Организация Объединенных Наций A/68/156/Add.1

Генеральная Ассамблея

Distr.: General
9 September 2013
Russian
Original: Arabic/English

Шестьдесят восьмая сессия
Пункт 94 предварительной повестки дня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Добавление**

Содержание

* A/68/150.

** Информация, приведенная в настоящем докладе, была получена после выхода основного доклада.

13-47547 (R) 091013 091013

II. Ответы, полученные от правительств

Армения

[Подлинный текст на английском языке]
[5 июля 2013 года]

Концепция информационной безопасности была утверждена указом президента Республики Армения № NK-97 от 25 июня 2009 года. В ней говорится, что национальная безопасности Республики Армения во многом зависит от информационной безопасности, которая включает такие компоненты, как информационные, коммуникационные и телекоммуникационные системы. Концепция также содержит общий анализ проблем в области информационной безопасности Республики Армения, существующих трудностей и угроз и их коренных причин и особенностей, а также методов по урегулированию в различных сферах общественной жизни.

Для координации осуществления программ, связанных с концепцией информационной безопасности, был создан межправительственный комитет.

25 февраля 2010 года правительство Республики Армения утвердило концепцию формирования электронного общества. Был создан Совет по электронному управлению и определены общие рамки информационной безопасности в рамках концепции формирования электронного общества. В приложении 4 к концепции излагаются мероприятия по обеспечению информационной безопасности государства. Для достижения вышеуказанных целей были сформированы государственные комитеты и группы экспертов.

Для укрепления информационной безопасности на национальном уровне были также приняты следующие меры.

В соответствии с постановлением правительства № 479-N от 30 апреля 2009 года был разработан и в настоящее время вступил в строй специальный информационный центр, занимающийся вопросами безопасности Интернета. Этот центр обеспечивает защищенность публичной информации государственных органов, загружаемой в Интернет, и защищенное подключение информационных систем государственных органов к Интернету.

В начале 2012 года группа экспертов разработала проект национальной программы создания системы информационной безопасности Республики Армения. В настоящее время проект программы обсуждается в правительстве Армении.

В 2006 году Республика Армения ратифицировала Конвенцию по киберпреступности, открытую для подписания в 2006 году в Будапеште, а в 2012 году — Конвенцию о защите физических лиц при автоматизированной обработке персональных данных. Компетентными государственными органами, отвечающими за выполнение положений вышеуказанных конвенций, являются Служба национальной безопасности и полиция Республики Армения. На данном этапе деятельностью по приведению соответствующих положений национального законодательства в соответствии с нормами Конвенции занимается межправительственная группа экспертов.

Республика Армения развивает активное сотрудничество в области информационной безопасности в рамках Организации по безопасности и сотрудничеству в Европе (ОБСЕ). В настоящее время армянская сторона участвует в рамках неофициальной рабочей группы в переговорах по разработке комплекса мер укрепления доверия в области информационной безопасности. Армянская сторона включила одну меру и семь вспомогательных мер в сфере кибербезопасности в План действий индивидуального партнерства, которое в настоящее время осуществляется в сотрудничестве с Организацией Североатлантического договора.

Канада

[Подлинный текст на английском языке]
[3 сентября 2013 года]

Принимая во внимание оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов по достижению в сфере информатизации и коммуникации в контексте международной безопасности, Канада хотела бы поделиться с Генеральным секретарем своими взглядами и оценками по следующим вопросам.

1. Информационная безопасность

Канада обеспокоена реальными и усиливающимися угрозами, которые представляет злонамеренная деятельность в киберпространстве, и признает, что борьба со злонамеренным использованием ИКТ требует национального, регионального и международного сотрудничества.

Канада стратегически заинтересована в сохранении открытого киберпространства ввиду его важности для процветания и безопасности Канады, а также ценности демократии и прав человека. Как государственный, так и частный сектора Канады зависят в своей повседневной деятельности от защищенной, надежной и стабильной информационной инфраструктуры. Компьютерные системы вместе с Интернетом и сетевыми подключениями являются центральным элементом большей части критически важной инфраструктуры Канады, включая энергоснабжение, финансы, телекоммуникации и промышленное производство, и государственных информационных систем. Бесперебойное функционирование критически важной инфраструктуры способствует поддержанию нашего образа жизни и экономическому, политическому и социальному благополучию Канады.

Национальный уровень

Еще в 1996 году правительство Канады признало, что системы, имеющие жизненно важное значение для функционирования критически важной инфраструктуры Канады, могут стать объектом кибератак, и что правительство надлежит принять необходимые меры по защите этих систем от таких атак. В последующие годы правительство приняло соответствующие меры. Изучив свои возможности в области оценки и снижении уязвимости объектов инфраструктуры, оно разработало и внедрило комплексный подход к защите ключевых инфраструктурных объектов посредством налаживания партнерских отношений и обеспечило контроль и анализ кибератак и угроз, которым подвергаются

системы федерального правительства. В 2010 году правительство утвердило национальную стратегию и план действий в отношении ключевых инфраструктурных объектов, а ранее в том же году — план действий по реализации стратегии информационной безопасности на 2010–2015 годы, которая предусматривает обеспечение защищенности государственных систем, установление партнерских отношений для обеспечения защищенности жизненно важных киберсистем за рамками федерального правительства и оказание канадцам помощи в получении защищенного онлайнового доступа.

Международный уровень

С 2007 года Канада является одним из ключевых участников программы кибербезопасности Организации американских государств (ОАГ), которая предусматривает оказание американским государствам помощи в предотвращении и отслеживании киберугроз и реагировании на них путем совершенствования национального планирования и координации, а также регионального сотрудничества. В рамках своей программы наращивания контртеррористического потенциала Канада оказывает ряду государств — членов ОАГ в разработке их собственных национальных стратегий кибербезопасности и входит в созданную ОАГ Защищенную сеть групп экстренной готовности к инцидентам в сфере кибербезопасности для стран Западного полушария.

С 2012 года Канада и другие государства — члены Организации по безопасности и сотрудничеству в Европе (ОБСЕ) занимаются разработкой мер укрепления доверия и безопасности для снижения вероятности возникновения недопонимания, эскалации напряженности и конфликтов, которые могут быть обусловлены использованием информационно-коммуникационных технологий.

Канада также активно участвует в международных инициативах по борьбе с киберпреступностью на ряде форумов, включая Группу восьми, Управление по наркотикам и преступности Организации Объединенных Наций и ОАГ. Канада также участвовала в работе последней Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (2012–2013 годы).

2. Международные концепции

Существующие нормы международного договорного и обычного права применимы к использованию информационно-коммуникационных технологий государствами и имеют важнейшее значение для поддержания мира и стабильности и создания открытых, безопасных, мирных и доступных условий для использования информационно-коммуникационных технологий. К существующим нормам международного права, имеющим непосредственное отношение к киберпространству, относятся Устав Организации Объединенных Наций, международные стандарты в области прав человека и международное гуманитарное право. Канада с удовлетворением отметила, что в последнем докладе Группы правительственных экспертов Организации Объединенных Наций содержится четкое подтверждение государствами применимости норм международного права в киберпространстве как основы для норм и принципов, регулирующих ответственное поведение государств.

Канада также убеждена в том, что усилия по обеспечению безопасности ИКТ должны гармонично сочетаться с уважением прав человека и основных

свобод, включая право беспрепятственно придерживаться своих мнений, а также право на их свободное выражение, свободу ассоциации и собраний и уважение тайны личной жизни. Право на свободное выражение мнений закреплено как во Всеобщей декларации прав человека, так и в Международном пакте о гражданских и политических правах. В этих инструментах предусматривается, что те права, которые человек имеет в офлайновой среде, должны также защищаться и в онлайновой среде, в частности право на свободу выражения мнений, которое осуществляется независимо от государственных границ и любыми средствами по собственному выбору.

3. Возможные меры по укреплению информационной безопасности во всем мире

В тесном сотрудничестве с международными партнерами, включая крупные многосторонние организации и ассоциации частного сектора, Канада занимается укреплением информационной безопасности сетей, от которых зависит экономическое процветание и безопасность страны. Канада также укрепляет сотрудничество и расширяет обмен информацией по вопросам кибербезопасности с некоторыми из своих ключевых партнеров и в рамках многосторонних организаций.

Канада разработала новую процедуру координации национальных мер, принимаемых в ответ на серьезные инциденты в киберпространстве, и привлекает владельцев и операторов своих ключевых инфраструктурных объектов к разработке и осуществлению собственной стратегии кибербезопасности.

Интерес к укреплению кибербезопасности и пресечению киберпреступности проявляют и многие другие страны. Главным международным инструментом, посвященным непосредственно киберпреступности, является Конвенция Совета Европы о киберпреступности, которую Канада подписала в 2001 году. Этот документ, известный также как Будапештская конвенция, содержит подробные указания по разработке всеобъемлющего национального законодательства по борьбе с киберпреступностью и определяет рамки международного сотрудничества между государствами.

Германия

[Подлинный текст на английском языке]
[25 июня 2013 года]

Общее положение в области информационной безопасности

Электронизация экономических, административных и личных связей не только продолжается, но и ускоряется. Это открывает беспрецедентно широкие возможности как для промышленно развитых, так и для развивающихся стран. В то же время усиление зависимости от информационно-коммуникационных технологий приводит к повышению уязвимости и возникновению системных недостатков. Кроме того, усиливается взаимосвязанность всех сторон: от частных пользователей до предпринимателей и государственных организаций. В области кибератак наблюдается явно выраженная тенденция к усложнению вредоносных действий, таких как целенаправленные устойчивые угрозы, или использованию чрезвычайно сложных вредоносных программ против целей

повышенной ценности. Эта деятельность ведется в интересах получения прибыли или информации, позволяющей контролировать ключевые активы, системы и, соответственно, объекты инфраструктуры, что чревато неблагоприятными последствиями для правительств, многочисленных предприятий и организаций, включая поставщиков ключевых инфраструктурных услуг. Злонамеренное использование продвинутых технических средств с огромным трудом поддается обнаружению. Попытки защитить существующие технологии, как правило, не поспевают за инновационной деятельностью. Опасность усугубляется и тем, что доступ к вредоносным инструментам и методам достаточно легко получить, поскольку они предлагаются за деньги на нерегулируемом или черном рынке. Защитить от них сложившуюся среду применения информационных технологий при помощи лишь традиционных подходов к обеспечению информационной безопасности невозможно.

Высокопрофессиональные хакеры тратят значительные технические и финансовые средства на выявление слабых мест в системах ИКТ и их использование в своих целях. Угрозы национальной и международной безопасности усугубляются и сложностью достоверной идентификации автора атак, что открывает возможности для совершения атак под чужим именем, приводя, в частности, к недопониманию и просчетам. Попытки взлома систем для сбора информации на первом этапе зачастую ничем не отличаются от попыток взлома с целью уничтожения. Это еще больше повышает опасность неправильной оценки характера происходящих атак и возможного нарушения ими запрета на применение силы в международных отношениях.

Дополнительная непредсказуемость обусловлена отсутствием ясности в вопросе о том, какие нормы должны применяться в киберпространстве.

Особенно уязвимыми для злонамеренного использования ИКТ оказались системы управления производственными процессами на ключевых объектах инфраструктуры. На глобальном уровне риски нанесения неконтролируемого сопутствующего ущерба, включая инфицирование систем производственного контроля, чреватое физическими разрушениями, велики. Кибератака на какой-либо ключевой объект телекоммуникационной инфраструктуры может причинить больше глобальных разрушений, чем реальное нападение на отдельный материальный объект.

Независимо от различий в уровне развития и безопасности ИКТ в разных государствах конкретные шаги по наращиванию потенциала противодействия зачастую откладываются или вообще снимаются с повестки дня в результате отсутствия ясности в вопросах рисков кибербезопасности и путей эффективного противодействия им, сложности и новизны кибератак, а также завесы тайны вокруг отдельных инцидентов.

Меры, принимаемые на национальном уровне

В 1991 году было создано Федеральное управление по информационной безопасности (Bundesamt für Sicherheit in der Informationstechnik, BSI), являющееся в первую очередь центральным поставщиком услуг по обеспечению безопасности информационных технологий для федерального правительства. В этом качестве ФУИБ выпускает обязательные минимальные стандарты безопасности в области информационных технологий для федеральных органов и является центральным органом по информированию об инцидентах в области

информационных технологий. Кроме того, Управление выступает в качестве нейтрального органа по оказанию консультационных услуг и поддержки в сфере безопасности информационных технологий. К числу главных достижений Управления относятся, например, стандарт в области обеспечения безопасности информационных технологий (IT-Grundschutz), Группа быстрого реагирования на компьютерные угрозы федеральным ведомствам (CERT-Bund) как платформа для организации действий в связи с инцидентами и обмена информацией (созданная еще в 1994 году) и Гражданская группа быстрого реагирования на компьютерные угрозы (Buerger-CERT), созданная в 2006 году для мобилизации более широких слоев населения и повышения уровня осведомленности. Кроме того, ФУИБ распространяет уведомления о вредоносных программах и уязвимости информационных продуктов и услуг с точки зрения безопасности, информирует заинтересованные стороны (включая поставщиков информационных технологий и широкую общественность) и готовит рекомендации в отношении контрмер.

Вслед за принятием в 2005 году национального плана действий по защите информационной инфраструктуры, предназначенного как для правительства, так и для предпринимателей, последовало принятие федеральным правительством в феврале 2011 году стратегии кибербезопасности. Ее главная цель заключается в защите ключевых инфраструктурных объектов.

С 2008 года правительство Германии и операторы ключевых инфраструктурных объектов Германии сотрудничают в рамках государственно-частного партнерства. Этот план действий по защите ключевых объектов инфраструктуры (UP KRITIS) предусматривает создание рабочих групп по различным аспектам кибербезопасности, таким как кризисное управление, функционирование и наличие важнейших услуг.

Национальный ситуационный центр по информационным технологиям (Nationales IT-Lagezentrum), которым руководит ФУИБ, следит за ситуацией в области безопасности информационных технологий на национальном и глобальном уровнях для оперативного выявления и анализа крупных инцидентов в сфере безопасности информационных технологий и вынесения рекомендаций в отношении мер защиты. В случае возникновения кризиса в сфере информационных технологий он привлекает дополнительные ресурсы и преобразуется в Национальный центр реагирования на кризис в сфере информационных технологий (Nationales IT-Krisenreaktionszentrum), в котором сосредоточены ресурсы для урегулирования всех национальных аспектов кризисов в сфере информационных технологий, включая государственные сети и ключевые инфраструктурные объекты.

В соответствии со стратегией кибербезопасности, принятой в 2011 году, все государственные органы, занимающиеся вопросами кибербезопасности, должны поддерживать тесное сотрудничество напрямую друг с другом и с частным сектором в рамках Национального центра кибербезопасности (Nationales Cyber-Abwehrzentrum), возглавляемого ФУИБ и расположенного в его помещениях.

Что касается политики, то Национальный центр кибербезопасности (Nationaler Cyber-Sicherheitsrat) на уровне государственного секретариата занимается ключевыми проблемами кибербезопасности и выработкой позиции Германии по отношению к ним. Эта деятельность охватывает координацию

внешней политики в отношении информационных технологий, включая ряд аспектов внешней политики, экономической политики и политики в области обороны и безопасности.

Кроме того, в октябре 2012 года началось создание на национальном уровне платформы для сотрудничества и обмена информацией: Альянс за кибербезопасность (Allianz für Cybersicherheit) оказывает помощь в налаживании тесного сотрудничества между партнерами в экономической, научной и административной областях и, в частности, с предприятиями, представляющими особый интерес для общества.

После четырех лет осуществления плана действий по защите ключевых объектов инфраструктуры началось его обновление. Теперь план будет распространен на большее число операторов ключевых инфраструктурных объектов и будет предусматривать создание ряда новых рабочих групп в ключевых инфраструктурных секторах. Кроме того, будет налажено сотрудничество с новым Альянсом за кибербезопасность.

Наличие международных соединений в киберпространстве определяет важность согласованных действий на международном уровне. Поэтому Германия решительно выступает в Европейском союзе и международных организациях за укрепление кибербезопасности и одновременно за защиту социальных и экономических преимуществ в киберпространстве.

Ввиду глобальной взаимопереплетенности информационных технологий Германия в рамках своей стратегии кибербезопасности выступает за разработку широких, не вызывающих разногласий и политически обязывающих норм поведения государств в киберпространстве. Эти нормы должны быть приемлемы для значительной части международного сообщества и должны включать меры укрепления доверия и безопасности.

Меры укрепления доверия и безопасности в киберпространстве

Киберпространство является общественным благом и публичным пространством. В силу этого мы должны рассматривать безопасность киберпространства с точки зрения устойчивости инфраструктуры, а также сохранности систем и содержащихся в них данных и их защищенности от сбоев. Поскольку киберпространство является публичным пространством, государства обязаны содействовать укреплению безопасности киберпространства, особенно безопасности от преступлений и злонамеренных действий, путем защиты тех, кто прибегает к программам проверки подлинности против хищения личных данных, и обеспечения сохранности и конфиденциальности данных и сетей.

Киберпространство по своей природе глобально. Обеспечение кибербезопасности, обеспечение соблюдения прав и защита ключевых объектов информационной инфраструктуры требуют от государства значительных усилий как на национальном уровне, так и в сотрудничестве с международными партнерами. На национальном уровне в Германии сложилась уникальная культура сотрудничества между большим числом групп быстрого реагирования на компьютерные угрозы, созданных в различных экономических, научных и административных органах. В этой связи следует указать, что традиционным координатором действий этих групп является CERT-Bund. На общеевропейском и международном уровнях CERT-Bund тесно сотрудничает с рядом других государ-

ственных групп быстрого реагирования на компьютерные угрозы, причем важнейшим глобальным форумом для налаживания взаимосвязи между группами быстрого реагирования на компьютерные угрозы выступает сеть Форума центров компьютерной безопасности и реагирования на компьютерные инциденты (FIRST).

В этих условиях Германия готова работать над подготовкой комплекса норм, которые регулировали бы поведение государств по отношению друг к другу в киберпространстве, включая прежде всего меры повышения доверия, транспарентности и безопасности, и которые были бы одобрены как можно большим числом стран. Поэтому Германия активно участвовала в 2012–2013 годах в работе Группы правительственных экспертов, которой было поручено «продолжить изучение существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, включая нормы, правила или принципы ответственного поведения государств и меры укрепления доверия в информационном пространстве…» (резолюция 66/24 Генеральной Ассамблеи).

На состоявшейся 9 и 10 мая 2011 года конференции Организации по безопасности и сотрудничеству в Европе (ОБСЕ), посвященной вопросам кибербезопасности, Германия представила следующие возможные элементы такого основанного на международных нормах кодекса поведения:

a) подтверждение общих принципов доступности, конфиденциальности, конкурентоспособности, сохранности и подлинности данных и сетей, защиты персональных данных и прав интеллектуальной собственности;

b) выполнение обязательств по защите ключевых объектов инфраструктуры;

c) расширение сотрудничества, направленного на укрепление доверия, осуществление мер по снижению рисков, повышение транспарентности и стабильности посредством:

i) обмена сведениями о национальных стратегиях, передовым опытом и национальными концепциями международного регулирования киберпространства;

ii) обмена мнениями на межгосударственном уровне относительно международно-правовых норм, касающихся использования киберпространства;

iii) создания контактных центров и уведомления о них;

iv) создания механизмов раннего предупреждения и расширения сотрудничества между группами быстрого реагирования на компьютерные угрозы;

v) модернизации линий связи в кризисных ситуациях с целью учета случаев компьютерных инцидентов, содействия разработке технических рекомендаций, направленных на поддержание надежной и безопасной глобальной киберинфраструктуры;

vi) выполнения задач по противодействию терроризму, включая обмен опытом и расширение сотрудничества по проблемам, связанным с негосударственными субъектами;

vii) поддержки укрепления потенциала развивающихся стран в сфере кибербезопасности и разработки принимаемых на добровольной основе мер по обеспечению кибербезопасности крупных мероприятий.

Руководствуясь этими положениями, Германия в июле 2012 года представила Группе правительственных экспертов Организации Объединенных Наций документ с изложением своей позиции. Мы горячо приветствуем рекомендации экспертов в отношении норм, правил и принципов ответственного поведения государств и в отношении мер укрепления доверия в киберпространстве, а также с удовлетворением отмечаем повышенное внимание, которое эксперты уделяют многостороннему подходу к кибербезопасности.

В 2011 и 2012 годах Германия оказывала поддержку проектам в области международной кибербезопасности и мер укрепления доверия и кибербезопасности, осуществлявшихся Институтом Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР) и Институтом по исследованию проблем мира и политики безопасности Гамбургского университета. Состоявшаяся в декабре 2011 года первая Берлинская киберконференция дала возможность начать международное обсуждение рисков, стратегий и мер укрепления доверия в области международной кибербезопасности. Вторая Берлинская киберконференция, состоявшаяся в сентябре 2012 года, была посвящена Интернету и правам человека. Один из главных выводов заключался в том, что безопасность, свобода и защищенность личной информации в онлайне являются взаимодополняющими концепциями. Германия также поддержала проведение 8 и 9 ноября 2012 года в Женеве Конференции ЮНИДИР по кибербезопасности, на которой основное внимание было уделено мерам укрепления доверия для обеспечения стабильности в киберпространстве.

Кроме того, мы считаем необходимым приступить к обсуждению возможностей международного сотрудничества в вопросах установления лиц, ответственных за кибератаки, которые обычно очень трудно отследить, установления ответственности государств за кибератаки, осуществленные с их территории, в случаях, когда государства, несмотря на получение информации о кибератаках, ничего не предпринимают для того, чтобы им воспрепятствовать, а также установления ответственности государств за отсутствие противодействия появлению в киберпространстве внеправовых зон, например в случае, когда государство знает о хранении на его территории незаконно собранных персональных данных и не борется с этим.

27 и 28 июня 2013 года на третьей Берлинской киберконференции, посвященной теме «Обеспечение безопасности и стабильности киберпространства: роль и значение международного права», и организованной федеральным министерством иностранных дел в тесном сотрудничестве с Потсдамским университетом, была предпринята попытка дать международно-правовую оценку кибероперациям, не отвечающим критериям вооруженного нападения и, таким образом, не подпадающим под положения права вооруженных конфликтов. В соответствии с действующими нормами и принципами международного права государства несут ответственность за действия лиц, находящихся на контролируемой ими территории, которые сказываются на безопасности и стабильности информационно-коммуникационных технологий. Каждое государство должно рассмотреть вопрос о том, как свести к минимуму или пресечь злонамеренную деятельность в киберпространстве, осуществляемую с контролируемой им тер-

ритории или по его сетям. Согласно действующим нормам международного обычного права, определяющим ответственность государств, государства несут ответственность за приписываемые им международно противоправные деяния в киберпространстве, в том числе за международно противоправные действия в киберпространстве, совершаемые любыми поддерживаемыми государством посредниками, которые действуют по указанию государства или под его руководством или контролем. Государства должны принимать все необходимые меры для недопущения использования их территории другими государствами или негосударственными субъектами в целях незаконного применения информационно-коммуникационных технологий против третьих государств и их интересов. Эти необходимые меры должны включать создание надлежащей нормативно-правовой базы, необходимой для выполнения международных обязательств. Государства могут оказаться связаны с международно противоправной деятельностью в киберпространстве тремя основными способами: 1) как страны, с территории которых совершаются злонамеренные действия в киберпространстве, способные привести к разрушительным последствиям; 2) как страны транзита, инфраструктура ИКТ которых используется при совершении злонамеренных действий в киберпространстве; и 3) как пострадавшие страны, которые понесли ущерб в результате злонамеренных действий в киберпространстве. Во всех этих случаях государства обязаны проявлять должную осмотрительность, которая может носить как существенный, так и процедурный характер и варьироваться от предупреждения, т.е. периода, предшествующего возможному нанесению ущерба, до сдерживания, т.е. периода фактического совершения пагубных действий в киберпространстве, и последующей деятельности, т.е. периода после совершения злонамеренных действий в киберпространстве.

Кибербезопасность в Организации по безопасности и сотрудничеству в Европе

В Организации по безопасности и сотрудничеству в Европе проблемы кибербезопасности обсуждаются в течение нескольких лет. На саммите ОБСЕ, состоявшемся в 2010 году в Астане, главы государств и правительств 56 государств — участников ОБСЕ подчеркнули необходимость достижения «большего единства целей и действий в противостоянии появляющимся транснациональным угрозам». В качестве одной из таких появляющихся транснациональных угроз в Астанинской юбилейной декларации упомянуты киберугрозы.

Германия приняла активное участие в работе конференции ОБСЕ по теме «Всеобъемлющий подход к кибербезопасности: определение будущей роли ОБСЕ», которая состоялась в 2011 году в Вене. В ходе этой конференции обсуждались конкретные рекомендации о последующих мерах, подлежащих принятию ОБСЕ. В мае 2012 годе Постоянный совет решением № 1039 (PC.DEC/1039) создал неофициальную рабочую группу и поручил ей разработать проект комплекса мер активизации доверия с целью активизации межгосударственного сотрудничества, повышения транспарентности, предсказуемости и стабильности и уменьшения рисков ошибочного восприятия, эскалации и конфликтов, которые могут возникнуть в результате применения информационно-коммуникационных технологий. В июне 2012 года Германия представила этой группе неофициальный документ со своими предложениями в отношении

первого комплекса мер укрепления доверия в рамках ОБСЕ. Германия выражает сожаление по поводу того, что в ходе заседания Совета министров, состоявшегося в декабре 2012 года в Дублине, не удалось добиться консенсуса по вопросу о принятии такого первого комплекса мер укрепления доверия, однако с удовлетворением отмечает, что в 2013 году Группа возобновила свою работу.

Германия будет и впредь активно поддерживать проходящие в ОБСЕ дискуссии по вопросам определения будущей роли этой организации в сфере кибербезопасности.

Военные аспекты кибербезопасности

Поскольку вооруженные силы также все более широко применяют информационные технологии для отработки все более сложных сценариев на всех уровнях командования, защита информации и средств ее обработки стала одной из первоочередных задач.

Вместе с тем военная доктрина считает, что угрозы информационной безопасности проистекают не только от потенциального оперативного противника, который может применить военную силу для физического уничтожения информационной инфраструктуры, но и от безответственных пользователей, сбоев в работе технических средств, действий преступников или же простонапросто аварийных ситуаций.

Таким образом, планируемые меры включают от повышения осведомленности каждого конкретного пользователя и обеспечения надежности цепочки поставок в сфере информационных технологий до создания гибких механизмов защиты от кибератак и обеспечения отказоустойчивости всех элементов архитектуры информационных технологий.

По сути необходимо создать всеобъемлющую систему управления рисками, которая предусматривала бы принятие мер по укреплению информационной безопасности на национальном и глобальном уровнях.

В вооруженных силах Германии (бундесвер) с самого начала создана надежная структура командования и управления, предусмотрены методы и процедуры обеспечения безопасности и создана организация по обеспечению информационной безопасности во всех родах войск, включающая группу быстрого реагирования на компьютерные угрозы, которая способна устранять критические сбои в работе информационных технологий. На постоянной основе ведется работа по обучению личного состава и наращиванию технического потенциала с учетом постоянного повышения уровня угрозы.

Вооруженные силы Германии тесно взаимодействуют с федеральным министерством внутренних дел Германии и решительно поддерживают укрепление информационной безопасности в Организации Североатлантического договора (НАТО) и Европейском союзе, а также разработку политики в этой сфере и укрепление координации между соответствующими структурами. Кроме того, вооруженные силы поддерживают регулярные контакты с рядом стран по вопросам информационной безопасности на политическом и рабочем уровнях.

Вооруженные силы Германии приветствуют международные инициативы по укреплению защиты полезных функций глобальных информационных сетей, в частности поддерживают разработку добровольного международного ко-

декса поведения в киберпространстве, и сотрудничают с другими ведомствами федерального правительства Германии в этой сфере.

Кибероборона в НАТО

НАТО считает угрозу кибербезопасности одной из ключевых новых проблем в сфере безопасности. В стратегической концепции, принятой главами государств и правительств на саммите НАТО, состоявшемся в ноябре 2010 года в Лиссабоне, указывается, что «кибератаки… могут достигать уровня, угрожающего национальному и евроатлантическому благополучию, безопасности и стабильности».

В июне 2011 года министры обороны стран НАТО, руководствуясь положениями декларации саммита, приняли политику и план действий НАТО в сфере кибероборонны. С этого момента НАТО осуществляет указанный план действий на постоянной основе.

В упомянутой политике основное внимание уделяется обеспечению защиты сетей НАТО и национальных сетей государств-членов, сопряженных с сетями НАТО или обрабатывающих информацию НАТО, необходимую для выполнения ее основных задач (включая разработку общих принципов и критериев для обеспечения минимального уровня кибероборонны во всех государствах-членах). Для снижения уровня глобальных угроз, проистекающих из киберпространства, НАТО намеревается сотрудничать с государствами-партнерами, соответствующими международными структурами, такими как Организация Объединенных Наций и Европейский союз, частный сектор и научные круги.

Германия с удовлетворением отмечает приверженность НАТО делу обеспечения кибербезопасности и активно поддерживает обсуждения по этому вопросу.

Исламская Республика Иран

[Подлинный текст на английском языке]
[7 июня 2013 года]

Исламская Республика Иран считает, что применение информационно-коммуникационных технологий и средств открывает многочисленные возможности для всех государств и человечества в целом. Сегодня информация и телекоммуникации являются важными элементами, на которых строятся современные общества. Они представляют собой важнейшие ресурсы обеспечения благосостояния и процветания стран. Иран считает, что на национальном и международном уровнях необходимо приложить все усилия для создания основ самого широкого применения информационно-коммуникационных технологий и средств во всех странах и обеспечения того, чтобы эти технологии и средства по-прежнему являлись важнейшей движущей силой развития во всех странах.

Вне всякого сомнения, достижение столь благородной цели в значительной мере зависит от обеспечения всестороннего уважения суверенных прав всех государств в сфере информации и телекоммуникаций, в том числе права на развитие, приобретение, применение, импорт и экспорт информационно-

коммуникационных технологий и средств и сопутствующих услуг, а также права на доступ к ним без каких бы то ни было ограничений или дискриминации. Обеспечение постоянной доступности, надежности, целостности и безопасности информации и создание безопасной и защищенной информационно-коммуникационной среды, безусловно, отвечает интересам всех стран и, следовательно, является задачей первостепенной важности. Неоспоримый факт заключается в том, что принятие любых мер для запрета или ограничения передачи передовых информационно-коммуникационных знаний, технологий и средств или оказания услуг в этой области развивающимся странам неблагоприятно повлияет на их общее развитие и, таким образом, является недопустимым.

В то же время информационно-коммуникационные технологии и средства могут применяться и для противоправных целей, в том числе для нанесения ущерба инфраструктурам и интересам государств в социальной, культурной, экономической и политической сферах и в сфере безопасности. Все большая зависимость стран от информационных потоков и телекоммуникационной инфраструктуры, с одной стороны, и применение информационно-коммуникационных технологий и средств для противоправных целей, в особенности преступниками и террористами, в том числе для целей государственного терроризма — с другой, являются свидетельством существующей уязвимости информации и телекоммуникаций и показывают, насколько широкомасштабные последствия может иметь любая связанная с ними потенциальная угроза. В соответствии с этим существенно важное значение имеет принятие всех надлежащих инфраструктурных, правовых и технических мер на национальном уровне для повышения уровня защиты информационно-коммуникационных технологий и средств во избежание их применения в противоправных целях.

Вместе с тем с учетом сложного характера и уникальных особенностей информационно-коммуникационных технологий и средств, в том числе безграничности виртуального пространства, его динамизма, анонимности, быстродействия и высоких темпов технического прогресса, а также все более широкой сопряженности существующих информационно-коммуникационных сетей, обеспечение безопасности информации и телекоммуникаций путем принятия только национальных мер представляется невозможным. По этой причине, а также вследствие увеличения числа случаев применения таких технологий и средств во многих странах для противоправных целей все государства должны принимать соответствующие меры на национальном уровне и участвовать в международном сотрудничестве.

Отмечая усилия, прилагаемые в Организации Объединенных Наций и других международных организациях для решения проблем, связанных с информацией и телекоммуникациями, Исламская Республика Иран считает, что наиболее целесообразным методом изучения на международном уровне изменений в сфере информации и телекоммуникаций в контексте международной безопасности является организация соответствующего процесса в Организации Объединенных Наций при равноправном участии всех государств. Иран твердо убежден в том, что главная цель такого процесса должна заключаться в выработке единого понимания государствами важности укрепления защиты информации и телекоммуникаций, характера, масштабов и остроты угроз для информационно-коммуникационных технологий и средств, а также в изыскании путей и средств предупреждения таких угроз. Такой процесс может завершиться

принятием программы действий, предусматривающей необходимые меры для принятия государствами-членами и проведение соответствующих международных конференций раз в пять лет с целью получения политических результатов, включающих от соответствующих деклараций до кодексов поведения. Вместе с тем конечная цель этого процесса должна заключаться в прогрессивном развитии прочных международно-правовых основ укрепления и обеспечения защиты глобальной информации и телекоммуникаций и недопущении применения информационно-телекоммуникационных технологий и средств для противоправных целей.

Исламская Республика Иран считает, что рассмотрение вопросов, связанных с достижениями в сфере информации и телекоммуникаций в контексте международной безопасности, должно осуществляться на базе следующих принципов и элементов:

a) применимость в качестве общего принципа международного права, которое, таким образом, должно распространяться на применение государствами информационно-коммуникационных технологий и средств. По этой причине государства в процессе применения таких технологий и средств должны соблюдать цели и принципы Организации Объединенных Наций и свои обязательства по ее Уставу, в частности пункту 3 статьи 2 о разрешении международных споров мирными средствами, пункту 4 статьи 2 о запрещении угрозы силой или ее применения любым образом, не совместимым с целями Объединенных Наций, а также пунктом 7 статьи 2 о запрещении вмешательства во внутренние дела государств;

b) ничто не ограничивает суверенных прав государств в сфере информации и телекоммуникаций, в том числе права на развитие, приобретение, применение, импорт и экспорт информационно-коммуникационных знаний, технологий и средств и всех сопутствующих услуг, а также права на доступ к ним без ограничений или дискриминации. В соответствии с этим государства строго воздерживаются от принятия любых мер для запрета или ограничения передачи передовых информационно-коммуникационных знаний, технологий и средств, а также оказания информационно-коммуникационных услуг развивающимся странам;

c) обеспечение защиты информации и телекоммуникаций на национальном уровне является исключительной ответственностью каждого государства. Вместе с тем с учетом глобального характера информации и телекоммуникаций государствам рекомендуется сотрудничать в деле предупреждения угроз, проистекающих из злонамеренного применения информационно-коммуникационных технологий и средств;

d) право на свободу выражения мнений не подлежит никаким ограничениям. В то же время это право ни при каких обстоятельствах не должно осуществляться в нарушение целей и принципов Организации Объединенных Наций, национального законодательства и принципов защиты национальной безопасности, правопорядка, общественного здравия, морали и приличий;

e) государства несут ответственность за совершение неоспоримо приписываемых им международно противоправных деяний с применением информационно-коммуникационных технологий и средств;

f) создание безопасной и защищенной информационно-коммуникационной среды в интересах всех стран должно являться главным руководящим принципом, в связи с чем государства должны при любых обстоятельствах воздерживаться от применения информационно-коммуникационных технологий и средств во враждебных, ограничительных или иных противоправных целях, в том числе для разработки и применения информационного оружия; подрыва или дестабилизации политических, экономических или социальных систем других государств или разрушения их культурных, моральных, этических или религиозных ценностей; трансграничного распространения информации в нарушение международного права, включая устав и положения Международного союза электросвязи или национальное законодательство затрагиваемых стран;

g) государства должны распространять информацию на национальном и международном уровнях о необходимости сохранения и укрепления охраны информации и телекоммуникаций путем ответственного применения соответствующих технологий и средств в целях выработки единой международной культуры в сфере охраны информации и телекоммуникаций.

Япония

[Подлинный текст на английском языке]
[12 августа 2013 года]

Общая ситуация в сфере информационной безопасности

Япония считает, что киберпространство обеспечивает базовую инфраструктуру для социально-экономической деятельности государственного и частного секторов. Киберпространство способствует экономическому росту, обеспечению занятости и развития, а также укреплению демократии и защите прав человека путем обеспечения свободы информационных потоков и свободы выражения мнений. Доступ к киберпространству имеет существенно важное значение для жизни людей во всем мире.

В то же время отмечается растущая необходимость защиты неприкосновенности личной жизни и прав интеллектуальной собственности, а также обеспечения безопасности киберпространства в целях использования всех благ, обеспечиваемых киберпространством. Кроме того, кибератаки происходят во всем мире и становятся транснациональной глобальной угрозой. Эти атаки могут совершаться различными структурами из всех районов мира и с применением различных методов. Страны по отдельности не в состоянии противостоять растущему числу киберпреступлений и кибератак, в связи с чем для решения этих проблем необходимо наладить взаимодействие в рамках международного сообщества, в том числе между соответствующими государствами и заинтересованными сторонами.

С учетом сказанного выше Япония выступает за создание защищенного и безопасного киберпространства путем уделения основного внимания обеспечению свободного потока информации и свободы выражения мнений при надлежащем учете необходимости обеспечения равновесия между охраной и неприкосновенностью личной жизни и сохранением безопасности.

Усилия на национальном уровне по укреплению информационной безопасности и международного сотрудничества в этой сфере

Усилия на национальном уровне по укреплению информационной безопасности

В последнее время обострились риски, связанные с киберпространством, а поддержание кибербезопасности стало важной задачей для обеспечения нашей национальной безопасности, управления кризисами, обеспечения социально-экономического процветания, а также безопасности и мира японского народа.

В этой связи в июне 2013 года Япония разработала стратегию кибербезопасности на период 2013–2015 годов. В рамках этой стратегии Япония будет принимать меры для укрепления информационной безопасности государственных учреждений и критических инфраструктур, а также для укрепления потенциала противодействия кибератакам.

В частности, Япония включила в эту стратегию следующие меры: содействие обмену в рамках партнерства между государственными и частными органами информацией о кибернападениях; совершенствование подготовки сотрудников по вопросам обеспечения безопасности не только для правительственных учреждений и промышленности, но и для всего японского народа; повышение осведомленности о кибербезопасности; укрепление потенциала по противодействию кибернападениям в рамках международного сотрудничества и расширение нашего вклада в разработку международных норм, касающихся кибербезопасности.

Усилия на национальном уровне по укреплению международного сотрудничества

Что касается разработки международных норм в сфере использования киберпространства, то мы должны безотлагательно приступить к разработке реалистичных и выполнимых норм поведения, не имеющих обязательного юридического характера, для решения существующих проблем в условиях быстрого развития кибертехнологий. Япония будет и далее активно участвовать в этих усилиях на международных форумах.

Если говорить о принятии мер укрепления доверия, то Япония активно участвует в двухсторонних консультациях с заинтересованными государствами и региональных диалогах, в том числе по линии Регионального форума АСЕАН, в целях «повышения транспарентности» и «содействия информационному обмену». Кроме того, в стремлении не допускать образования пробелов в кибербезопасности Япония оказывает помощь в подготовке кадров развивающимся странам в Азии, Океании и Африке, в частности в формировании и укреплении групп реагирования на связанные с компьютерами чрезвычайные ситуации. Помимо этого, Япония поддерживает международный обмен информацией путем укрепления координации с такими национальными группами других государств. Япония считает, что эти усилия являются вкладом в дело укрепления доверия между заинтересованными государствами.

Суть концепций, упомянутых в пункте 2 резолюции 67/27

Япония считает, что действующие международно-правовые нормы, включая Устав Организации Объединенных Наций и нормы международного гуманитарного права, применимы к киберпространству. Вместе с тем, учитывая уникальные особенности информационно-коммуникационных и сетевых технологий, необходимо продолжить обсуждение вопросов о применимости отдельных норм и принципов.

Учитывая ту важную роль, которую международное право играет в обеспечении правовой стабильности и предсказуемости в международном сообществе, мы считаем, что определение и разъяснение вопросов применимости действующих международно-правовых норм к киберпространству будет способствовать разработке конкретных международных норм в отношении киберпространства, а также способствовать обеспечению стабильности киберпространства.

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

Международные нормы, касающиеся использования киберпространства

В настоящее время не существует каких-либо международных норм по борьбе с кибератаками и кибершпионажем в сфере безопасности и социально-экономических сферах. Кроме того, на данном этапе не существует четкого понимания в вопросах применимости обязательных правовых норм в сфере киберпространства. В настоящее время трудно предвидеть общую картину развития киберпространства в будущем, поскольку кибертехнологии развиваются довольно быстрыми темпами. Кроме того, для выработки консенсуса в отношении юридически обязательных норм требуется весьма длительное время. В этой связи в том, что касается правового характера таких норм, Япония считает важным начать с обсуждения вопросов выработки необязательных общих норм поведения.

Меры укрепления доверия

Поскольку активизация усилий в сфере укрепления доверия между государствами может позитивно повлиять на развитие международных норм, международное сообщество должно и далее прилагать усилия в этом направлении. В сфере принятия мер укрепления доверия необходимо обеспечивать транспарентность и обмен информацией, однако уровень принимаемых мер в разных государствах является различным, поскольку каждое государство может решать этот вопрос самостоятельно. В этой связи необходимо способствовать обмену информацией по линии глобальных сетей, в частности сетей, находящихся под эгидой Организации Объединенных Наций, и региональных сетей.

Нидерланды

[Подлинный текст на английском языке]
[7 августа 2013 года]

Нидерланды тепло приветствуют возможность предоставить информацию о принятых ими мерах в связи с резолюцией 67/27.

Общая оценка проблем информационной безопасности

Нидерланды выступают за безопасные и надежные информационно-коммуникационные технологии и защиту открытого, свободного Интернета, основанного на соблюдении прав человека. Это является непременным условием нашего процветания и благополучия и служит катализатором устойчивого экономического роста.

Киберпространство не только открывает благоприятные возможности, но и делает наше общество более уязвимым. В силу трансграничного характера угроз огромное значение имеет международное сотрудничество. Многие меры будут эффективными только в том случае, если они будут приниматься или координироваться на международном уровне. В этой связи Нидерланды придают важное значение государственно-частным партнерствам, позволяющим наводить мосты при помощи мер повышения доверия и улучшать понимание индивидуальной ответственности всех пользователей информационно-коммуникационных технологий.

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

Нидерланды предпринимают усилия как на национальном уровне, так и на международном в интересах обеспечения безопасности цифровой среды. На национальном уровне Нидерланды осуществляют национальную стратегию кибербезопасности под названием «Сила через сотрудничество». Они пересмотрят эту стратегию в 2013 году и планируют опубликовать ее пересмотренную версию во второй половине 2013 года. Пересмотренная стратегия будет отражать более комплексный подход к кибербезопасности с учетом экономических возможностей, открытости, свобод и безопасности.

В Нидерландах существует Национальный совет по кибербезопасности, цель которого заключается в обеспечении взаимодействия между государственным и частным секторами, высшими учебными заведениями и научно-исследовательскими институтами и консультировании руководителей высшего звена по вопросам кибербезопасности. В стране создан также Национальный центр кибербезопасности для выявления тенденций и угроз и оказания содействия в деле урегулирования инцидентов и кризисных ситуаций. Перед Центром поставлена троякая задача: проводить анализ киберугроз на основе информации из государственных и частных источников; реагировать на киберугрозы и инциденты в части кибербезопасности; и осуществлять оперативную координацию в случае возникновения кризисных ситуаций в области информационно-коммуникационных технологий. В состав Центра входит существующая правительственная группа по реагированию на чрезвычайные ситуации в компьютерной сфере. За последний год Центр укрепил свой потенциал и установил прочные взаимоотношения с ключевыми информационными и аналитическими центрами. В ежегодной международной конференции, организуемой Национальным центром кибербезопасности, участвуют эксперты от правительств, из частных компаний и правоохранительных органов, а также технические эксперты, которые обмениваются передовым опытом в этой области. Нидерланды приняли ряд существенных мер, направленных на повышение ки-

бербезопасности, и готовы обменяться применяемыми ими моделями с третьими странами.

Примером государственно-частного партнерства в сфере ядерной безопасности служат технические совещания, организуемые правительством с участием представителей атомной отрасли, на которых оно может обозначать свои потребности в области информационной безопасности. Эта информация используется правительством для совершенствования «моделируемой угрозы». Ключевыми словами в данном случае являются «реалистичность» и «пропорциональность».

На международном уровне Нидерланды принимают активное участие в соответствующей деятельности Европейского союза, Организации Североатлантического договора (НАТО), Организации по безопасности и сотрудничеству в Европе (ОБСЕ), Форума по вопросам управления Интернетом и других партнерств. Нидерланды положительно восприняли совместное обращение Европейской комиссии и Высокого представителя Европейского союза по иностранным делам и политике безопасности, в котором содержится призыв к созданию открытого, свободного и безопасного киберпространства для Европейского союза и которое было одобрено Европейским советом. Европейский союз принимает меры по урегулированию этого вызова совместно со своими международными партнерами и организациями, частным сектором и гражданским обществом. Нидерланды полностью поддерживают цели Европейского союза по обеспечению безопасности Интернета при одновременном поощрении его открытости и свободы, содействию принятию мер и норм поведения, направленных на укрепление доверия, и применению существующих норм международного права в сфере киберпространства. Мы твердо убеждены в том, что безопасность и право доступа являются ключевыми элементами обеспечения непрерывного развития Интернета. В этих целях Европейский союз руководствуется такими основополагающими ценностями, как человеческое достоинство, свобода, демократия, равенство, верховенство права и уважение основных прав. Нидерланды поддерживают эти основополагающие ценности и считают их основой для любой стратегии кибербезопасности. Нидерланды согласны с тем, что для продвижения идеи здорового и жизнестойкого киберпространства и государственный, и частный сектора должны развивать свой потенциал и эффективно работать сообща.

На оперативном уровне Нидерланды содействуют практическому сотрудничеству между центрами кибербезопасности (включая организации по реагированию на чрезвычайные ситуации в компьютерной сфере) и укреплению Международной сети наблюдения и предупреждения. Стремительный рост киберпреступности диктует необходимость эффективного правоприменения в интересах сохранения веры в цифровое общество. Что касается правоприменения, то Нидерланды поощряют расширение практики трансграничных расследований совместно с правоохранительными органами других европейских и иных стран. Нидерланды являются стороной Конвенции Совета Европы о киберпреступности и призывают другие государства присоединиться к ней.

Что же касается информационной безопасности в ядерной области, то Нидерланды обмениваются с Европейской ассоциацией регулирующих органов в сфере ядерной безопасности информацией о стратегических подходах и передовым опытом в области ядерной безопасности, включая кибербезопасность.

Нидерланды активно участвуют в технических совещаниях Международного агентства по атомной энергии (МАГАТЭ), призванных обеспечить обмен сведениями по кибербезопасности и информационной безопасности.

Нидерланды считают, что свобода, транспарентность и безопасность неразрывно связаны между собой и взаимоусиливают друг друга. По этой причине Нидерланды явились инициатором создания Коалиции сетевой свободы, в которой на сегодняшний день участвует 21 правительство. Коалиция сетевой свободы привержена поощрению свободы Интернета и подчеркивает важное значение прав в цифровой сфере. В этих целях коалиция правительств-единомышленников координирует их усилия и работу с гражданским обществом и частным сектором в рамках многостороннего процесса поддержки способности людей осуществлять свои права человека и основные свободы в сети. В интересах достижения цели обеспечения открытости и свободы Интернета для всех члены коалиции образовали Партнерство защитников цифровых прав — фонд поддержки инновационных решений для защиты находящихся в опасности блогеров и сетевых активистов в странах, где Интернет не является свободным и доступным. Взнос Нидерландов в этот фонд на период с 1 октября 2012 года по 31 декабря 2014 года составляет 1 000 000 евро.

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

Отправным пунктом для Нидерландов является открытый Интернет, способствующий инновациям, стимулирующий экономический рост и защищающий основные свободы. Нидерланды особо отмечают важность постоянного диалога по формированию стандартов поведения государств, призванных обеспечить безопасное пользование киберпространством. Страна стремится вносить активный вклад в этот диалог. Нидерланды с удовлетворением отмечают важные усилия, которые предпринимают различные международные и региональные силы и заинтересованные стороны, такие как Совет Европы, Европейский союз, ОБСЕ и Группа правительственных экспертов Организации Объединенных Наций, в части мер укрепления доверия в сфере кибербезопасности.

В рамках процесса саммитов по ядерной безопасности информационная безопасность играет центральную роль. В Плане работы Вашингтонского саммита по физической ядерной безопасности и Сеульском коммюнике заявлено, что государства-участники саммитов по физической ядерной безопасности преследуют цель предотвращения «возможности получения неуполномоченными государством субъектами доступа к информации и технологиям, необходимым для использования такого материала в злоумышленных целях; и предотвращения нарушения работы систем управления ядерными установками, основанных на информационных технологиях». Как председатель саммита по ядерной безопасности Нидерланды поддерживают все усилия, способствующие достижению этой цели.

В рамках процесса саммитов по ядерной безопасности Нидерланды поддерживает инициативу Соединенного Королевства Великобритании и Северной Ирландии по практической реализации передового опыта в области информационной безопасности в ядерном секторе и обмена им. Это осуществляется посредством разработки и упрочения национальных мер, механизмов и потен-

циала в части эффективного управления такой информацией и обеспечения ее безопасности с целью укрепления соответствующей национальной культуры безопасности; вовлечения национальных научных, промышленных и академических кругов в работу по дальнейшему улучшению понимания, формированию и распространению передового опыта и повышения профессиональных стандартов; и поддержки на основе взаимодействия с МАГАТЭ, другими ключевыми международными организациями и странами-партнерами взаимных усилий по достижению этих целей. Нидерланды придают весьма важное значение всеохватывающей модели управления Интернетом с участием частного сектора, а также образовательных и научных учреждений в этом диалоге и стремятся обмениваться опытом и передовой практикой с другими сторонами.

Интенсивный международный обмен знаниями и информацией между всеми заинтересованными сторонами и организациями является непременным условием повышения безопасности и надежности киберпространства и полной реализации его потенциала с точки зрения и развития и сближения обществ во всем мире. В этой связи Нидерланды приветствуют конференции по кибертематике, состоявшиеся в Лондоне и Будапеште, и предстоящую конференцию в Сеуле.

И наконец, Нидерланды придерживаются того мнения, что для формирования норм поведения государств не требуется изобретать заново международное право, а следует обеспечить последовательность применения существующей международно-правовой базы. Мы призываем к дальнейшему диалогу и размышлению, с тем чтобы достичь консенсуса по практическим результатам применения существующих норм и международного права к киберпространству.

Оман

[Подлинный текст на арабском языке]
[26 июня 2013 года]

Министерство транспорта и коммуникаций хотело бы препроводить следующую информацию, касающуюся резолюции 67/27 Генеральной Ассамблеи о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности.

1. Общая оценка проблем информационной безопасности

Стремительное развитие информационных технологий и телекоммуникаций сопровождалось растущими рисками. Повсюду в мире хакеры используют все более продвинутые способы получения доступа к информации. Наиболее серьезные вызовы, с которыми сталкиваются государства и учреждения, связаны с отсутствием или недостаточным уровнем культуры информационной безопасности у пользователей информационно-коммуникационных технологий, недостатком квалифицированных кадров и различиями в законодательстве, регулирующем электронные коммуникации в мире. Государства должны объединить свои усилия и осуществлять сотрудничество в деле противодействия угрозам информационной безопасности, повышения своей готовности к принятию мер реагирования, улучшения глобального понимания этой проблемы и обмена соответствующей информацией и опытом.

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

- В 2002 году учрежден Орган по регулированию в сфере телекоммуникаций, а 2006 году создано Управление информационных технологий для регулирования секторов телекоммуникаций и информационных технологий.
- Введено в действие соответствующее законодательство: Закон «Об электронных транзакциях» (указом султана № 69/2008) и Закон «О регулировании в сфере телекоммуникаций» (указом султана № 30/2002).
- Международный союз электросвязи и Международное многостороннее партнерство против киберугроз (IMPACT) недавно создали в Омане первый центр кибербезопасности в Арабском регионе.
- В целях урегулирования рисков и угроз технического характера Управление информационных технологий сформировало в апреле 2010 года национальную группу по реагированию на чрезвычайные ситуации в компьютерной сфере.
- Действуя через Управление информационных технологий, Оман участвует в ряде соответствующих региональных и международных учреждений, включая группу по реагированию на чрезвычайные ситуации в компьютерной сфере Организации исламского сотрудничества, группу по реагированию на чрезвычайные ситуации в компьютерной сфере Совета сотрудничества стран Залива и Форум групп оперативного реагирования и обеспечения безопасности.
- Компетентные органы непрерывно обновляют свои стратегии.
- Государственные органы имеют доступ к ряду технологий и программ информационной безопасности.
- Создан центр для обеспечения защиты государственных сетей.
- Созданы службы хостинга, гарантирующие защиту веб-сайтов правительства.
- Оказывается техническая поддержка для укрепления информационной безопасности.
- Принят ряд нормативных документов и стандартов по информационной безопасности.
- По информационной безопасности организован ряд специальных учебных мероприятий.
- Проведены соответствующие информационно-просветительские кампании.
- Осуществлены программы по оценке готовности к реагированию на чрезвычайные ситуации в плане информационной безопасности.
- Проведен ряд соответствующих региональных и глобальных семинаров и конференций.

- На местном уровне проведены информационно-разъяснительные мероприятия.
- Все слои общества охвачены работой по укреплению информационной безопасности.
- В январе 2012 года запущена оманская национальная программа послов по линии реагирования на чрезвычайные ситуации в компьютерной сфере.
- Создан веб-сайт по укреплению сетевой безопасности детей (cop.cert.gov.om).
- Организованы информационно-пропагандистские выезды в школы, университеты, интернет-кафе и на другие объекты, часто посещаемые молодежью.
- Проведены семинары с целью повышения осведомленности учащихся/студентов и преподавательского состава.
- Центр играл активную роль в общественных мероприятиях, ориентированных на как можно большее число молодых людей, с целью информирования их о рисках в плане безопасности и мерах по их устранению.
- Центр занимался реализацией программ подготовки инструкторов, с тем чтобы молодые оманцы могли получить соответствующую квалификацию.
- Открылся первый на Ближнем Востоке оперативный центр информационной безопасности.

3. Содержание концепций

- Оман постоянно отслеживает и изучает такие международные концепции, с тем чтобы быть в курсе усилий по укреплению безопасности информации и систем связи на глобальном уровне.
- Необходимо учитывать специфику стран и их законодательство по электронным операциям.
- Заинтересованные стороны должны уважать конкретные ценности и принципы, за которые выступает каждая страна.

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

- Регулирование электронных операций и информации и межгосударственной кибербезопасности посредством создания международной организации под эгидой Организации Объединенных Наций, как было предложено на Конференции по киберзащите, состоявшейся в марте 2013 года в Омане.
- Поощрение сотрудничества между государствами в области защиты сектора информационно-коммуникационных технологий, от которого во многом зависит большинство стран в своих усилиях по содействию развитию. Такое сотрудничество должно осуществляться под эгидой международной организации.

- Обеспечение координации действий государств в области укрепления информационной безопасности и обмена передовым опытом.
- Сотрудничество в деле реагирования на инциденты в сфере информационной безопасности и назначение координаторов по каждой стране.
- Участие в формировании политики и нормативной базы и обмен передовым опытом.
- Обмен специальными знаниями и опытом, а также визитами.
- Проведение симпозиумов и семинаров для сотрудников по информационной безопасности.
- Организация совместных международных программ с целью повышения осведомленности населения и формирования культуры глобальной безопасности.
- Поощрение сотрудничества между академическими кругами и формулирование соответствующих программ и учебных планов.
- Поощрение и стимулирование совместных программ исследований и разработок в этой области.

Турция

[Подлинный текст на английском языке]
[10 июня 2013 года]

Общая оценка проблем информационной безопасности

В условиях мировой глобализации информационная безопасность стала необходимостью ввиду развития информационных технологий. Информационная безопасность и кибербезопасность — это область, которая должна регулироваться при сотрудничестве всех соответствующих сторон. В Турции решением правительства о проведении, регулировании и координации национальных исследований по кибербезопасности (опубликовано в «Официальной газете» № 28447 от 20 октября 2012 года) учрежден Совет по кибербезопасности как центральный механизм координации действий соответствующих сторон и проведения исследований в указанной области.

На первом заседании Национального совета по кибербезопасности 20 декабря 2012 года были утверждены национальные стратегия и план действий в области кибербезопасности на 2013–2014 годы.

Цели стратегии и плана действий заключаются в следующем:

- создание инфраструктуры, обеспечивающей возможность пользования услугами, процессами и данными, предоставляемыми при помощи информационных технологий государственными организациями;
- обеспечение безопасности информационных систем, используемых в важнейших типах инфраструктуры, которые находятся в ведении государства или частного сектора;

- определение стратегических действий в сфере кибербезопасности с целью сведения к минимуму последствий кибератак и сокращения времени, требующегося для восстановления после таких атак;
- формирование инфраструктуры, способствующей расследованию киберпреступлений органами юстиции и правоохранительными органами.

Основными направлениями плана действий являются следующие:

1. регулирование;

2. проведение исследований с целью содействия судебным процессам;

3. формирование национальной группы по реагированию на чрезвычайные ситуации в компьютерной сфере;

4. укрепление национальной инфраструктуры в области кибербезопасности;

5. учебная подготовка и повышение осведомленности людских ресурсов по вопросам кибербезопасности;

6. разработка национальных технологий кибербезопасности;

7. расширение сферы охвата национальных механизмов кибербезопасности.

План действий насчитывает 29 отдельных мероприятий, подлежащих выполнению в вышеуказанных основных областях.

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

Турецкий национальный орган регулирования — Управление информационно-коммуникационных технологий, учрежденное Законом «Об электронных коммуникациях» (№ 5809), — осуществляет ряд мероприятий в интересах содействия усилиям по обеспечению соблюдения национальных и международных требований в области информационной безопасности.

В этой связи деятельность Управления в области кибербезопасности состоит в следующем.

1. Регулирование и инспекции

Постановлением по безопасности электронных коммуникаций и инструкциями по его применению установлено несколько требований для авторизованных операторов. Соответствующие исследования призваны содействовать непосредственно обеспечению надлежащего уровня национальной кибербезопасности в деятельности операторов и косвенно укреплению международной кибербезопасности.

С другой стороны, имеются также нормативные документы Управления по электронной подписи и заказным электронным отправлениям, составленные в духе Закона «Об электронной подписи» (№ 5070) и национального Закона «О торговле» (№ 6112). Эти нормативные акты способствуют активизации уси-

лий, направленных на повышение безопасности и надежности документов и обмена сообщениями электронной почты.

2. Учения в области кибербезопасности

Управление информационно-коммуникационных технологий организует учения по кибербезопасности в интересах развития технического и административного ресурса, повышения осведомленности и создания возможностей для международного сотрудничества.

2.1. Национальные учения «Кибербезопасность-2011»

Национальные учения «Кибербезопасность-2011» проходили с 25 по 28 января 2011 года и охватывали 41 государственную, частную и неправительственную организацию из сферы финансов, ИКТ, образования, обороны и здравоохранения, а также судебные и правоохранительные органы и различные министерства. Шесть из них участвовали в учениях в качестве наблюдателей.

2.2. Учения «Киберщит-2012»

В учениях, которые проходили в мае 2012 года и координировались Управлением информационно-коммуникационных технологий, приняли участие 12 Интернет-провайдеров, функционирующих в секторе электронных коммуникаций. Среди участников были организации с крупнейшей долей на рынке в данном секторе, а также провайдеры мобильного Интернета третьего поколения (3G). В ходе учений отрабатывались распределенные атаки типа «отказ в обслуживании» и оценивалась адекватность мер безопасности, принимаемых с целью противодействия таким атакам.

2.3. Национальные учения «Кибербезопасность-2013»

Национальные учения «Кибербезопасность-2013», которые были организованы совместно Управлением информационно-коммуникационных технологий и Советом научно-технических исследований Турции под эгидой министерства транспорта, мореходства и коммуникаций, проходили с 24 декабря 2012 года по 11 января 2013 года с участием 61 государственной, частной и неправительственной организации. Несмотря на то, что большинство участников являлись государственными организациями, частные и неправительственные организации также участвовали в учениях. Кроме того, Председатель Международного союза электросвязи (МСЭ) — Международного многостороннего партнерства против киберугроз (IMPACT) и один из членов совета Форума групп оперативного реагирования и обеспечения безопасности (FIRST), которые служат платформами для международного сотрудничества в области кибербезопасности, участвовали в качестве выступающих в мероприятии, посвященном завершению учений.

3. Проект по предотвращению кибератак

Проект по предотвращению киберугроз (Siber Tehditleri Önleme Projesi — STOP) предполагает разработку необходимых механизмов создания в качестве приманки специальной незащищенной системы для выявления киберугроз, формирование и совершенствование системы извещения о кибератаках и подготовки метаданных о киберугрозах. Эта предусматриваемая проектом дея-

тельность осуществляется в сроки, установленные в краткосрочном национальном плане действий в области кибербезопасности. В рамках международного сотрудничества по проекту Управление информационно-коммуникационных технологий стало членом МСЭ-IMPACT, которое функционирует под эгидой МСЭ.

4. *Проект по предотвращению спама в электронной почте*

Данный проект осуществлялся в 2009 году и координировался Управлением информационно-коммуникационных технологий при содействии Интернет-провайдеров и организаций, предоставляющих услуги хостинга. Его цель заключалась в предотвращении спама в электронной почте, который может создавать угрозу сетевой безопасности и перегружать сетевые ресурсы. По завершении проекта число Интернет-провайдеров, способствовавших распространению спама, сократилось на 99 процентов, и это улучшение нашло отражение в отчетах мировых фирм, работающих в сфере кибербезопасности.

5. *Создание национальной точки обмена трафиком Интернета*

Обычная для Интернет-провайдеров практика ненужных межсетевых обменов между двумя оконечными точками из удаленной точки снижает качество обслуживания ввиду излишних задержек в передаче и усиления опасений по поводу безопасности.

С учетом этого благодаря обеспечению эффективной точки обмена трафиком Интернета и способности операторов обмениваться трафиком в более привлекательных условиях можно существенно сократить такую нежелательную практику маршрутизации и связанные с ней опасения по поводу безопасности. Поэтому Управление информационно-коммуникационных технологий осуществляет совместно с соответствующими сторонами (внутренними Интернет-провайдерами и международными поставщиками информации) целый ряд мероприятий, направленных на формирование эффективной национальной точки обмена трафиком Интернета.

Меры по укреплению информационной безопасности на глобальном уровне

Создание национальной группы по реагированию на чрезвычайные ситуации в компьютерной сфере

На данном этапе необходимо создать организацию по реагированию на киберинциденты, которая будет эффективно функционировать на национальном уровне в части обнаружения вновь возникающих киберугроз и принимать необходимые меры к сокращению или подавлению воздействия потенциальных киберинцидентов и обмену информацией. В этих целях в феврале 2013 года министерство транспорта, мореходства и коммуникаций поручило задачу по созданию и руководству работой национальной группы реагирования на чрезвычайные ситуации в компьютерной сфере на сектор коммуникаций, в связи с чем были инициированы различные мероприятия по формированию такой группы, которая функционировала бы круглосуточно на постоянной основе, противодействуя киберугрозам. Эта группа приступила к работе в мае 2013 года и будет осуществлять тесное взаимодействие с аналогичными структурами других стран и международных организаций.

В результате стремительного развития и распространения информационно-коммуникационных технологий угрозы информационной безопасности выходят за пределы национальных границ. В этой связи крайне важно, чтобы международные организации и правительства содействовали сотрудничеству в вопросах, связанных с информационной безопасностью, и осуществляли такое сотрудничество на практике в кратчайшие сроки.