Организация Объединенных Наций A/72/315

Генеральная Ассамблея

Distr.: General
11 August 2017
Russian
Original: Arabic/English/French/
Russian/Spanish

Семьдесят вторая сессия
Пункт 95 предварительной повестки дня*

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Содержание

* A/72/150.

17-13876 (R) 220917 250917

I. Введение

1. 5 декабря 2016 года Генеральная Ассамблея приняла резолюцию 71/28 о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности. В пункте 3 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 2 резолюции;

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

2. Во исполнение этой просьбы 16 февраля 2017 года всем государствам-членам была направлена вербальная нота с просьбой предоставить информацию по данному вопросу, а затем еще одна вербальная нота — от 12 июня 2017 года. Ответы, полученные на момент составления настоящего доклада, содержатся в разделе II. Дополнительные ответы, полученные после 31 июля 2017 года, будут размещены на веб-сайте Управления по вопросам разоружения (www.un.org/disarmament/) на том языке, на котором они были представлены.

II. Ответы, полученные от правительств

Афганистан

[Подлинный текст на английском языке]
[26 мая 2017 года]

В связи с пунктом 3 постановляющей части резолюции 71/28 Генеральной Ассамблеи о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности Министерство коммуникационных и информационных технологий Исламской Республики Афганистан сообщило следующее.

Достижения

В целях содействия созданию международной системы обеспечения безопасности информационных технологий и подлинности электронных операций Министерство коммуникационных и информационных технологий разработало инфраструктуру сертификации открытых ключей. Кроме того, Министерство создало систему сетевых операционных центров и намерено увязать ее с соответствующими системами государств-членов для целей идентификации и проверки текущих статистических параметров и потоков данных в Интернете.

Министерство разработало законы о киберпреступности и направило их в Министерство юстиции на рассмотрение. Что касается отыскания фундаментальных решений, то эти законы обеспечивают осуществление защищенных электронных сделок и возможность предотвращения киберпреступлений.

Министерство разработало национальную киберстратегию для обмена защищенной информацией, создания рамочного механизма обеспечения безопасности информационных технологий для проекта NIXA, который будет осуществляться Министерством, а также выявления и решения проблем киберпреступности.

Предложения

Министерство коммуникационных и информационных технологий просит развитые страны, в которых имеется киберполиция, оказывать Министерству содействие и сотрудничать с ним в деле создания киберполиции.

Для решения проблемы киберпреступности и ведения серьезной борьбы с этим явлением на международном уровне должна быть разработана согласованная система, обеспечивающая получение сведений уголовного характера.

Одно из условий обеспечения безопасности Интернета заключается в создании системы регулирования Интернета. Посредством регулирования Интернета могут быть обеспечены основы для обмена конфиденциальной информацией и данными между всеми департаментами и управлениями правительства в целях внедрения вышеупомянутой сети. В этой связи Министерство обращается ко всем государствам-членам с просьбой о сотрудничестве.

Министерство также просит государства-члены поддержать его сотрудников в деле борьбы с киберпреступностью и повышения информационной безопасности путем предоставления им программ профессионально-технической подготовки.

Армения

[Подлинный текст на английском языке]
[31 мая 2017 года]

Общая оценка проблем информационной безопасности

С учетом темпов развития электронного общества в Республике Армения вопросы, относящиеся к информационной безопасности, приобретают особую значимость, поскольку они оказывают огромное воздействие на все аспекты национальной безопасности.

В свете тенденций развития информационно-коммуникационных технологий (ИКТ) возникают качественно новые угрозы и вызовы, требующие систематической координации и новых подходов в интересах обеспечения безопасного использования ИКТ. Принимая во внимание, что методы ведения «информационной войны» используются в различных конфликтных ситуациях, Армения придает огромное значение обеспечению информационной безопасности в интересах поддержания международного мира и безопасности.

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

Армения проводит мероприятия, направленные на защиту государственных и общественных интересов в сфере информационной безопасности и на приведение соответствующего законодательства в соответствие с международными стандартами. Вступили в силу ряд нормативных актов, регламентирующих эту сферу, в том числе национальная стратегия безопасности и концепция информационной безопасности, а также законы о борьбе с терроризмом; о государственной и служебной тайне; об электронных документах и цифровых подписях; о защите личных данных; о свободе информации; и о средствах массовой информации.

Во исполнение соответствующих решений правительства:

a) был принят ряд практических мер по обеспечению защиты имеющейся в открытом доступе онлайновой информации государственных органов, а также по обеспечению безопасного подключения их информационных систем к Интернету;

b) были утверждены минимальные требования к официальным вебсайтам государственных органов.

Армения приняла и применяет набор стандартов Международной организации по стандартизации (ИСО), относящихся к информационной безопасности. В октябре 2006 года была ратифицирована Конвенция Совета Европы о киберпреступности, после чего были внесены соответствующие изменения в национальное законодательство.

Армения активно участвует в соответствующих программах, учебных курсах и совместных инициативах, осуществляемых в рамках различных международных организаций, таких как Содружество Независимых Государств, Организация Договора о коллективной безопасности, Европейский союз и Организация Североатлантического договора. В частности, в 2016 году были проведены совместные двухэтапные учения «Кибер-антитеррор» с участием стран — членов Содружества Независимых Государств. Ранее в 2017 году был предложен для внутреннего межведомственного утверждения проект Соглашения о сотрудничестве государств — членов ОДКБ в области обеспечения информационной безопасности.

Содержание концепций, упомянутых в пункте 2

В концепции информационной безопасности Республики Армения термин «информационная безопасность» определяется как «защита национальных интересов в информационной сфере, которая связана со всей совокупностью согласованных интересов личности, общества и государства».

С учетом стремительного развития информационно-коммуникационных технологий была создана межучрежденческая рабочая группа, перед которой была поставлена задача разработать к концу 2017 года обновленную концепцию обеспечения информационной безопасности и информационной политики в Республике Армения.

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

Армения подчеркивает важность обеспечения более широкого и эффективного международного сотрудничества по проблемам информационной безопасности, особо отмечая роль Международного союза электросвязи.

Беларусь

[Подлинный текст на русском языке]
[5 июня 2017 года]

Общая оценка проблем информационной безопасности

Нынешнее состояние международной информационной безопасности нельзя признать удовлетворительным. Имеют место попытки использования информационных технологий в политических целях.

Для Беларуси характерно наличие ряда проблем информационной безопасности:

a) недостаточная степень защищенности национального сегмента от DDoS-воздействия как на уровне магистральных, так и внутренних провайдеров вплоть до хостинг-площадок;

b) потенциальное наличие незаявленных возможностей и факторов уязвимости в средствах защиты информации наряду с отсутствием возможности их своевременного выявления, что зачастую сводит на нет эффект от реализации комплекса мер по защите информации;

c) наличие угроз деструктивного воздействия злоумышленников на критическую инфраструктуру и объекты информатизации: системы электроснабжения, автоматизированные системы управления производством и транспортом.

Национальные усилия по укреплению информационной безопасности и содействию международному сотрудничеству в этой области

Такие усилия включают в себя:

a) проведение системной работы по актуализации требований по технической и криптографической защите информации, распространение и (или) предоставление которой ограничено;

b) организацию и осуществление технического нормирования и стандартизации по вопросам технической и криптографической защиты информации;

c) реализацию соглашений об обмене информацией с ведущими компаниями в сфере информационной безопасности;

d) организацию постоянного взаимодействия с государственными органами и организациями, позволяющего обеспечить оперативное реагирование на конкретные инциденты информационной безопасности;

e) сопровождение собственного комплекса обнаружения вредоносного программного обеспечения;

f) взаимодействие со странами Организации Договора о коллективной безопасности в формате консультационного координационного центра.

Изучение международных концепций по укреплению безопасности глобальных информационных и телекоммуникационных систем

Ключевой подход Беларуси к проблематике международной информационной безопасности заключается в необходимости недопущения возможности использования информационно-коммуникационных технологий (ИКТ) вразрез с национальной безопасностью и стабильностью и с безопасностью на международном уровне.

Беларусь принимает активное участие в обсуждении тематики международной информационной безопасности на площадках различных международных организаций, включая Организацию Объединенных Наций, Организацию Договора о коллективной безопасности, Организацию по безопасности и сотрудничеству в Европе.

Беларусь поддерживает инициативу по принятию в рамках Организации Объединенных Наций универсального документа по обеспечению международной информационной безопасности.

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

Важным является поэтапное продвижение на международной арене принципа невмешательства во внутренние дела суверенных государств и взаимного отказа от агрессивных действий в информационной сфере. Основным вектором таких шагов должно стать поддержание информационного суверенитета государств — членов Организации Объединенных Наций в целях:

a) реализации прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;

b) развития информационного общества при равноправном участии государств — членов Организации Объединенных Наций в мировых информационных отношениях;

c) эффективного информационного обеспечения межгосударственной политики по недопущению распространения террористических и экстремистских идей;

d) обеспечения устойчивости функционирования критически важных объектов.

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

a) Развитие механизмов международного взаимодействия, предусмотренных действующими и перспективными международно-правовыми инструментами;

b) выстраивание эффективного взаимодействия международного сообщества с транснациональными корпорациями, контролирующими подавляющий объем ИКТ, позволяющий эффективно выявлять и блокировать источники угроз информационной безопасности.

Бруней-Даруссалам

[Подлинный текст на английском языке]
[29 июня 2017 года]

Бруней-Даруссалам отдает себе отчет в том, что в условиях все более значимых изменений в информационно-телекоммуникационной сфере происходит сдвиг в глобальных тенденциях. Одновременно это порождает новые угрозы и вызовы в виде действий хакеров, киберпреступности и кибертерроризма, подвергающих опасности жизненно важные объекты инфраструктуры, сети и услуги во всем мире. Транснациональный и нематериальный характер этих явлений требует совместных усилий со стороны международного сообщества по созданию безопасной и надежной онлайновой среды.

На национальном уровне под эгидой Комитета национальной безопасности страна поддерживает тесное взаимодействие с целым рядом местных служб безопасности в деле управления внутренними угрозами кибербезопасности. В мае 2004 года была создана Брунейская национальная группа по реагированию на чрезвычайные ситуации в компьютерной сфере, которая стала единым национальным органом, к которому можно обращаться в случае возникновения инцидентов в сфере безопасности, связанных с компьютерами и Интернетом. Благодаря глобальным связям с другими группами по реагированию на чрезвычайные ситуации в компьютерной сфере Национальная группа получает ценную информацию об угрозах безопасности информационно-коммуникационных технологий (ИКТ) и предоставляет сведения об угрозах безопасности, выявленных в рамках национальной инфраструктуры информационно-коммуникационных технологий.

Бруней-Даруссалам привержен сотрудничеству с региональными и международными партнерами в целях поддержания постоянной готовности противостоять крупным международным киберугрозам. В рамках региональной архитектуры Ассоциации государств Юго-Восточной Азии (АСЕАН) Бруней-Даруссалам примет участие в совещании Рабочей группы экспертов по кибербезопасности, которое пройдет в контексте расширенного Совещания министров обороны стран АСЕАН («СМОА плюс»); это мероприятие с участием 18 стран будет направлено на поощрение практического и эффективного сотрудничества и укрепление возможностей по защите киберпространства в регионе и решению проблем, касающихся кибербезопасности.

Правительство отдает себе отчет в том, что киберпространство во всех его формах (включая облачные вычисления и мобильные системы) содержит в себе угрозы, борьба с которыми является одной из важнейших приоритетных задач Брунея-Даруссалама в сфере безопасности и обороны.

Канада

[Подлинный текст на английском языке]
[17 июля 2017 года]

По вопросу о кибербезопасности Канада желает заявить следующее:

a) свободное, открытое и безопасное киберпространство имеет решающее значение для поощрения безопасности, процветания и соблюдения прав человека;

b) существующие нормы международного права применяются к использованию информационно-коммуникационных технологий государствами;

c) поощрение норм мирного времени способствует поддержанию среды, в которой ответственное поведение лежит в основе деятельности государств;

d) практические меры по укреплению доверия являются испытанным методом снижения риска вооруженного конфликта.

Что касается мер, принимаемых на национальном уровне, то в 2010 году правительство обнародовало свою стратегию в области кибербезопасности, направленную прежде всего на обеспечение безопасности канадских киберсистем и защиту деятельности канадцев в Интернете. Недавно правительство завершило обзор существующих мер в области кибербезопасности. Исходя из этого в конце 2017 года должна быть обнародована новая национальная концепция кибербезопасности.

Оборонная политика 2017 года предусматривает новые инвестиции и политическое руководство, направленные на оптимальное использование потенциала киберпространства в поддержку военных операций. К активному потенциалу канадских вооруженных сил в киберпространстве будет применяться столь же строгий подход, что и к другим военным средствам; в частности, в его отношении будут действовать соответствующие нормы внутреннего и международного права и правила применения вооруженной силы.

На международном уровне Канада активно участвует в следующих видах деятельности:

a) она продолжает содействовать разработке норм поведения государств в киберпространстве в мирное время, включая итоговые документы совещаний Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2012–2013 и 2014–2015 годов;

b) в июле 2015 года она ратифицировала Конвенцию Совета Европы о киберпреступности (Будапештская конвенция). Канада призывает другие страны стать участниками Конвенции или использовать ее в качестве модели при разработке своего собственного законодательства в области противодействия киберпреступности;

c) начиная с 2007 года Канада выделила 11 млн. долл. США на поддержку проектов по наращиванию потенциала в области кибербезопасности;

d) она сотрудничает с Соединенными Штатами Америки в области внедрения совместного плана действий двух стран в области кибербезопасности, целью которого является повышение устойчивости ее киберинфраструктуры;

e) она 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;

f) она поддерживает усилия Организации Североатлантического договора, направленные на укрепление кибероборонs Организации и отдельных союзников.

Куба

[Подлинный текст на испанском языке]
[5 апреля 2017 года]

Как указано в резолюции 71/28 Генеральной Ассамблеи, достижения науки и техники могут иметь как гражданское, так и военное применение, и нельзя допускать, чтобы эти достижения отрицательным образом сказывались на международной безопасности.

Необходимо на многостороннем уровне содействовать изучению реальных и потенциальных угроз в области информационной безопасности и возможных стратегий их предотвращения и устранения.

Единственным способом, позволяющим избежать превращения киберпространства в театр военных действий, является широкое сотрудничество между всеми государствами.

Куба поддерживает работу созданной в соответствии с резолюцией 58/32 Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, в которой участвует кубинский эксперт.

Мы считаем, что следует создать юридически обязательную международную нормативно-правовую базу, дополняющую существующие нормы международного права, применимые к информационно-коммуникационным технологиям.

Информационные и телекоммуникационные системы могут превратиться в оружие, если они разрабатываются или используются с целью причинения ущерба инфраструктуре того или иного государства. Все государства обязаны уважать существующие международные стандарты в этой сфере. Доступ к информационным или телекоммуникационным системам другого государства должен осуществляться с соблюдением международных соглашений о сотрудничестве на основе принципа согласия соответствующего государства. Формы и масштабы обмена должны определяться на основе уважения законодательства того государства, к системе которого открывается доступ.

Использование телекоммуникаций с враждебными намерениями с явной или скрытой целью изменить правовую и политическую систему государств является нарушением международно признанных норм в этой области и представляет собой незаконное и безответственное применение этих средств, последствия которого могут привести к возникновению напряженных ситуаций, ставящих под угрозу международный мир и безопасность, и отрицательно сказаться на целостности инфраструктуры государств в ущерб их безопасности в гражданской и военной сферах.

Куба вновь выражает 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.

С помощью незаконных радио- и телепередач совершаются постоянные вторжения в информационное пространство Кубы, а также распространяются программы, специально предназначенные для подстрекательства к свержению конституционного строя, установленного кубинским народом. На протяжении 2016 года с территории Соединенных Штатов Америки велось незаконное вещание на Кубу в среднем в течение 1875 часов в неделю на 25 частотах. Не-

прерывные трансляции радио- и телепрограмм из Соединенных Штатов на территорию Кубы противоречат целям и принципам Устава Организации Объединенных Наций, международному праву и положениям Международного союза электросвязи.

Куба вновь призывает к немедленному прекращению этой агрессивной политики, наносящей ущерб ее суверенитету и, помимо всего прочего, несовместимой с налаживанием отношений между Кубой и Соединенными Штатами на основе взаимного уважения и сотрудничества.

Куба 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.

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 пятом саммите СЕЛАК, состоявшемся в январе 2017 года в Пунта-Кане (Доминиканская Республика), вновь была подчеркнута важность информационно-коммуникационных технологий, включая Интернет, в качестве средств поощрения мира, благосостояния человечества, развития, обмена знаниями, социальной интеграции и экономического роста.

Куба вновь заявляет, что обязательным условием успешного противодействия угрозам, порождаемым неправомерным использованием информационно-коммуникационных технологий, является международное сотрудничество. Кроме того, она отмечает важную роль Международного союза электросвязи в обсуждениях проблематики кибербезопасности на межправительственном уровне.

Эквадор

[Подлинный текст на испанском языке]
[28 июля 2017 года]

Эквадор считает, что безопасность в международных отношениях должна опираться на доверие и уважение в отношениях между государствами. Постоянные разоблачительные сообщения о системах массовой, поголовной слежки за всеми жителями планеты в коммуникационной сфере, а также об использовании информационно-коммуникационных технологий в нарушение норм международного права, что подрывает принципы уважения к суверенитету и невмешательству во внутренние дела государств, — все это привносит серьезный элемент нестабильности в отношения между государствами и тем самым негативно влияет на международную безопасность. Кроме того, использование этих систем слежки представляет собой покушение на целый ряд основополагающих прав человека.

Именно поэтому Эквадор поддерживает усилия по дальнейшему изучению реальных и потенциальных угроз в области информационной безопасности и возможных мер сотрудничества в целях их устранения, а также того, каким образом к использованию государствами информационно-коммуника-

ционных технологий должно — в дополнение к нормам, правилам и принципам ответственного поведения государств в этой сфере — применяться международное право.

Сальвадор

[Подлинный текст на испанском языке]
[24 мая 2017 года]

Что касается выполнения обязательств перед Организацией Объединенных Наций, то в связи с резолюцией 71/28 Генеральной Ассамблеи, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», Сальвадор просит принять к сведению, что в 2016 году в целях повышения информационной безопасности его Вооруженные силы приобрели в пользование и в настоящее время внедряют систему шифрования ведомственной документации.

Эстония

[Подлинный текст на английском языке]
[31 мая 2017 года]

Эстония признает тот факт, что безопасность мирового киберпространства стала весьма важным вопросом в более широком контексте международной безопасности. Поэтому роль и участие Организации Объединенных Наций становятся все более актуальными.

Обеспечение безопасности Интернета является одной из высокоприоритетных задач эстонского правительства. Основным руководящим документом по этому вопросу является Национальная стратегия кибербезопасности (2014–2017 годы). Совет по вопросам кибербезопасности Комитета безопасности правительства поддерживает межучрежденческое сотрудничество на стратегическом уровне и следит за осуществлением задач, поставленных в Стратегии кибербезопасности. По состоянию на 30 мая 2017 года в деятельности созданного в Таллине Экспертного центра по совместной кибероборонe Организации Североатлантического договора участвовало 20 государств-членов.

Эстония убеждена, что для повсеместного использования цифровых услуг требуется высокий уровень кибербезопасности. По мнению Эстонии, социально-экономические и военно-политические аспекты кибербезопасности связаны друг с другом. Эстония считает элементарным требование о том, чтобы страны воздерживались от нападения на важнейшие объекты национальной инфраструктуры. Эстония также призывает к ответственному поведению в отношении глобальной коммуникационной инфраструктуры, с тем чтобы поощрять доступ к информации и доверие к информационно-коммуникационным технологиям (ИКТ). Она считает, что каждая страна обязана разрабатывать и осуществлять на практике национальные законы, которые способствуют контролю за злонамеренным использованием ИКТ негосударственными субъектами и поиску путей для более эффективной разработки, распространения и поощрения ответственной и активной киберполитики, концепций и аргументации.

Эстония четвертый срок подряд входит в состав Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Группа является весьма продуктивным форумом. В будущем ее деятельность может быть полезна не только для изучения киберугроз и возможных средств защиты от них, но и для понимания

того, как различные страны применяют существующие нормы, правила и принципы международного права. По мнению Эстонии, Группе следует продолжать свою работу по продвижению вперед диалога между государствами-членами, который облегчает обмен информацией и передовым опытом. Кроме того, ей нужно обсудить практические меры и механизмы сотрудничества в целях содействия укреплению потенциала государств-членов, с тем чтобы в конечном итоге обеспечить государствам-членам полномочия и возможности для решения проблем, возникающих в Интернете, во всех их аспектах.

Важно развивать прогресс, достигнутый на состоявшихся в 2014 и 2015 годах совещаниях Группы правительственных экспертов, путем поощрения государств к соблюдению таких норм поведения, которые способствуют закреплению в киберпространстве принципов открытости и подотчетности и других демократических ценностей. Эстония надеется, что в июне 2017 года Группа представит еще один консенсусный доклад.

Финляндия

[Подлинный текст на английском языке]
[21 июля 2017 года]

Финляндия приветствует возможность представить доклад об осуществлении резолюции 71/28 Генеральной Ассамблеи.

На национальном уровне были приняты следующие меры:

a) в национальной стратегии кибербезопасности 2013 года и обновленной программе ее осуществления 2017 года изложены основные руководящие указания и меры по повышению уровня кибербезопасности и способности к восстановлению нормального функционирования;

b) в Финляндии созданы Национальный центр кибербезопасности и Центр предупреждения киберпреступности, а в Министерстве иностранных дел назначен Посол по вопросам киберпространства. В 2016 году была принята национальная стратегия информационной безопасности;

c) Финляндия активно участвует в сотрудничестве по вопросам киберпространства в рамках Европейского союза;

d) Финляндия поддерживает различные виды проектов по наращиванию потенциала в сферах информационно-коммуникационных технологий в целях развития и проектов в области компьютерных технологий. Она является одним из партнеров-основателей Глобального форума по обмену опытом в области компьютерных технологий. В 2016 году она присоединилась к созданному Всемирным банком Целевому фонду партнерства в области развития цифровых технологий. Финляндия поддерживает управление Интернетом на основе модели, предполагающей участие многих заинтересованных сторон. Она принимает активное участие в работе Всемирной встречи на высшем уровне по вопросам информационного общества и последующей деятельности в связи с ней, включая участие в работе Форума по вопросам управления Интернетом и его финансировании. В апреле 2017 года в Хельсинки был проведен восьмой Финский интернет-форум;

e) Финляндия активно участвует в 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) она работает над укреплением доверия, безо-

пасности и стабильности в киберпространстве и принимает согласованные меры по укреплению доверия при использовании компьютерных технологий;

f) Финляндия одобрила выпущенный в 2015 году доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и непосредственно задействована в работе этой группы в ее нынешнем составе. Она активно участвует в обсуждениях, посвященных нормам международного права применительно к киберпространству, в том числе в консультациях по второй версии Таллинского руководства и в практикумах, организуемых Институтом Организации Объединенных Наций по исследованию проблем разоружения;

g) в 2012 году Финляндия присоединилась к организации «Коалиция за свободу в Интернете», а также вносит свой вклад в работу Партнерства защитников цифровых прав. В 2016 году она организовала конференцию по случаю Всемирного дня свободы печати, которая состоялась в Хельсинки;

h) Финляндия является участницей Конвенции Совета Европы о киберпреступности. Новый стратегический план работы полиции 2015 года предусматривает выделение ресурсов на предупреждение преступлений, совершаемых с помощью компьютеров, и на разработку ноу-хау в области кибербезопасности. Также был разработан комплексный план предупреждения киберпреступлений.

Приоритетные направления дальнейшей работы международного сообщества состоят в следующем:

a) работа нынешней Группы правительственных экспертов, которой Финляндия придает большое значение и успеху которой она готова и далее содействовать, включая дальнейшее определение норм ответственного поведения государств в киберпространстве с особым акцентом на деятельность в мирное время;

b) дальнейшая разработка и внедрение региональных мер укрепления доверия в рамках ОБСЕ;

c) дальнейшая поддержка мероприятий по наращиванию потенциала в области компьютерных технологий с целью повышения уровня устойчивости и безопасности в киберпространстве;

d) диалог с участием многих заинтересованных сторон, который Финляндия будет и далее поддерживать и поощрять, и укрепление партнерских отношений между государственным и частным секторами на национальном и международном уровнях.

Германия

[Подлинный текст на английском языке]
[30 мая 2017 года]

Развитие информационно-коммуникационных технологий (ИКТ) открывает многочисленные возможности в экономической, социальной и научной сферах. Обеспечение доступа к киберпространству и сохранение целостности, аутентичности и конфиденциальности данных в киберпространстве приобрели в XXI веке жизненно важное значение.

Во все более взаимозависимом мире от надежного функционирования ИКТ зависят государства, важнейшие объекты инфраструктуры, предприятия и отдельные лица. Последствия злонамеренного использования ИКТ могут выходить за рамки киберпространства и чреваты причинением социального, экономического, политического и культурного ущерба. Например, нападения, нацеленные на государственные институты или на подрыв демократических и политических процессов, могут негативно повлиять на общественный порядок и безопасность.

Германия решает эти проблемы, поощряя международное применение ИКТ государствами, основанное на соблюдении законов и норм и на укреплении доверия, на трех уровнях:

a) в глобальном масштабе Германия поддерживает усилия по согласованию того, как международное право применяется к использованию ИКТ государствами для разработки добровольных и необязывающих норм, правил или принципов ответственного поведения государств, направленных на создание открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды. Особое значение в этом контексте имеет работа сменяющих друг друга групп правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Немецкие эксперты принимают активное участие в деятельности таких групп, и Германия стремится содействовать выполнению их рекомендаций. Настало время расширить рамки обсуждений и привлечь к ним более широкий круг государств — членов Организации Объединенных Наций с целью придания универсального характера работе по вопросам ИКТ в контексте международной безопасности. Германия поддерживает ведущую роль Организации Объединенных Наций и укрепление потенциала Организации в этой области. Вопросы, которые следует изучить дополнительно, касаются, в частности, международного обмена информацией и сотрудничества в области выявления источников кибератак. Необходимы четкие и повсеместно соблюдаемые правила, применяемые к злонамеренному использованию потенциала киберпространства, а также к онлайновому шпионажу в экономических целях;

b) на региональном уровне меры укрепления доверия помогают устранять опасность перерастания инцидентов в сфере ИКТ в политические или даже военные кризисы. В рамках Организации по безопасности и сотрудничеству в Европе (ОБСЕ) Германия на протяжении многих лет принимает активное участие в разработке и осуществлении мер укрепления доверия с целью обеспечения безопасности в связи с использованием ИКТ государствами. В период председательства Германии в ОБСЕ в 2016 году участвующие государства договорились о введении таких дополнительных мер. Эти меры были одобрены на состоявшемся в Гамбурге заседании Совета министров ОБСЕ 2016 года, в ходе которого были также даны указания не только в отношении их осуществления, но и в отношении дальнейшей работы. Эта работа должна выйти за рамки военно-политических аспектов и охватить различные аспекты безопасности. За пределами региона ОБСЕ Германия также поддерживает аналогичные усилия, прилагаемые региональными организациями на других континентах;

c) на двустороннем уровне Германия поддерживает диалоги и регулярно проводит консультации в киберпространстве с различными партнерами. Опираясь на сложившиеся партнерские отношения, Германия также поддерживает усилия по укреплению потенциала других стран в области кибербезопасности. Обновляя свою стратегию обеспечения кибербезопасности в ноябре 2016 года, правительство Германии решило добиваться создания Германского

института международной кибербезопасности с целью систематизации и активизации этих усилий.

Усилия Германии, касающиеся информатизации и телекоммуникаций в контексте международной безопасности, являются частью интенсивной работы по обеспечению безопасности ИКТ в целом. Недавние национальные нормативно-правовые меры, такие как принятие Закона о безопасности информационных технологий 2015 года и Закона о реформе национальной стратегии кибербезопасности 2016 года, направлены на общее повышение безопасности ИКТ в Германии.

Греция

[Подлинный текст на английском языке]
[26 мая 2017 года]

В рамках Совета Европы Греция ратифицировала в соответствии с законом 4411/2016 («Правительственный вестник» № A-142 от 3 августа 2016 года) Конвенцию Совета Европы о киберпреступности (Будапешт, 23 ноября 2001 года) и Дополнительный протокол к Конвенции о киберпреступности, касающийся уголовной ответственности за акты расистского и ксенофобского характера, совершаемые через компьютерные системы (Страсбург, 28 января 2003 года).

Следует отметить, что уже идет процесс включения директивы Европейского союза о безопасности сетей и информационных систем в национальное законодательство. Эта директива имеет первостепенное значение для повышения устойчивости перед лицом кибератак на национальном уровне и устанавливает для всех государств — членов Европейского союза ряд обязательств, имеющих отношение к этой цели, а также предполагает принятие национальной стратегии в области безопасности сетей и информационных систем.

Согласно информации, полученной от Министерства национальной обороны, концепция кибербезопасности Греции состоит в том, чтобы задействовать весь спектр возможностей для защиты своей национальной инфраструктуры и сетей от появившихся в последнее время киберугроз и киберпреступников. Это предполагает организацию кибероборонs на самом высоком стратегическом уровне в рамках национальных организаций, связанных с обороной, дальнейшую интеграцию кибероборонs в оперативную деятельность и обеспечение охвата развертываемых сетей. На национальном уровне были предприняты следующие усилия, направленные на укрепление информационной безопасности и содействие международному сотрудничеству:

a) в настоящее время разрабатывается национальная стратегия кибероборонs, в то же время национальная стратегия кибербезопасности, в которой регламентируются общие рамки кибербезопасности и определяются меры, необходимые для поддержания минимальных требований кибербезопасности, приобретает статус закона;

b) кибероборонa уже является частью оперативных планов национальной обороны, в то время как национальная система оповещения в чрезвычайных ситуациях включена в большинство программных документов, касающихся информационных систем, и интегрирована во все крупные национальные инициативы. Обеспечение кибербезопасности включено в планы оперативных мероприятий в периоды кризисов во всех государственных организациях;

c) Греция создала и постоянно совершенствует потенциал для реагирования на происшествия/чрезвычайные ситуации в рамках Центра реагирования на инциденты в области компьютерных технологий. В целях содействия реагированию на инциденты в области компьютерных технологий, возникающие в вооруженных силах или в общественных сетях, и ликвидации их последствий могут быть в короткие сроки развернуты группы быстрого реагирования. Инструкции по ликвидации последствий сбоев в работе или кибератак включены в директивные документы по безопасности компьютерной информации;

d) ведется создание оперативного центра кибербезопасности для всех национальных сетевых военно-оборонительных систем, в то же время на национальном уровне действуют четыре компьютерные группы экстренного реагирования, отвечающие за государственный и частный секторы.

Меры, которые могли бы быть приняты международным сообществом в целях достижения более высокого уровня информационной безопасности, заключаются в следующем:

a) укрепление потенциала в сферах реагирования на инциденты, мониторинга сетей и эффективной защиты от киберугроз на базе полностью функционирующих национальных центров кибербезопасности;

b) полная интеграция кибероборонs в оперативную деятельность;

c) разработка национальных стратегий кибербезопасности/кибероборонs;

d) расширение осведомленности о киберпространстве персонала, занятого в области кибероборонs, и совершенствование существующих технических возможностей;

e) непрерывное обучение персонала, работающего в организациях кибероборонs;

f) согласование национальных законов с положениями законов и директив в области глобальной кибербезопасности.

Согласно информации, полученной от греческой полиции, в соответствии со статьей 30 президентского указа 178/2014 в задачи Отдела греческой полиции по борьбе с киберпреступностью входит предупреждение, расследование и судебное преследование в связи с преступлениями, совершенными через Интернет или другие электронные средства связи. Отдел по борьбе с киберпреступностью является автономной центральной службой и напрямую подчиняется начальнику штаба греческой полиции.

Одно из подразделений Отдела отвечает за обеспечение безопасности электронной и телефонной связи и программного обеспечения и за защиту авторских прав. Если говорить более конкретно, то это подразделение расследует дела, связанные с незаконным проникновением в компьютерные системы и похищение, уничтожение или оборот средств программного обеспечения, цифровых данных и аудиовизуальных произведений на территории всей страны.

Отдел по борьбе с киберпреступностью греческой полиции тесно сотрудничает с Национальным органом по борьбе с нападениями с использованием электронных средств, который является подразделением Национальной разведывательной службы. Задача Национального органа состоит в обеспечении предотвращения и пресечения (в пассивной и активной форме) нападений на коммуникационные сети, хранилища данных и системы информационно-коммуникационных технологий. Кроме того, Орган отвечает за обработку данных и уведомление компетентных органов.

Япония

[Подлинный текст на английском языке]
[27 июля 2017 года]

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 изоляции без законного основания. В своих усилиях Япония руководствуется следующими пятью принципами: свобода информационных потоков, верховенство права, открытость, самоуправление и применение подхода, подразумевающего участие многих заинтересованных сторон.

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

Усилия Японии сосредоточены на следующих трех основных направлениях: поощрение верховенства права в киберпространстве, меры укрепления доверия и наращивание потенциала.

Что касается поощрения верховенства права, то Япония активно участвует в международных дискуссиях, направленных на формирование общего понимания того, что действующие нормы международного права должны применяться и в киберпространстве, а также при разработке необязательных и добровольных норм. Они служат основой для обеспечения стабильности и предсказуемости международного сообщества. Вместе с тем с учетом уникальных особенностей информационно-коммуникационных технологий необходимо дальнейшее прояснение вопроса о том, как будут применяться отдельные нормы и принципы.

Для продвижения мер по укреплению доверия требуется обеспечить транспарентность и обмен информацией; однако уровень принимаемых мер варьируется от государства к государству, поскольку каждое государство имеет право определять уровень, отвечающий его возможностям. Япония участвует в деятельности по укреплению доверия в рамках двустороннего диалога и многосторонних механизмов, таких как Региональный форум Ассоциации государств Юго-Восточной Азии. Необходимо изучать возможные пути налаживания реального сотрудничества.

Что касается наращивания потенциала, то Япония выступает за разработку законов, статутов и основ политики в области кибербезопасности, а также ведет работу по обеспечению кибербезопасности правительственных органов и операторов критической информационной инфраструктуры (КИИ); принятию мер борьбы с киберпреступностью; развитию людских ресурсов в целях содействия подготовке экспертов по кибербезопасности; и проведению научных исследований и разработок в области технологий обеспечения кибербезопасности. Опираясь на этот опыт и накопленные знания, Япония будет и впредь активно сотрудничать в деле укрепления потенциала.

Иордания

[Подлинный текст на арабском языке]
[23 марта 2017 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, используемых ею для защиты информации и проводной и беспроводной связи. В качестве примеров ее деятельности можно привести следующие:

a) на всей территории страны, в том числе на границах, усовершенствованы информационно-коммуникационные системы и внедрены защищенные сети с использованием технологии шифрования данных, передаваемых по протоколу IP. Армия использует эти сети с целью укрепления национальной и региональной безопасности;

b) Армия осуществляет сотрудничество в области безопасности с международным сообществом, применяя коммуникационные системы, совместимые с системами, используемыми Организацией Североатлантического договора и Армией Соединенных Штатов, и отвечающие международным стандартам шифрования первого типа;

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

d) Армия самостоятельно (без привлечения компании-поставщика) осуществляет обучение и сертификацию всех пользователей систем связи, а также технического и вспомогательного персонала, стремясь обеспечить максимальную надежность и безотказность этих систем 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.

Необходимо уделять постоянное внимание вопросам осведомленности граждан о масштабных угрозах в компьютерной сфере, связанных с использованием электронных систем, и о том, каким образом благодаря мерам в области кибербезопасности можно свести такие угрозы к минимуму и противодействовать им. При обработке любой информации крайне важно повышать осведомленность в вопросах безопасности при условии, что это не будет препятствовать применению технологий в благих целях.

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

a) использование алгоритмов шифрования для защиты коммуникационных систем речевой и видеосвязи и систем передачи данных;

b) использование закрытых сетей (интранет);

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

d) применение способов защиты информационно-коммуникационных систем и принципа минимальной необходимой осведомленности. Ведется постоянная проверка наличия разрешения на доступ и личности пользователей;

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

f) Иордания приняла следующие нормативно-правовые документы в области кибербезопасности:

1. принят закон о киберпреступности;

2. принят закон об электронных сделках;

3. разработан проект национальной стратегии по обеспечению кибербезопасности и защиты информации в киберпространстве;

4. разработана национальная политика в области кибербезопасности и защиты информации в киберпространстве;

5. национальная стратегия по обеспечению кибербезопасности и защиты информации в киберпространстве 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 информации в киберпространстве;

c) необходимо применять принцип минимальной необходимой осведомленности;

d) следует использовать такие технические приемы, как шифрование и скачкообразное 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 связанные с компьютерами чрезвычайные ситуации 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 предоставления мобильных банковских услуг, которые во всем мире принесли прямые и ощутимые выгоды миллионам людей, не имевшим 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) следует сформировать международные группы реагирования и восстановления, которые будут устранять инциденты, кризисы и катастрофы в области кибербезопасности;

b) в состав созданной в 2003 году Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности следует включить представителя Иордании;

c) следует расширить обмены между членами Совета Безопасности по линии сотрудничества в области НИОКР и профессиональной подготовки.

Мадагаскар

[Подлинный текст на французском языке]
[20 июня 2017 года]

Рекомендации Организации Объединенных Наций основаны на требованиях международной безопасности и предусматривают следующие меры:

– проведение исследований, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем;

– оценку всех существующих и потенциальных угроз в сфере информационной безопасности и принятие надлежащих стратегий для борьбы с этим злом;

– участие государственных должностных лиц в укреплении информационной безопасности, с тем чтобы разработать общую концепцию глобальной безопасности.

В резолюции 71/28 конкретно говорится о сфере информатизации и телекоммуникаций, которая активно развивается в Мадагаскаре. Для представления ответа в связи с этой резолюцией требуется запросить мнение экспертов в этой области.

Нидерланды

[Подлинный текст на английском языке]
[31 мая 2017 года]

Нидерланды весьма удовлетворены возможностью представить информацию о мерах, принятых ими в связи с резолюцией 71/28 Генеральной Ассамблеи.

Киберпространство, и в особенности Интернет, является важнейшим ресурсом экономического и общественного роста. Возросшее значение киберпространства ставит перед международным сообществом новые вызовы. Различные общества тесно связаны между собой; они зависят от Интернета и информационно-коммуникационных технологий и стали более уязвимыми к ненадлежащему использованию этих технологий. Геополитическая напряженность проявляется в киберпространстве, и государства и другие субъекты все чаще используют кибероперации, преследуя свои стратегические интересы. В то же время кибероперации способны дестабилизировать международные отношения и могут угрожать международному миру и безопасности.

Необходимость международного сотрудничества в целях уменьшения этих рисков очевидна. В свете вышесказанного Нидерланды активизируют свое участие в кибердипломатии в интересах поддержания мира и стабильности в киберпространстве, поощрения международного правопорядка и укрепления культуры совместной безопасности, как об этом говорится в их международной киберстратегии «Наведение цифровых мостов».

Международное сообщество предпринимает шаги для устранения таких угроз. В этом плане весьма важную роль играют доклады Группы правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Нидерланды также признательны за предоставленную им возможность принять участие в работе Группы правительственных экспертов в 2017 году.

Нидерланды продолжают поощрять всеохватный диалог по вопросам ответственного поведения государств в киберпространстве, ведут работу по защите прав человека в онлайновом режиме и содействуют наращиванию потенциала посредством проведения различных мероприятий. Нидерландами был предпринят целый ряд усилий, из которых необходимо выделить следующие:

a) в лучших традициях оказания поддержки в развитии международного правопорядка Нидерланды организовали консультативное совещание по второй версии Таллинского руководства по международно-правовым нормам, применимым к операциям в киберпространстве, с участием юридических советников государств;

b) Нидерланды оказали поддержку Институту Организации Объединенных Наций по исследованию проблем разоружения в организации серии из трех практикумов по кибернормам, нормам международного права и борьбе с распространением вредоносных инструментов и методов, в которых успешно приняли участие дипломаты и представители технического сообщества;

c) и наконец, Нидерланды выступили с целым рядом инициатив по содействию разработке руководящих норм, включая создание Глобальной комиссии по стабильности в киберпространстве, которая разработает предложения в отношении норм и политики, направленных на укрепление международной безопасности и стабильности.

Все вышеперечисленные усилия призваны сделать международные отношения в цифровой сфере и само киберпространство более стабильными и безопасными. Нидерланды придают этим усилиям важнейшее значение с точки зрения снижения риска конфликтов и сохранения открытого, свободного и безопасного киберпространства.

Норвегия

[Подлинный текст на английском языке]
[27 июля 2017 года]

Норвегия входит в число мировых лидеров в области внедрения цифровых технологий и в растущей степени зависит от хорошо функционирующего и безопасного киберпространства. Она твердо привержена поддержанию свободного, открытого, мирного и безопасного киберпространства, с тем чтобы обеспечиваемые им экономические и социальные преимущества были защищены и доступны для всех. Киберпространство не знает национальных границ, и его безопасность может быть обеспечена только в международном масштабе и на основе тесного сотрудничества между государствами и частным сектором.

Меры, принятые в целях укрепления информационной безопасности

Национальные подходы

Правительство выпустило официальный документ, озаглавленный «Безопасность ИКТ: совместная ответственность» (2016–2017 годы), который содержит планы разработки национальной программы улучшения координации между заинтересованными сторонами на национальном уровне и создания технической платформы для улучшения обмена информацией между государственными и частными структурами.

31 марта 2017 года был учрежден Объединенный координационный центр по вопросам киберпространства для служб безопасности и разведки.

Международные подходы

Правительство опубликовало официальный документ по вопросу о глобальных вызовах в области безопасности во внешней политике страны (2014–2015 годы), в котором борьбе с киберугрозами уделено значительное внимание.

Норвегия собирается приступить к осуществлению международной стратегии в области киберпространства в стране.

Норвегия принимает участие в ряде инициатив, касающихся регионального сотрудничества по вопросам киберпространства, таких как:

a) работа в рамках Организации по безопасности и сотрудничеству в Европе (ОБСЕ) по подготовке соответствующих норм и мер укрепления доверия, призванных уменьшить риск возникновения конфликтов, связанных с использованием информационно-коммуникационных технологий (ИКТ);

b) тесное сотрудничество с Экспертным центром по совместной кибероборо не Организации Североатлантического договора в Таллине, в том числе по вопросам применения международного права в киберпространстве и развития доктрины;

c) Конвенция Совета Европы о киберпреступности.

Норвегия поддерживает работу Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Норвегия принимает участие в двусторонних и региональных диалогах по вопросам киберпространства, особенно в рамках государств Северной Европы.

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

Норвегия считает, что международное право применимо к киберпространству и что соблюдение норм международного права, в частности обязательств, вытекающих из Устава Организации Объединенных Наций, является важной основой для деятельности ее государств-членов, связанной с использованием ИКТ. Международному сообществу необходимо продолжить изучение вопроса о применимости международного права в киберпространстве, а также норм ответственного поведения в киберпространстве.

Устойчивость глобального Интернета зависит от наличия надлежащего баланса между открытостью, безопасностью, надежностью и свободой. Это может быть обеспечено только на основе международного сотрудничества и диалога на глобальном и региональном уровнях. Текущая работа по этому вопросу в рамках таких форумов, как Организация Объединенных Наций, Европейский союз, Организация экономического сотрудничества и развития и ОБСЕ, должна быть продолжена.

Всеобщие права человека также применяются в киберпространстве. В режиме онлайн должна обеспечиваться защита тех же прав, которыми люди пользуются в обычной жизни, в частности права на свободу выражения мнений, в том числе права искать, получать и распространять информацию, а также права на неприкосновенность частной жизни.

Парагвай

[Подлинный текст на испанском языке]
[31 июля 2017 года]

Парагвай разделяет мысль о растущей важности информационной безопасности на глобальном уровне с учетом большой зависимости правительств от информационно-коммуникационных технологий и киберпространства. Реакция на эволюцию кибератак должна быть коллективной, динамичной и пропорциональной. Без стратегического реагирования на глобальном уровне усилия отдельно взятых стран в области кибербезопасности будут неустойчивыми, спорадическими и неэффективными и будут постоянно дублироваться.

В целях укрепления информационной безопасности на национальном уровне в апреле 2017 года правительство Парагвая одобрило национальный план обеспечения кибербезопасности, в разработке которого непосредственно участвовали представители всех секторов, имеющих определенные функции и интересы в киберпространстве. Этот план служит основой для государственной и национальной политики в этой области и устанавливает направления действий, которые должны быть приняты Парагваем для укрепления безопасности его важнейших активов и обеспечения безопасного, надежного и устойчивого киберпространства. В парагвайском уголовном законодательстве предусмотрена ответственность за компьютерные преступления. В течение последних пяти лет Парагвай принимает у себя в стране Конгресс и Иберо-американскую ярмарку по вопросам информационной безопасности — форум для обмена опытом, ознакомления с новыми наработками и оценки решений проблем, связанных с ростом масштабов использования информационно-коммуникационных технологий.

Что касается субрегионального уровня, то у «Южноамериканского общего рынка» (МЕРКОСУР) имеется постоянный орган, который именуется Совещанием органов по вопросам, касающимся конфиденциальности, информационной безопасности и технологической инфраструктуры МЕРКОСУР и в рамках которого выдвигаются предложения об общих стратегиях и инициативах в области кибербезопасности. При этом в регионе Северной и Южной Америки существует своя Межамериканская комплексная стратегия кибербезопасности, в которой признается, что для формирования культуры кибербезопасности все участники сетей и информационных систем должны осознавать свои функции и обязанности в вопросах обеспечения безопасности.

Создание эффективной основы для защиты сетей и информационных систем, включая Интернет, в глобальных масштабах, а также для реагирования на инциденты и ликвидации их последствий, будет зависеть от принятия международным сообществом следующих мер:

– предоставление пользователям информации для защиты их информационных систем от угроз и факторов уязвимости;

– поощрение партнерских отношений между государственным и частным секторами в целях повышения уровня информированности и осведомленности;

– выявление и оценка технических стандартов и передовой практики для обеспечения безопасности информации, передаваемой по каналам сетей связи, и содействие их принятию;

– содействие принятию касающихся киберпреступлений политики и законов, которые защищают пользователей и не допускают ненадлежащего и незаконного использования компьютерного оборудования при соблюдении неприкосновенности прав отдельных пользователей.

Португалия

[Подлинный текст на английском языке]
[27 июля 2017 года]

В своей резолюции 71/28 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. Прогресс в области информатизации и телекоммуникаций означает

расширение возможностей для развития знаний, сотрудничества между государствами, поощрения человеческого творчества и распространения информации в обществе в целом; с другой стороны, Португалия считает, что эти технологии и средства потенциально могут быть использованы в ущерб международной стабильности и безопасности и могут негативно воздействовать на национальную целостность государств.

В резолюции 71/28 государствам-членам было предложено представить информацию по четырем направлениям:

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 своем докладе 2013 года (A/68/98) Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности приводит некоторые рекомендации относительно следующих областей: нормы, правила и принципы ответственного поведения государств; меры укрепления доверия и обмен информацией; и меры по наращиванию потенциала.

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

Нормы, правила и принципы, характеризующие ответственное поведение государств

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

Важно отметить прогресс, достигнутый в работе по осуществлению законодательства об обеспечении безопасности и целостности сетей посредством применения таких методов оценки рисков, которые требуют принятия надлежащих совместных мер безопасности на техническом и организационном уровнях и представления информации о нарушениях режима безопасности или утрате целостности, которые существенно сказываются на функционировании служб.

В концептуальном плане важно пропагандировать идею о том, что регулирование должно в первую очередь основываться на международных нормах.

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

Меры укрепления доверия и обмена информацией

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

На национальном уровне усилия Португалии были направлены на проведение совместных учебных мероприятий, в которых приняли участие государственные и частные структуры; на поощрение технической стандартизации и на организацию конференций и семинаров, в том числе с участием международных докладчиков.

Меры по наращиванию потенциала

Разработка мер по наращиванию потенциала представляет собой важную задачу. Вместе с тем организация учебной подготовки и обеспечение людских ресурсов, необходимых для проведения этой деятельности, сопряжены с определенными трудностями.

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

Катар

[Подлинный текст на английском языке]
[4 мая 2017 года]

Некоторое время назад Государство Катар признало, что информационная безопасность и кибербезопасность — это вопрос не только технологий, но и национальной политики. В этой связи в 2005 году был создана Катарская группа реагирования на связанные с компьютерами чрезвычайные ситуации (см. www.Qcert.org), с тем чтобы активизировать процесс перемен, и в частности ускорить повсеместное внедрение эффективной практики и политики в области кибербезопасности; в настоящее время у Группы имеется национальный мандат на защиту цифровых активов Государства Катар.

В 2013 году премьер-министр учредил Национальный комитет по кибербезопасности. Комитет разработал национальную стратегию кибербезопасности, призванную повысить безопасность Катара и обеспечить дальнейший рост и успешное развитие страны и включающую следующие пять базовых принципов, которые определяют направления будущей деятельности:

- защита важнейшей национальной информационной инфраструктуры;
- принятие мер реагирования, преодоление и ликвидация последствий инцидентов и нападений в компьютерной сфере на основе своевременного обмена информацией, сотрудничества и практических действий;
- создание нормативно-правовой базы для обеспечения безопасного и жизнеспособного киберпространства;
- формирование культуры кибербезопасности, которая содействует безопасному и надлежащему использованию киберпространства;
- развитие и укрепление национального потенциала в области кибербезопасности.

Группа реагирования на связанные с компьютерами чрезвычайные ситуации успешно предоставляет широкий перечень услуг в сфере информационной безопасности, направленных на удовлетворение потребностей населения, предприятий и организаций страны, особенно в таких областях, как реагирование на инциденты, разведка, устойчивость к внешним воздействиям, учебная и информационная деятельность, урегулирование кризисов, лицензирование и идентификация ключевых объектов общественной инфраструктуры, а также

создание национальной системы соблюдения требований информационной безопасности.

Катар считает, что в настоящее время на региональном и международном уровнях существует разрыв в способности различных государств получать и распространять достаточный объем данных о ситуации в киберпространстве , необходимых для эффективного принятия решений. Необходимо продолжать совместную профилактическую работу по укреплению кибербезопасности всей информационной инфраструктуры и соответствующих служб в целях обеспечения устойчивости к внешнему воздействию, особенно в том, что касается нормального ежедневного функционирования органов управления, сферы услуг, деловых кругов, потребителей и граждан.

Кибербезопасность может быть максимально эффективно обеспечена только в условиях обмена информацией. Разработка соглашений об обмене информацией принесла бы государствам большую пользу посредством создания рамочных основ для сотрудничества, позволяющих конкретизировать методы проверки и контроля за соблюдением.

Нападения неминуемы — и государства, правительства, организации и промышленные круги должны быть готовы отражать их на совместной основе.

Сингапур

[Подлинный текст на английском языке]
[31 июля 2017 года]

Как малое государство с высокой степенью подключенности к Интернету Сингапур поддерживает идею создания защищенного и устойчивого к внешним воздействиям киберпространства, опирающегося на фундамент международного права, тщательно проработанные нормы ответственного поведения государств и скоординированные усилия по наращиванию потенциала, необходимого для соблюдения этих норм. Для решения новых проблем, порождаемых киберугрозами, необходимо эффективное международное сотрудничество, в котором Сингапур готов играть свою роль.

В 2015 году Сингапур учредил Агентство информационной безопасности для централизованного надзора за осуществлением функций по обеспечению национальной кибербезопасности. В октябре 2016 года была принята Сингапурская стратегия обеспечения кибербезопасности, в которой излагается комплексный подход к защите основных служб от киберугроз и созданию безопасного киберпространства. В основе стратегии лежат четыре компонента: создание устойчивой к внешним воздействиям инфраструктуры; формирование более безопасного киберпространства; развитие динамичной экосистемы кибербезопасности; и укрепление международных партнерств.

На региональном уровне Сингапур работает над формированием и укреплением потенциала соседних стран. В целях поддержки региональных усилий по укреплению потенциала он в сотрудничестве с Ассоциацией государств Юго-Восточной Азии (АСЕАН) приступил к осуществлению программы «Киберпотенциал» стоимостью в 10 млн. сингапурских долларов. В рамках этой программы Сингапур провел в мае 2017 года практикум по тематике кибернорм, а в августе 2017 года проведет практикум по наращиванию потенциала в области кибербезопасности стран — членов АСЕАН. Он также ежегодно проводит у себя в стране Сингапурскую международную неделю кибербезопасности, в ходе которой организуются Конференция на уровне министров стран АСЕАН по вопросам кибербезопасности и Международный симпозиум лиде-

ров по цифровому информационному пространству, в рамках которых мировые лидеры, представляющие правительственные, промышленные и научные круги, налаживают контакты с региональными участниками и обсуждают новые и сквозные вопросы.

Что касается многостороннего сотрудничества, то Сингапур поддерживает работу Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, включая 11 норм, изложенных в его докладе 2015 года. Важно определить и применять те нормы, которые пользуются единодушной поддержкой, особенно нормы оперативной деятельности. Они включают в себя отказ от поддержки онлайновой деятельности, которая наносит преднамеренный ущерб важнейшим объектам инфраструктуры; отказ от поддержки деятельности, препятствующей группам реагирования на инциденты в области компьютерной безопасности в принятии ответных мер в связи с инцидентами в компьютерной сфере; и недопущение задействования этих групп реагирования в злонамеренной международной деятельности.

Турция

[Подлинный текст на английском языке]
[31 июля 2017 года]

Информационно-коммуникационные технологии (ИКТ) стали неотъемлемой частью жизни современного общества и экономической жизни. Они способствуют повышению благосостояния и развитию общества, а также улучшению повседневного быта. Они используются в самых различных сферах, охватывающих деятельность государственного и частного секторов, важнейшие объекты инфраструктуры и отдельных людей, и получили широкое распространение в стране и в мире, несмотря на риски в области кибербезопасности.

С учетом этого Турция участвует во многих инициативах, содействуя сотрудничеству по вопросам кибербезопасности. Преследуемая цель заключается в обеспечении кибербезопасности. В этом контексте были проведены национальные учебные мероприятия по обеспечению кибербезопасности, которые координировало Министерство транспорта, мореходства и коммуникаций; в Стамбуле состоялись первые международные учения «Электронный щит»; Турция также регулярно (на ежегодной основе) принимает участие и оказывает помощь в проведении международных учений по кибербезопасности, таких как «Кибер-коалиция» Организации Североатлантического договора (НАТО), «Сомкнутые щиты» НАТО и учения по отработке взаимодействия при разрешении кризисных ситуаций НАТО.

Повысилась эффективность диалога и сотрудничества с Организацией Объединенных Наций, НАТО, Европейским союзом, Организацией по безопасности и сотрудничеству в Европе и другими международными и неправительственными организациями, научными кругами и лидерами, формирующими общественное мнение. Этот подход укрепляется в рамках конференций, курсов, семинаров, совещаний, программ последипломного образования и других программ поддержки. Турция играет ведущую роль в региональных усилиях в области кибербезопасности путем заключения двусторонних соглашений с различными государствами.

Комитетом кибероборонны НАТО был утвержден меморандум о взаимопонимании, посвященный вопросам сотрудничества между НАТО и ее союзниками, и ведется соответствующая работа по его подписанию. Турция — одна из стран, предоставляющих средства для Экспертного центра НАТО по совмест-

ной кибероборонe. Отслеживается работа Комитета НАТО по планированию на случай чрезвычайных ситуаций гражданского характера и совещаний Регионального центра по содействию проверке и осуществлению контроля над вооружениями – Центра по сотрудничеству в области безопасности, развивается сотрудничество и по различным другим вопросам. Турция является одним из основателей Глобального форума по киберэкспертизе и стала участником рамочного документа и Гаагской декларации о Глобальном форуме.

В ходе Саммита Группы 20, который прошел в Турции 15 и 16 ноября 2015 года, было принято решение по вопросам кибербезопасности с акцентом на деятельности Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Конвенция Совета Европы о киберпреступности была подписана Турцией в 2010 году в Страсбурге и утверждена Законом № 6533 в 2014 году; впоследствии была проведена работа по ее адаптации к национальному законодательству.

В результате сбора, анализа и оценки информации, полученной в рамках совещаний и аналитических платформ, были подготовлены национальная стратегия и план действий в области кибербезопасности на период 2016–2019 годов.

Укрепление информационной безопасности на глобальном уровне и — тем самым — формирование культуры безопасности в рамках международного сообщества является исключительно важным для всех вопросом. В то же время каждое государство в интересах сохранения национальной безопасности имеет право принимать меры для защиты от злонамеренного использования ИКТ террористами, экстремистами, организованными преступными группами и действующими в одиночку хакерами. В этой связи огромное значение имеет также укрепление международно-правовых актов и расширение двусторонних международных соглашений.

Соединенное Королевство Великобритании и Северной Ирландии

[Подлинный текст на английском языке]
[31 июля 2017 года]

Соединенное Королевство приветствует возможность представить ответ на просьбу, содержащуюся в резолюции 71/28 Генеральной Ассамблеи, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», который основывается на его ответе на резолюцию 70/237, представленном в 2016 году. В своем ответе во избежание путаницы Соединенное Королевство использует предпочитаемый им термин «кибербезопасность» и связанные с ним понятия, 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. Реальные и потенциальные угрозы, создаваемые в результате деятельности в киберпространстве, вызывают серьезную озабоченность. На основе новой национальной стратегии кибербезопасности, опубликованной в октябре 2016 года, будут определяться меры, которые будут прини-

маться страной в течение следующих пяти лет для защиты своих активов, сдерживания своих противников и развития своего сектора кибербезопасности.

Соединенное Королевство продолжает играть одну из ведущих ролей в международных дискуссиях по вопросам кибербезопасности. Оно предоставляло экспертов в состав всех пяти групп правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Несмотря на отсутствие консенсуса в Группе 2017 года, страна исполнена решимости поощрять создание международных рамок для обеспечения стабильности киберпространства на основе применения существующих международно-правовых норм, согласованных добровольных норм ответственного поведения государств и мер укрепления доверия с опорой на скоординированные программы наращивания потенциала. Соединенное Королевство также приветствует усилия Организации по безопасности и сотрудничеству в Европе и других региональных форумов, направленные на представление предложений по осуществлению мер укрепления доверия, и будет продолжать подавать пример в принятии таких мер.

В настоящем ответе в общих чертах обрисованы основные усилия Соединенного Королевства, направленные на обеспечение и укрепление кибербезопасности и осуществление обмена передовым опытом как на внутригосударственном, так и на общемировом уровне, в том числе в сотрудничестве с международными партнерами, в рамках деятельности по борьбе с киберпреступностью и серьезными инцидентами и наращиванию потенциала. Соединенное Королевство рассчитывает на достижение дальнейшего прогресса и с удовлетворением принимает активное участие в работе по этим вопросам. Оно будет и далее в полной мере участвовать в укреплении потенциала и международного сотрудничества в области кибербезопасности.