страны стать участниками Конвенции или использовать ее в качестве модели при принятии их собственных законов в области киберпреступности.
- Начиная с 2007 года Канада выделила 8,25 млн. долл. США на поддержку проектов по наращиванию потенциала в области кибербезопасности в Северной и Южной Америке и Юго-Восточной Азии.
- Канада является одним из партнеров-основателей Глобального форума по обмену опытом в области компьютерных технологий.
- Канада сотрудничает с Соединенными Штатами в области унификации инициатив обеих стран по проведению общественных информационных кампаний по теме кибербезопасности в рамках коалиции «Остановись. Подумай. Подключись».
- Канада также сотрудничает с Соединенными Штатами в области внедрения совместного плана действий Канады и Соединенных Штатов в области кибербезопасности, целью которого является повышение сопротивляемости киберинфраструктуры обеих стран.
- Канада участвует в разработке мер укрепления доверия в рамках различных форумов, в том числе Организации по безопасности и сотрудничеству в Европе и Регионального форума Ассоциации государств Юго-Восточной Азии.

- Канада поддерживает усилия Организации Североатлантического договора (НАТО) в области укрепления систем кибербезопасности Организации и ее отдельных членов. Канада предоставила средства в размере 1 млн. долл. США для Экспертного центра НАТО по совместной кибероборонe.
- Канада поддерживает использование информационно-коммуникационных технологий (ИКТ) в качестве инструментов развития, в том числе для оказания помощи общественным организациям в предоставлении важнейших услуг, таких как экстренная помощь в условиях конфликтов.
- Канадский Международный исследовательский центр по проблемам развития вносит свой вклад в поощрение развития по всему миру, проводя научные исследования и мероприятия по наращиванию потенциала в области использования ИКТ в интересах развития.

Колумбия

[Подлинный текст на испанском языке]
[13 июня 2016 года]

Посредством реализации своего плана «Цифровые технологии для жизни» (2010–2014 годы) и нового плана «Цифровые технологии для людей» (2014–2018 годы) Колумбия осуществила цифровую революцию, в результате которой общее количество пользователей Интернета всего за пять лет возросло с 2,2 млн. человек до более чем 12,2 млн. человек. Колумбия станет первой латиноамериканской страной, обеспечившей высокоскоростной доступ к Интернету во всех своих муниципалитетах. За указанный период образовательным учреждениям было выделено более 2 млн. компьютерных терминалов; 74 процента микропредприятий, малых и средних предприятий теперь подключены к Интернету (по сравнению 7 процентами в 2010 году); мы добились 90-процентного увеличения количества пользующихся Интернетом домашних хозяйств; мы также обеспечили доступ в Интернет для жителей самых отдаленных сельских районов благодаря установке в рамках программы «Цифровые технологии для жизни» 7621 киоска в сельских центрах с населением более 100 человек. Помимо многих других достижений, в нашей стране теперь существует самое большое сообщество цифровых предпринимателей в Латинской Америке, насчитывающее более 100 000 членов.

Национальное правительство понимает, что невозможно извлекать из использования информационно-коммуникационных технологий максимальную выгоду и эффективно применять их, если граждане или субъекты предпринимательства не могут им доверять — другими словами, если цифровая среда считается недостаточно безопасной. Растущее число инцидентов в области компьютерной безопасности оказывает все большее воздействие на восприятие людей.

а) Меры, принятые на национальном уровне для укрепления информационной безопасности и поощрения международного сотрудничества в этой области

В 2016 году Колумбия приступила к осуществлению новой национальной стратегии в области цифровой безопасности, которая изложена в документе CONPES 3854 и целью которой является обеспечение того, чтобы правитель-

ство, общественные и частные организации, персонал правоохранительных органов, научные сотрудники и население Колумбии в целом могли иметь доступ к безопасной и надежной цифровой среде, предназначенной для максимальной реализации экономических и социальных выгод, поощрения конкуренции и повышения продуктивности во всех секторах экономики. Эта стратегия стала результатом процесса взаимодействия многих заинтересованных сторон и является одной из первых национальных стратегий в мире и первой стратегией в регионе, в которой учтены рекомендации по управлению рисками в области информационной безопасности, вынесенные Организацией экономического сотрудничества и развития в сентябре 2015 года.

Стратегия предусматривает в первую очередь создание четкой институциональной структуры по вопросам цифровой безопасности. В этой связи на самом высоком правительственном уровне будут созданы координационные и надзорные органы по вопросам цифровой безопасности, а во всех органах исполнительной власти будут созданы группы по межсекторальным связям. Во-вторых, будут созданы благоприятные условия, позволяющие многим заинтересованным сторонам контролировать риски в области информационной безопасности в своей социально-экономической деятельности, а также укреплять доверие в вопросах использования цифровых технологий посредством создания механизмов для обеспечения активного и постоянного участия, создания надлежащей нормативно-правовой структуры и обеспечения возможностей для обучения по вопросам ответственного поведения в цифровой среде. В-третьих, на национальном и транснациональном уровнях будут приняты меры для укрепления национальных систем охраны и безопасности в контексте цифровых технологий на основе подхода, подразумевающего минимизацию рисков. И наконец — что не менее важно — на национальном и международном уровнях будут созданы постоянные механизмы, стратегической направленностью которых будет поощрение сотрудничества, взаимной работы и взаимопомощи в области цифровой безопасности.

b) Содержание концепций, упомянутых в пункте 3 резолюции 70/237

Колумбия как член Группы правительственных экспертов последнего созыва (2014–2015 годы) полностью согласна с тем, что существует необходимость в дальнейшем изучении концепций, связанных с безопасностью информации и глобальных телекоммуникационных систем, и вопросов, связанных с применением норм международного права в киберпространстве.

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

В свете вышеизложенного мы полностью согласны с важными рекомендациями, вынесенными на основе консенсуса экспертами, входившими в состав Группы правительственных экспертов, в том числе касающимися добровольных мер и передовой практики, а также мер по наращиванию потенциала и сотрудничества между государствами для поощрения использования информационно-коммуникационных технологий в мирных целях, с тем чтобы они могли по-прежнему служить инструментом экономического и социального развития для всех стран, особенно стран, менее продвинутых с технологической точки зрения.

Куба

[Подлинный текст на испанском языке]
[6 мая 2016 года]

Куба разделяет выраженную в резолюции 70/237 озабоченность тем, что информационные технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной безопасности и стабильности, и могут негативно воздействовать на целостность инфраструктуры государств, нарушая их безопасность применительно как к гражданской, так и к военной сферам.

Кроме того, в резолюции 70/237 сделан надлежащий упор на необходимость предотвратить использование информационных ресурсов или технологий в преступных или террористических целях.

В этой связи Куба вновь выражает глубокую обеспокоенность по поводу скрытого и незаконного использования отдельными лицами, организациями и государствами компьютерных систем других стран для совершения нападений на третьи страны, поскольку это в потенциальном плане способно провоцировать международные конфликты.

Единственным способом предотвращения и устранения этих угроз в целях недопущения превращения киберпространства в театр военных действий является сотрудничество между всеми государствами.

Использование телекоммуникаций в открытых или скрытых целях, заключающихся в подрыве юридического и политического строя государств, является нарушением международно признанных норм в этой области и может приводить к росту напряженности и возникновению ситуаций, способных иметь губительные последствия для международного мира и безопасности.

На состоявшемся в январе 2014 года в Гаване втором саммите Сообщества государств Латинской Америки и Карибского бассейна (СЕЛАК) главы государств и правительств стран Латинской Америки и Карибского бассейна провозгласили этот регион зоной мира и, среди прочего, обязались укреплять сотрудничество и дружественные отношения между собой и с другими государствами, вне зависимости от различий в их политических, экономических и социальных системах или уровнях развития, проявлять терпимость и жить вместе в мире друг с другом как добрые соседи.

На четвертом саммите СЕЛАК, состоявшемся в Кито в январе 2016 года, вновь была подчеркнута важность информационно-коммуникационных технологий, включая Интернет, в качестве средств поощрения мира, благосостояния человечества, развития, обмена знаниями, социальной интеграции и экономического роста. Также был вновь подтвержден принцип мирного использования информационно-коммуникационных технологий в соответствии с целями и принципами Устава Организации Объединенных Наций и нормами международного права, а также было вновь отмечено, что эти технологии ни при каких обстоятельствах не должны использоваться в целях разрушения общественного строя или создания ситуаций, способных провоцировать конфликты между государствами.

Тем не менее эти усилия по-прежнему находятся под угрозой срыва из-за того, что правительство Соединенных Штатов продолжает непрерывные трансляции радио- и телепрограмм на территорию Кубы в нарушение целей и принципов Устава Организации Объединенных Наций, различных положений Международного союза электросвязи, а также суверенитета Кубы.

С помощью этих незаконных радио- и телепередач совершаются постоянные нападения на информационное пространство Кубы, а также распространяются программы, специально предназначенные для подстрекательства к свержению конституционного строя, установленного кубинским народом. В качестве примера можно указать, что только в первом квартале 2016 года против Кубы были направлены незаконные передачи в объеме в среднем 1880 часов в неделю с использованием 23 частот.

Куба надеется на немедленное прекращение этой агрессивной политики, которые, кроме всего прочего, несовместима с налаживанием связей между Кубой и Соединенными Штатами на основе взаимного уважения и сотрудничества, как это было согласовано правительствами обеих стран на этапе восстановления дипломатических отношений.

Она также надеется, что экономическая, торговая и финансовая блокада, нанесшая серьезный урон кубинскому народу, будет отменена. Эта блокада оказывает пагубное воздействие на сектор информации и коммуникаций, а также на другие аспекты повседневной жизни кубинского народа.

Обязательным условием успешного противодействия угрозам, порождаемым неправомерным использованием информационно-коммуникационных технологий, является международное сотрудничество. Важную роль в межправительственных обсуждениях вопросов кибербезопасности должен сыграть Международный союз электросвязи.

Куба поддержала резолюцию 70/237 и будет и впредь вносить свой вклад в мирное глобальное развитие информационно-телекоммуникационных технологий и их использование на благо всего человечества.

Сальвадор

[Подлинный текст на испанском языке]
[26 апреля 2016 года]

Вооруженные силы Сальвадора осуществили модернизацию компьютерного оборудования для периметровой охраны и внедрили правила безопасности, регулирующие доступ к компьютерным сетевым ресурсам (регулярная смена паролей пользователей, ограничение доступа к портам USB и дисководам (DVD и CD), а также блокирование доступа к блоку оборудования C).

Финляндия

[Подлинный текст на английском языке]
[31 мая 2016 года]

Финляндия приветствует возможность предоставить информацию во исполнение резолюции 70/237 Генеральной Ассамблеи. Ниже приводится информация о принятых на национальном уровне мерах.

a) В национальной стратегии обеспечения кибербезопасности 2013 года и программе ее осуществления 2014 года изложены основные руководящие указания и меры по повышению уровня кибербезопасности и сопротивляемости. В настоящее время в рамках консультативного процесса с участием многих заинтересованных сторон проводится обновление программы осуществления стратегии с целью ее окончательной доработки в 2016 году.

b) С момента принятия национальной стратегии обеспечения кибербезопасности в Финляндии были созданы Национальный центр по вопросам кибербезопасности и Центр по предотвращению киберпреступлений, а также был назначен Посол по вопросам кибербезопасности. В феврале 2016 года была принята национальная стратегия по информационной безопасности.

c) В рамках сотрудничества в целях развития Финляндия поддерживает различные инициативы по использованию информационно-коммуникационных технологий (ИКТ) в целях развития, а также проекты по наращиванию потенциала в области кибербезопасности. Финляндия является одним из партнеров-основателей Глобального форума по обмену опытом в области компьютерных технологий. Финляндия присоединилась к осуществляемой под руководством Соединенных Штатов инициативе «Глобальная связь» (“Global Connect”), задача которой заключается в предоставлении доступа к Интернету 1,5 миллиарда человек к 2020 году. Финляндия намеревается присоединиться к недавно созданному Всемирным банком Целевому фонду партнерства в области развития цифровых технологий. Финляндия поддерживает управление использованием Интернета на основе модели, подразумевающей участие многих заинтересованных сторон.

d) Финляндия активно участвует в международном диалоге по вопросам компьютерных технологий в рамках многосторонних и региональных форумов, а также по линии двусторонних контактов. В рамках Организации по безопасности и сотрудничеству в Европе (ОБСЕ) Финляндия работает над укреплением доверия, безопасности и стабильности в киберпространстве и принимает согласованные меры по укреплению доверия и безопасности при использовании компьютерных технологий.

e) Финляндия одобрила подготовленный в 2015 году доклад Группы правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Финляндия активно участвует в обсуждениях, посвященных нормам международного права применительно к киберпространству, в том числе в консультациях по второй версии Таллинского руководства и в практикумах Института Организации Объединенных Наций по исследованию проблем разоружения. В 2012 году Финляндия присоединилась к организации

«Коалиция за свободу в Интернете», а также вносит свой вклад в работу Партнерства защитников цифровых прав.

f) С 2007 года Финляндия является участником Будапештской конвенции. В 2015 году был разработан стратегический план работы полиции, подразумевающий выделение ресурсов на предупреждение преступлений, совершаемых с помощью компьютеров, и разработку ноу-хау в области кибербезопасности. Также был разработан комплексный план предупреждения киберпреступлений.

Приоритетные направления дальнейшей работы международного сообщества, по мнению Финляндии, сводятся к следующему:

a) Финляндия придает большое значение работе новой Группы правительственных экспертов и готова внести вклад в успешное выполнение ею своих обязанностей, включая дальнейшее формулирование норм ответственного поведения государств в киберпространстве с особым упором на деятельность в мирное время.

b) Необходимо и далее разрабатывать и внедрять региональные меры укрепления доверия в рамках ОБСЕ.

c) Необходимо и далее поддерживать мероприятия по наращиванию потенциала в области компьютерных технологий с целью повышения уровня сопротивляемости и безопасности в киберпространстве;

d) Финляндия будет и впредь поддерживать и поощрять диалог с участием многих заинтересованных сторон. Также приоритетной задачей является укрепление партнерских связей между государственным и частным секторами на национальном и международном уровнях.

Индия

[Подлинный текст на английском языке]
[9 июня 2016 года]

Хотя информационные технологии способствуют экономическому росту и социальной сплоченности, в этой области есть серьезные проблемы, которые необходимо решить. Развитие сектора информационно-коммуникационных технологий сопровождается ростом киберугроз, к которым относятся угрозы кибернападений, киберпреступлений, кибертерроризма, шпионажа и отмывания денег. Факты свидетельствуют о том, что террористические группировки (например, ИГИЛ) используют Интернет и социальные сети в своих гнусных целях, в том числе для вербовки, мобилизации средств, пропаганды и радикализации. Злонамеренное использование социальных сетей вызывает серьезное беспокойство. Хотя они открывают огромные возможности для взаимодействия, они также могут использоваться в неправомерных в целях для усугубления этнической и социальной разобщенности.

Важно, чтобы международное сообщество пришло к общему мнению по поводу поведения государств в киберпространстве и приняло меры по укреплению доверия и безопасности в соответствии с рекомендациями, изложенными в докладе Группы правительственных экспертов Организации Объединенных Наций 2015 года. Дискуссии на тему управления использованием Интер-

нета не должны погрязать в болоте пустословных разногласий. Хотя различные заинтересованные стороны могут быть компетентными в своих соответствующих областях, в контексте национальной безопасности главную роль в вопросах кибербезопасности играют правительства. Существует необходимость в разработке надлежащих механизмов для обмена информацией о киберугрозах, киберпреступлениях и кибертерроризме. Также существует потребность в сотрудничестве в режиме реального времени между государственными учреждениями, занимающимися проблемой киберпреступности. Более того, на всех международных форумах должны обсуждаться такие вопросы, как войны в киберпространстве и идеологическая обработка с помощью компьютерных средств. Хотя правила ответственного поведения государств в киберпространстве пока находятся на стадии разработки, для принятия необходимых мер по наращиванию потенциала в области кибербезопасности можно было бы использовать общие идеи о мерах укрепления доверия, изложенные в докладе Группы правительственных экспертов Организации Объединенных Наций 2015 года. В этой связи полезным ориентиром могут служить рамки, разработанные Глобальным форумом по обмену опытом в области компьютерных технологий.

Индия является активным участником сектора информационно-коммуникационных технологий. Она поддерживает задействование многих заинтересованных сторон в вопросах управления использованием Интернета и на основе упреждающего подхода участвует в работе различных международных форумов, в том числе в работе Группы правительственных экспертов, открытых консультациях, посвященных общему обзору хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества, и работе Корпорации по присвоению имен и номеров в Интернете. Индия в консультации со всеми заинтересованными сторонами взяла за основу комплексный подход и приняла ряд политических, правовых, технических и административных мер для решения проблем в области кибербезопасности и поощрения международного сотрудничества в этой сфере. Ее нормативно-правовая база согласуется с нормативно-правовой базой других стран мира. В 2013 году была принята национальная политика в области кибербезопасности, целью которой является создание надежного и устойчивого киберпространства для граждан, участников предпринимательской деятельности и правительства. Ее основными элементами являются наращивание потенциала, развитие навыков и партнерские отношения между государственным и частным секторами в области кибербезопасности.

Япония

[Подлинный текст на английском языке]
[27 мая 2016 года]

Общее мнение по вопросу об информационной безопасности

Япония считает, что киберпространство должно быть таким пространством, где свобода гарантируется без ненужных ограничений и где все субъекты, желающие получить к нему доступ, не получают отказа и не оказываются в изолированном положении без правомерной причины. Предпринимаемые нами усилия в этой области основываются на следующих пяти принципах: свобод-

ное движение информации, верховенство права, открытость, самоуправление и участие многих заинтересованных сторон.

Усилия, прилагаемые на национальном уровне для укрепления информационной безопасности и поощрения международного сотрудничества в этой области

1. Усилия, прилагаемые на национальном уровне для укрепления информационной безопасности

Меры, принимаемые Японией в области укрепления информационной безопасности, основаны на Стратегии обеспечения кибербезопасности, разработанной в сентябре 2015 года.

2. Усилия, прилагаемые на национальном уровне для поощрения международного сотрудничества

Усилия Японии в этой области имеют три основных компонента: поощрение верховенства права в киберпространстве, принятие мер укрепления доверия и наращивание потенциала. Что касается поощрения верховенства права, то Япония активно участвует в международных дискуссиях, направленных на формирование общего мнения на предмет того, как действующие нормы международного права должны применяться в киберпространстве, а также для разработки необязательных и добровольных норм ответственного поведения государств. Что касается мер укрепления доверия, то Япония участвует в соответствующей деятельности в рамках двустороннего диалога и многосторонних форумов, таких как Ассоциация государств Юго-Восточной Азии (АСЕАН). Что касается наращивания потенциала, то Япония активно оказывает помощь в проведении мероприятий в области развития человеческого потенциала и участвует в проектах по линии технического сотрудничества с упором на страны АСЕАН.

Содержание концепций, упомянутых в пункте 3 резолюции

Подтверждение применимости международного права в киберпространстве и разработка необязательных и добровольных норм ответственного поведения в нем государств являются для международного сообщества основой для обеспечения стабильности и предсказуемости.

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

Что касается поощрения верховенства права, то Япония настаивает на необходимости продолжения обсуждений по поводу выработки норм международного права, относящихся к мирному времени, законов, касающихся права на самозащиту, и норм международного гуманитарного права, а также разработки добровольных норм в рамках последующей работы Группы правительственных экспертов. Что касается укрепления доверия и наращивания потенциала, то особо важно поощрять выполнение рекомендаций, содержащихся в докладах Группы, каждым государством или регионом. Также важно изучить возможные пути налаживания эффективного сотрудничества.

Иордания

[Подлинный текст на арабском языке]
[2 мая 2016 года]

Информационно-коммуникационные технологии стали неотъемлемой частью нашей повседневной жизни. Они способствуют социальному, культурному и экономическому росту и развитию местных общин в различных формах и во многом определяют взаимодействие людей со своими местными общинами и с внешним миром.

Чрезвычайно стремительное развитие информационно-коммуникационных технологий делает их уязвимыми перед лицом угроз и вызовов. Противодействие этим угрозам должно осуществляться с помощью технических и правовых средств, направленных на поиск эффективных и практических решений для смягчения рисков и предотвращения потенциально катастрофических последствий.

Иорданская армия играет активную и важную роль в деле поощрения мира и безопасности на национальном, региональном и глобальном уровнях, в том числе посредством разработки технологий, которые она использует для защиты информации и проводной и беспроводной связи. В качестве примеров ее деятельности можно привести следующие:

a) на всей территории Королевства, в том числе на границах, были усовершенствованы информационно-коммуникационные системы и внедрены защищенные сети с использованием технологии шифрования данных, передаваемых по протоколу IP, что было сделано для повышения уровня национальной и региональной безопасности;

b) Армия осуществляет сотрудничество в области безопасности с международным сообществом, используя коммуникационные системы, совместимые с системами, используемыми Организацией Североатлантического договора и армией Соединенных Штатов, и относящиеся к типу 1 международных стандартов шифрования;

c) технические возможности Армии были расширены благодаря приобретению инфраструктурно независимой системы связи, используемой для целей поддержания национальной безопасности в зонах конфликта, в лагерях беженцев и в отдаленных районах. Иорданская армия также использует эту технологию при осуществлении операций по поддержанию мира в зонах конфликтов по всему миру;

d) она самостоятельно (без привлечения поставщика) осуществляет обучение и сертификацию всех пользователей систем связи, а также технического и вспомогательного персонала, стремясь обеспечить максимальную надежность и безотказность при любых обстоятельствах;

e) ко всем системам, используемым вооруженными силами, применяются самые высокие стандарты контроля и управления, с тем чтобы обеспечить более высокий уровень координации и сотрудничества в вопросах обеспечения национальной и региональной безопасности;

f) Армия принимает активное участие в международных конференциях и следит за их итогами, преследуя цель повысить уровень взаимодействия между дружественными армиями, избежать помех при использовании коммуникационных систем соседними государствами региона и обеспечить скоординированный контроль и наблюдение на международных границах.

Всегда нужно уделять самое пристальное внимание обеспечению осведомленности граждан о наличии повсеместных киберугроз и о том, как соблюдение мер кибербезопасности при использовании электронных систем может свести к минимуму или ликвидировать эти угрозы. Повышение информированности в вопросах безопасности при обращении с какой-либо информацией не должно противоречить использованию технических достижений на благо людей.

Ниже перечислены меры, которые были приняты для защиты жизненно важных национальных информационных сетей:

a) использование алгоритмов шифрования для защиты коммуникационных систем для передачи голоса, данных и видео;

b) использование закрытых сетей (интранет);

c) налаживание связи с другими службами безопасности посредством использования обособленных периферийных устройств;

d) применение способов защиты информационно-коммуникационных систем и принципа минимальной необходимой осведомленности. Разрешения на доступ и личности пользователей проверяются на постоянной основе;

e) использование виртуальных сетей, при котором пользователь работает с экраном, связанным с сетью на основе разрешений на доступ к информации. Доступ или связь не могут быть обеспечены посредством каких-либо других устройств, таких как флеш-накопители;

f) Иордания разработала или приняла следующие нормативные акты в области кибербезопасности:

1) был принят закон о киберпреступности;

2) был принят закон об электронных сделках;

3) был разработан проект национальной стратегии по обеспечению кибербезопасности и защиты;

4) была разработана национальная политика в области кибербезопасности и защиты;

5) национальная стратегия по обеспечению кибербезопасности и защиты была утверждена Кабинетом министров в 2012 году.

Мы считаем, что на глобальном уровне должны быть приняты следующие меры:

a) коммуникационные сети и информация должны классифицироваться по принципу значимости;

b) необходимо принимать меры в области кибербезопасности и защиты;

c) необходимо применять принцип минимальной необходимой осведомленности;

d) следует использовать такие технические приемы, как шифрование и переключение частоты;

e) информация о пользователях и разрешениях на доступ к сети должна проверяться и классифицироваться;

f) сети должны быть связаны с помощью обособленных периферийных устройств;

g) в отношении некоторых категорий связи следует использовать закрытые внутренние сети и по возможности избегать использования Интернета;

h) необходимо усовершенствовать внутреннюю сеть Организации Объединенных Наций и использовать ее отдельно от общедоступных сетей. Она должна быть защищена с помощью технических средств и мер безопасности, таких как шифрование, элементы защиты и проверка разрешений на доступ;

i) следует поощрять сотрудничество между группами реагирования на нарушения компьютерной защиты с целью отслеживания происшествий, принятия мер безопасности и устранения пробелов;

j) необходимо распространять информацию о мерах безопасности и процедурах анализа нарушений.

Мы хотели бы особо подчеркнуть, что информационно-коммуникационные технологии могут внести большой вклад в обеспечение устойчивого развития, особенно в наиболее бедных и наиболее отдаленных районах, следующим образом:

a) Они могут способствовать ускорению процесса искоренения нищеты, в том числе, например, с помощью мобильных банковских услуг, которые во всем мире принесли прямые и ощутимые выгоды для миллионов людей, которые не имели опыта взаимодействия с банками.

b) Современные технологии и новые средства связи могут уменьшить масштабы голода, потому что благодаря им фермеры смогут получать важнейшую информацию о том, какие сельскохозяйственные культуры им следует выращивать.

Рекомендации:

a) Необходимо сформировать международные группы реагирования и восстановления, которые будут устранять инциденты, кризисы и катастрофы в области кибербезопасности.

b) В состав учрежденной Организацией Объединенных Наций Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности в 2016 году должен войти представитель Иордании.

c) Необходимо расширить сотрудничество в области научных исследований и профессиональной подготовки среди членов Совета Безопасности.

Ливан

[Подлинный текст на арабском языке]
[24 мая 2016 года]

Кибербезопасность в современном мире влияет на целый ряд экономических, социальных, политических, военных и гуманитарных вопросов. В будущем одной из наиболее серьезных угроз как для супердержав, так и для развивающихся государств станет кибертерроризм.

Информационные войны ведутся на нескольких фронтах и включают в себя такие аспекты, как вербовка и мобилизация средств через специальные веб-сайты, психологическое воздействие, обмен информацией и ее распространение через Интернет, электронное взламывание веб-сайтов и информационных систем, а также кибертерроризм.

Угроза кибертерроризма для всех государств становится все сильнее. Ливан стал жертвой ряда кибернападений, направленных в первую очередь против банковского сектора (вирус «Гаусс») и сектора связи. Нападениям регулярно подвергается большинство электронных сервисов.

Ниже перечислены усилия, принятые на национальном уровне для поощрения кибербезопасности и международного сотрудничества.

- В 1999 году были приняты Закон № 140 о конфиденциальности телекоммуникаций и Закон № 75 об интеллектуальной собственности. В обоих законах в некоторой степени затрагиваются вопросы нарушения авторских прав на программное обеспечение.
- В 2006 году на базе Отдела уголовных расследований Генерального директората Внутренних сил безопасности было создано Управление по борьбе с киберпреступностью и защите интеллектуальной собственности.
- В 2007 году было создано Управление по регулированию связи, которое стало активным членом Международного многостороннего партнерства по борьбе с киберугрозами (IMPACT).
- В 2009 году командование вооруженных сил создало на базе Разведывательного управления Отдел по электронной криминалистической экспертизе.
- Министерство обороны в сотрудничестве с национальными и международными органами работает над созданием в Ливане группы по реагированию на происшествия, связанные с компьютерной безопасностью. Оно принимает участие во всех соответствующих инициативах, а также проводит конференции и учебные курсы.
- В 2012 году Кабинет министров принял решение создать Комитет национальной безопасности, отвечающий за хостинг правительственных веб-сайтов. В состав Комитета входит представитель Министерства обороны.
- В 2013 году Кабинет министров сформировал комитет для изучения угроз, создаваемых израильскими вражескими башнями связи, направленными в сторону территории Ливана. Председателем этого комитета является представитель Министерства обороны; в его состав входят представители других соответствующих министерств.

- В 2015 году на базе ливанской армии было создано отдельное подразделение по кибербезопасности.
- На рассмотрении Парламента в настоящее время находится проект закона об электронных сделках.

Ниже перечислены меры, которые могло бы принять международное сообщество для укрепления кибербезопасности на глобальном уровне:

- Необходимо выполнять резолюции, принятые Организацией Объединенных Наций, и решения Всемирной встречи на высшем уровне по вопросам информационного общества, а также создать механизм сотрудничества между соответствующими международными органами для обеспечения обмена информацией и передовой практикой.
- Национальные законы и положения, касающиеся борьбы с информационными преступлениями, должны быть приведены в соответствие с мировыми правилами в целях предотвращения появления «цифровых убежищ».
- Необходимо создать глобальную систему управления информационными кризисами. Также необходимо разработать надежную международную законодательную базу для расширения возможностей национальных законодательных органов в деле противостояния киберпреступности, имеющей глобальную и международную природу.

Польша

[Подлинный текст на английском языке]
[18 июля 2016 года]

1. Общее мнение

Кибербезопасность играет жизненно важную роль для поддержания экономического роста и обеспечения функционирования гражданского общества. Кибернападениям могут подвергаться не только частный сектор или органы государственного управления, но и системы автоматизации промышленных предприятий на критически важных инфраструктурных объектах.

Создание согласованной системы обеспечения безопасности информационно-телекоммуникационных систем необходимо в свете появления все больших угроз и растущей зависимости предприятий, органов управления и общества от информационных технологий. В обеспечение кибербезопасности должны вносить свой вклад все заинтересованные стороны, включая государства, предприятия и неправительственные организации.

Необходимым условием для поддержания мира между государствами и безопасности в киберпространстве является уважение норм и принципов международного права.

Развитие национального потенциала является важнейшим элементом укрепления международной безопасности в киберпространстве.

Укрепление доверия между государствами в киберпространстве будет оказывать положительное воздействие на взаимоотношения между ними в других областях.

Защита прав человека и основных свобод должна обеспечиваться в равной степени и в киберпространстве, и в реальном мире. Уважение основных свобод в Интернете имеет большое значение для демократического общества, устойчивого развития и процветания.

2. Национальные инициативы в области укрепления кибербезопасности и международного сотрудничества

Система обеспечения кибербезопасности в Польше основывается на взаимодействии нескольких учреждений. Она опирается на сотрудничество между учреждениями как в гражданской, так и в военной отраслях, а также в сфере, касающейся киберпреступлений.

Правительство Польши прилагает все больше усилий для разработки национальной стратегии в области кибербезопасности и национального законодательства в этой же области. Основными элементами польской системы обеспечения кибербезопасности будут являться процедуры, персонал и технологии.

В прошлом году Польша выступила организатором нескольких крупных международных мероприятий, которые внесли свой вклад в поощрение международного сотрудничества, а именно: Конференции по кибербезопасности 2015 года (SECURE 2015), Европейского форума по кибербезопасности (cybersecforum.eu) и Международной конференции по кибербезопасности, посвященной трансграничным аспектам охраны и безопасности.

3. Возможные меры, которые могли бы быть приняты для укрепления кибербезопасности на глобальном уровне

Необходимо и далее принимать меры укрепления доверия в отношении киберпространства на глобальном, региональном и национальном уровнях.

Международное сообщество должно способствовать наращиванию национального потенциала в области кибербезопасности.

Важно расширять двустороннее и региональное сотрудничество. Хорошим примером регионального сотрудничества является Центральноевропейская платформа кибербезопасности, в состав которой входят Польша, Чешская Республика, Словакия, Венгрия и Австрия.

Международное взаимодействие в области кибербезопасности позволяет лучше понять природу угроз и способы реагирования на них. Удачным примером этого являются программа «Кибернетическая Европа» или инициатива «Стена из щитов» Организации Североатлантического договора.

Не стоит недооценивать пользу вовлечения в международный диалог заинтересованных сторон, представляющих неправительственные организации, деловые круги и научно-педагогическое сообщество.

Португалия

[Подлинный текст на английском языке]
[31 мая 2016 года]

В своей резолюции 70/237 о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности Генеральная Ассамблея напомнила о важной роли науки и техники в этом контексте, признав, что достижения в этих областях могут иметь как гражданское, так и военное применение. Хотя прогресс в области информатизации и телекоммуникаций означает появление новых возможностей для развития знаний, сотрудничества между государствами, укрепления созидательного потенциала человечества и обмен информацией в масштабе всего мирового сообщества, мы видим, что, с другой стороны, эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут иметь негативные последствия для национальной целостности государств.

В резолюции 70/237 Ассамблея, ссылаясь на доклад Группы правительственных экспертов 2015 года, просит государства-члены представлять информацию по следующим четырем 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, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем;

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

В докладе, содержащемся в документе A/68/98, приводится ряд рекомендаций по следующим вопросам: рекомендации в отношении норм, правил и принципов ответственного поведения государств; рекомендации в отношении мер укрепления доверия и обмена информацией; и рекомендации в отношении мер по наращиванию потенциала.

В связи с этими рекомендациями Португалия хотела бы сделать следующие замечания.

I. Нормы, правила и принципы, характеризующие ответственное поведение государств

1. Португалия считает, что безопасность в области сетевой информации имеет большое значение и ее уровень повышается.

2. Мы отмечаем прогресс, достигнутый в работе по осуществлению законодательства об обеспечении безопасности и целостности сетей посредством принятия мер в отношении рисков, для чего требуется принять надлежащие меры безопасности на техническом и организационном уровнях и установить требование в отношении информирования о нарушениях режима безопасности

или утрате целостности, которые существенно сказываются на функционировании служб.

3. На концептуальном уровне необходимо пропагандировать идею о том, что регулирование должно в первую очередь основываться на международных нормах.

4. На международном уровне необходимо расширять обмен информацией и деятельность по проведению учебных мероприятий в приграничных районах.

II. Меры укрепления доверия и обмена информацией

1. Крайне важно поощрять обмен информацией между всеми заинтересованными сторонами (как государственными, так и частными) с учетом более широкого контекста глобализации.

2. Прилагая усилия на национальном уровне, мы уделяем особое внимание проведению совместных мероприятий, в которых участвуют государственные и частные структуры, поощрению технической стандартизации, а также организации конференций и семинаров, в том числе с участием международных докладчиков.

III. Меры по наращиванию потенциала

1. Разработка мер по наращиванию потенциала имеет большое значение. Тем не менее организация учебной подготовки и обеспечение людских ресурсов, необходимых для проведения этой деятельности, сопряжены с некоторыми трудностями.

2. Необходимо содействовать расширению доступа к знаниям и развивать коллективные формы обучения по ряду направлений, включая вопросы безопасности, среди всех основных заинтересованных сторон.

Сербия

[Подлинный текст на английском языке]
[31 мая 2016 года]

Республика Сербия признает огромное значение обеспечения и укрепления информационной безопасности и считает это направление одним из своих стратегических приоритетов.

В январе 2016 года Народной скупщиной Республики Сербия был принят закон об информационной безопасности. Этим законом был учрежден компетентный орган по вопросам информационной безопасности, которому поручено разрабатывать положения в соответствии с национальными и международными стандартами, сотрудничать с компетентными органами других стран и проводить инспекции органов охраны правопорядка. В законе были определены информационно-коммуникационные системы, которые имеют особое значение для Сербии и в отношении которых операторы будут обязаны принимать надлежащие технические и организационные меры для обеспечения защиты информации. К ним относятся: a) информационно-коммуникационные системы государственных учреждений; b) системы, предназначенные для обращения конфиденциальными персональными данными; и c) системы, используемые в

сферах, представляющих общественный интерес (энергетика, транспорт, газовая отрасль, банковская отрасль, здравоохранение и прочее).

Компетентный орган отвечает за международное сотрудничество и предоставляет оповещения о рисках и происшествиях, которые имеют одну из следующих характеристик: a) стремительно растут или имеют тенденцию перерастать в серьезную угрозу; b) превышают национальный потенциал реагирования; и c) могут иметь последствия для более чем одной страны.

Также в соответствии с Законом в рамках регулирующего органа по электронной связи и почтовым услугам была создана национальная группа чрезвычайного реагирования на компьютерные происшествия, которая будет, помимо прочего, сотрудничать с аналогичными структурами в других странах.

Закон также регулирует такие вопросы, как криптографические методы защиты информации и защита от вредного электромагнитного излучения.

В целях укрепления безопасности глобальных информационно-коммуникационных систем государства должны сотрудничать друг с другом, в частности в рамках эффективных и действенных механизмов обмена информацией, оповещений и уведомлений о происшествиях в области кибербезопасности. Для этой цели государства должны назначать координаторов и обеспечивать легкий доступ к контактной информации. Особое внимание следует уделять защите критически важной инфраструктуры, особенно если то или иное происшествие касается территории более чем одного государства. Государства также должны сотрудничать друг с другом в области обмена информацией и проведения учебных мероприятий по этим вопросам.

Принимая во внимание увеличение рисков кибернападений в современном взаимосвязанном мире и их характеристики, международное сообщество должно призывать государства сотрудничать друг с другом и налаживать диалог, содействовать наращиванию общего потенциала в области кибербезопасности и поддерживать международные организации, отвечающие за взаимодействие в области информационной безопасности. Всеобщее и эффективное сотрудничество внесет свой вклад в обеспечение того, что глобальная информационно-коммуникационная среда станет более безопасной и защищенной и что государства и граждане будут ограждены от различных рисков в киберпространстве.

Испания

[Подлинный текст на испанском языке]
[26 мая 2016 года]

Испания считает, что информационно-коммуникационные технологии являются источником огромных возможностей и что их важность для международного сообщества растет с каждым днем. Однако в этой области есть ряд тревожных тенденций, которые представляют собой угрозу для международного мира и безопасности. Следовательно, государства должны эффективно сотрудничать друг с другом, чтобы пресекать вредную деятельность в киберпространстве и непреднамеренно не допускать того, чтобы их территория использовалась для совершения международных преступлений с применением таких технологий.

В июля 2015 года Национальный совет по кибербезопасности утвердил девять планов, составленных на основе Национального плана обеспечения кибербезопасности и предназначенных для реализации мер, предусмотренных Национальной стратегией в области кибербезопасности 2013 года.

Испания активно участвует во всех стратегических инициативах, касающихся кибербезопасности, в Европейском союзе, Организации по безопасности и сотрудничеству в Европе, Организации Североатлантического договора, Совете Европы и Организации экономического сотрудничества и развития.

В 2015 году Испания присоединилась к организации «Коалиция за свободу в Интернете» и Глобальному форуму по обмену опытом в области компьютерных технологий.

Испания поддерживает итоговый документ совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества, принятый в декабре 2015 года.

Расширение возможностей для сетевого взаимодействия, инновации и доступ к информационно-коммуникационным технологиям играли важную роль в обеспечении прогресса в достижении целей в области развития, сформулированных в Декларации тысячелетия.

Испания считает, что процесс в рамках Всемирной встречи на высшем уровне по вопросам информационного общества должен быть тесно связан с Повесткой дня в области устойчивого развития на период до 2030 года, поскольку доступ к информационно-коммуникационным технологиям вошел в число показателей развития и сам по себе является целью.

Испания поддерживает процесс, нацеленный на обеспечение международного консенсуса по вопросам кибербезопасности, и считает, что государства должны по-прежнему задумываться о том, как принципы и нормы международного права, в частности касающиеся угрозы или применения силы, нормы гуманитарного права и принципы защиты основных прав и свобод людей должны толковаться и применяться в киберпространстве.

Испания поддерживает стремление международного сообщества к мирному использованию информационно-коммуникационных технологий на общее благо человечества и считает, что положения Устава в данном случае применяются полностью и что государства имеют неотъемлемое право принимать в соответствии с международным правом меры для того, чтобы иметь возможность своевременно, закономерно и рационально реагировать на угрозы или нападения, которые могут сказываться на их национальной безопасности.

Швейцария

[Подлинный текст на английском языке]
[7 июня 2016 года]

1. Общая оценка проблем информационной безопасности

Информационно-коммуникационные технологии (ИКТ) стали неотъемлемой движущей силой социальной, экономической и политической деятельно-

сти. Швейцария стремится использовать возможности, которые открывает применение ИКТ. Вместе с тем, в результате использования ИКТ информационно-коммуникационная инфраструктура стала неправомерно использоваться в уголовных, разведывательных, военно-политических или террористических целях и подвергаться атакам, призванным нарушить ее функционирование. Помехи, манипуляции и конкретные нападения, совершаемые с использованием электронных сетей, — вот риски, которые влечет за собой создание информационного общества.

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

В 2012 году Федеральное правительство Швейцарии приняло Национальную стратегию защиты Швейцарии от компьютерных рисков, что позволило заложить основу для применения всеобъемлющего подхода к решению проблем. Эта стратегия направлена на повышение эффективности раннего обнаружения компьютерных рисков и возникающих угроз и устойчивости инфраструктуры Швейцарии в целом по отношению к кибератакам и на сокращение компьютерных рисков. Эта стратегия отражает также необходимость формирования культуры кибербезопасности, совместной ответственности всех участников и необходимость подхода, основанного на учете рисков. Она также содействует координации на государственном и национальном уровнях (т.е. партнерству государственного и частного секторов) и международному сотрудничеству. Стратегия включает 16 мер. Федеральное правительство Швейцарии разработало подробный план осуществления стратегии в 2013 году.

3. Содержание концепций, упомянутых в пункте 3 (резолюции)

Киберугрозам должно противостоять укрепление международного сотрудничества (определение сферы действий 5, содержащееся в стратегии). Внешнеполитическая деятельность Швейцарии в сфере кибербезопасности сосредоточена на разработке норм ответственного поведения государств, мерах укрепления доверия и наращивании потенциала. В этой связи Швейцария участвует в различных международных процессах. Организация по безопасности и сотрудничеству в Европе (ОБСЕ) принимает меры укрепления доверия в области кибербезопасности. Швейцария считает, что этот процесс имеет первостепенное значение. Помимо этого, еще одним важным процессом, в котором Швейцария принимает участие, является Лондонская программа действий. Швейцария поддерживает ряд проектов, направленных на развитие потенциала.

4. Меры, которые могло бы принять международное сообщество для укрепления безопасности на глобальном уровне

Все меры, принимаемые международным сообществом, должны обеспечивать баланс между соображениями безопасности и соображениями прав человека. В онлайновом режиме людям необходимо гарантировать те же права, которые они уже имеют. Необходимо обеспечить дальнейшее развитие мер, направленных на укрепление доверия. Комплекс мер по укреплению доверия, принятых ОБСЕ, имеет первостепенное значение для укрепления безопасности. Повышение уровня транспарентности путем обмена информацией и рас-

ширения сотрудничества на основе практических и совместных мер, будет способствовать общей стабильности в киберпространстве.

Того

[Подлинный текст на французском языке]
[2 июня 2016 года]

Хотя прогресс информационных и телекоммуникационных технологий имеет огромное значение для развития стран, этот процесс также представляет собой угрозу для национальной и международной безопасности. Виртуальное пространство нередко используется в преступных или террористических целях.

Того не застрахована от этой угрозы и уже сталкивалась с преступностью в сфере информационно-коммуникационных технологий, начиная от мошенничества и других видов обмана до детской порнографии и преступлений против свободы и неприкосновенности личности.

В эпоху терроризма интернет и социальные сети используются для пропаганды и вербовки в террористические организации. Большинство стран также переходят к электронному управлению, что представляет собой серьезный вызов для правительств, сталкивающихся с возможностью кибератак, которые могут подорвать деятельность администраций и угрожать безопасности в сфере гражданской и военной деятельности.

В этой связи важно принимать меры на национальном и международном уровнях для регулирования сектора ИКТ и обеспечивать, чтобы эти технологии не использовались в преступных целях.

В Того был принят ряд мер в этой связи, в том числе:

- Издан Указ № 2011-120/PR от 6 июля 2011 года о систематизированной и обязательной идентификации подписчиков телекоммуникационных услуг;
- Принят Закон № 2012-018 об электронных сообщениях и Закон № 2013-003, вносящий поправки в Закон № 2012-018;
- Подготовлен законопроект о киберпреступности, шифровании, кибербезопасности, защите личных данных и электронных сделках.

Цель этих документов заключается в том, чтобы обеспечить возможность отслеживания всей деятельностью в области ИКТ и создать механизм безопасности для защиты сетей ИКТ от незаконного проникновения.

Того также считает необходимым установить институциональный надзор. В этой связи Того учредила группу по реагированию на чрезвычайные ситуации в компьютерной сфере, которая отвечает за обеспечение кибербезопасности на национальном уровне, что позволит укрепить службу, регулирующую деятельность почты и телекоммуникационного сектора.

Кроме того, укрепляется кадровый потенциал, с тем чтобы правоохранительные органы и государственные и частные организации, участвующие в обеспечении кибербезопасности, принимали эффективные меры по борьбе с любыми угрозами.

Наконец, международное сотрудничество, в том числе в рамках Международного союза электросвязи и Организации Объединенных Наций, будет способствовать укреплению безопасности информации и телекоммуникаций.

Туркменистан

[Подлинный текст на русском языке]
[28 марта 2016 года]

Основой внутренней и внешней политики Туркменистана является статус нейтралитета, основанный на тесной взаимосвязи национальных интересов, глобальной безопасности и всеобщего прогресса. Основополагающим условием для Туркменистана, вытекающим из его нейтрального статуса и международных обязательств, является миролюбивый характер внешнеполитического курса, предполагающий решение всех вопросов только политическими и дипломатическими средствами, в основном через Организацию Объединенных Наций и другие международные организации. Туркменистан полностью поддерживает международные усилия по борьбе с распространением оружия массового поражения, систем его доставки и связанных с ним технологий и выдвигает разоружение основным условием обеспечения безопасности в мире. Законодательство Туркменистана провозглашает отказ страны от владения ядерным, химическим, бактериологическим и иными видами оружия массового поражения (включая новые виды и технологии их производства), а также от их производства, хранения и транспортировки.

Туркменистан присоединился к ряду международно-правовых актов по разоруженческой проблематике, основной целью которых является способствование государствами-участниками сохранению всеобщего мира, согласия и безопасности на Земле.

Придавая особую значимость укреплению международного мира и безопасности, Туркменистан призывает сокращать объем вооружения, высказывая убежденность народа Туркменистана в том, что чем меньше оружия будет в мире, тем стабильнее и спокойнее будет его развитие, тем больше будет доверия и понимания между странами и народами. Как подчеркивается в Концепции внешнеполитического курса Туркменистана на период 2013–2017 годов, Туркменистан продолжит оказание активного содействия процессам разоружения и сокращения арсеналов оружия, прежде всего оружия массового поражения.

В своем выступлении на заседании Кабинета Министров 5 июня 2015 года Президент Туркменистана, уделяя особое внимание международным обязательствам нашей страны перед мировым сообществом, подчеркнул, что нейтралитет — это неприсоединение к политическим, экономическим, военным союзам и блокам; наличие собственной армии с необходимой для государства численностью, достаточной для защиты мира и свободы страны; отказ от оружия массового поражения, запрет на провоз такого оружия по территории и через воздушное пространство нашей страны; приверженность общечеловеческим ценностям, принципам демократии, гарантии гражданского согласия и мира внутри страны; проведение внутренней и внешней политики в тесном со-

трудничестве с Организацией Объединенных Наций и гуманитарными международными организациями.

Выраженное 193 государствами мира 3 июня 2015 года на шестьдесят девятой сессии Генеральной Ассамблеи единодушное признание резолюции 69/285 о постоянном нейтралитете Туркменистана стало ярким доказательством всеобщего признания эффективной политики, нацеленной на обеспечение мира, безопасности и устойчивого развития в региональном и международном масштабах. В резолюции подчеркнуты актуальное значение постоянного нейтралитета Туркменистана для укрепления мира и безопасности в регионе и вклад нашей страны в наращивание дружественных и взаимовыгодных отношений в мире.

Как страна местонахождения штаб-квартиры Регионального центра Организацию Объединенных Наций по превентивной дипломатии для Центральной Азии, Туркменистан выступает за еще более активную вовлеченность этой структуры в различные аспекты региональной проблематики при поддержке государств — членов Организации Объединенных Наций и международными организациями (Организация по безопасности и сотрудничеству в Европе, Европейский союз, Содружество Независимых Государств и др.).

В 2015 году в Ашхабаде был успешно проведен международный форум по обеспечению мира, стабильности и безопасности в Центральноазиатском регионе. Являясь участником международных договоров и конвенций Организации Объединенных Наций и многосторонних документов в разоруженческой сфере, Туркменистан намерен и далее оказывать всемерное содействие этим процессам, в первую очередь в региональном направлении, и нацелен на регулярной основе проводить у себя региональные совещания по вопросам разоружения в Центральной Азии.

Соединенное Королевство Великобритании и Северной Ирландии

[Подлинный текст на английском языке]
[31 мая 2016 года]

Соединенное Королевство приветствует возможность представить ответ на просьбу, содержащуюся в резолюции 70/237 Генеральной Ассамблеи, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», который основывается на его ответе на резолюцию 69/28, представленном в 2015 году. В своем ответе во избежание путаницы Соединенное Королевство использует предпочитаемый им термин «кибербезопасность» и связанные с ним концепции, поскольку в данном контексте существуют различные толкования термина «информационная безопасность».

Соединенное Королевство признает, что киберпространство является одним из основных элементов жизненно важной национальной и международной инфраструктуры и необходимой основой для экономической и социальной деятельности в интернете. Соединенное Королевство ссылается на Национальную оценку рисков в области безопасности 2015 года, в которой подтверждается, что киберпреступность по-прежнему является угрозой первого уровня для

национальной безопасности. В дополнение к средствам в размере 860 млн. фунтов стерлингов, выделенным Соединенным Королевством за время осуществления предыдущей Национальной стратегии кибербезопасности (2011–2016 годы), в течение следующих пяти лет будут выделены дополнительные ассигнования в размере 1,9 млрд. фунтов стерлингов. Новая национальная стратегия кибербезопасности будет опубликована в 2016 году, и она будет предусматривать создание нового Национального центра кибербезопасности.

Соединенное Королевство признает, что международное сотрудничество имеет решающее значение для успешного обеспечения кибербезопасности. Мы продолжаем содействовать свободе и открытости, мирному использованию и безопасности киберпространства, с тем чтобы его экономические и социальные выгоды были защищены и доступны для всех. Соединенное Королевство играет ведущую роль в решении трансграничных проблем в области кибербезопасности посредством таких инициатив, как Глобальный альянс по защите детей от сексуальной эксплуатации детей в интернете (#WePROTECT). Мы также полны решимости обмениваться передовым опытом на международном уровне и обеспечивать, чтобы мировое сообщество получало помощь в укреплении их потенциала в области кибербезопасности.

Соединенное Королевство продолжает принимать активное и конструктивное участие в международных дискуссиях по вопросам кибербезопасности. Мы предоставили экспертов для участия во всех четырех группах правительственных экспертов Организации Объединенных Наций и считаем, что принятый на основе консенсуса доклад предыдущей Группы позволил достичь существенного прогресса и вновь подтвердить, что международное право распространяется на киберпространство и что соблюдение государствами норм международного права, в частности их обязательств по Уставу Организации Объединенных Наций, служит прочной основой для их действий по использованию информационно-коммуникационных технологий.

Соединенное Королевство также приветствует продолжающиеся в Организации по безопасности и сотрудничеству в Европе обсуждения возможных последующих мер укрепления доверия в киберпространстве, а также аналогичную работу в других региональных организациях.

Соединенное Королевство с удовлетворением принимает активное участие в решении этих важных вопросов и надеется на дальнейшее участие в укреплении потенциала и международном сотрудничестве в области кибербезопасности.