УДК
ББК

Настоящее издание подготовлено
при поддержке Фонда содействия развитию интернета
«Фонд поддержки интернет» и не предназначено
для коммерческого использования

Ответственный редактор *М.Б. Касенова*
Составители *О.В. Демидов и М.Б. Касенова*

Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / Отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. – М.: Статут, 2013. – с.]

ISBN 978-5-8354-0000-0 (в пер.)

Документы и материалы, вошедшие в настоящее издание, представляют собой опыт систематизации нормативных правовых и политических документов, относящихся к такой сравнительно новой сфере регулирования, как управление интернетом и кибербезопасность.

Издание может представлять интерес для российских государственных органов, осуществляющих нормативно-правовое и политико-административное регулирование в сфере кибербезопасности и управления интернетом и участвующих в формировании позиции Российской Федерации на международной арене в этой сфере. Кроме того, документы и материалы настоящего издания могут быть полезными для российского экспертного и академического сообщества.

Материалы, вошедшие в настоящее издание, приведены по состоянию на 30 декабря 2013 г.

УДК
ББК

Издание подготовлено с использованием
справочной правовой системы «КонсультантПлюс».

При подготовке сборника использованы также документы и материалы, находящиеся в открытом доступе на официальных интернет-сайтах органов государственной власти Российской Федерации и международных организаций и форумов

ISBN 978-5-8354-0000-0

© М.Б. Касенова, О.В. Демидов, составление, предисловие, раздел I, 2013
© М.Б. Касенова, перевод на русский язык, 2013
© Издательство «Статут», оформление, 2013

ПРЕДИСЛОВИЕ

Интернет явился концентрированным отражением общих тенденций информационной революции конца XX – начала XXI в. Становится очевидным, что интернет интегрирует не только коммуникационные и технологические ресурсы, но и материальные, финансовые, интеллектуальные, гуманитарные, политические и прочие ресурсы, формирует и диверсифицирует процессы социальной регуляции. Логика регулирования собственно самого интернета и отношений, связанных с его использованием, в частности решение вопросов управления интернетом, его безопасного использования, объективно находится в плоскости как национального, так и международного права. Последние несколько лет и подходящий к концу 2013 г. стали периодом чрезвычайно быстрых и масштабных изменений в области информационно-коммуникационных технологий (ИКТ) и обусловленных ими трансформаций мировой политики.

Можно смело утверждать, что влияние интернета и компьютерных технологий перестало быть *феноменом* глобальных процессов и стало их *осью*, двигателем – столь же, если не более, определяющим и фундаментальным, чем экономический упадок Запада и *подъем остальных* государств, расцвет многополярности и *архаизация* ООН, глобальное старение населения, урбанизация развивающегося мира и коллапс расширенного типа семьи. Цифровые технологии стали кровеносной и нервной системой человеческих коммуникаций и взаимодействий и прямо на наших глазах стремительно превращаются в ее *глобальный мозг*. При этом любая сфера деятельности в масштабе индивида, группы или общества в целом неизбежно несет на себе отпечаток ИКТ, трансформируется за счет них и ими же опосредуется; международные отношения не являются исключением. Политические конфликты в киберпространстве, киберпреступность, цифровая дипломатия, онлайн-экономика и образование, электронное правительство – с этой реальностью приходится сталкиваться уже всем без исключения членам мирового сообщества, а не только технологически развитым странам, как всего десятилетие назад. Российская Федерация не является исключением и в большей или меньшей степени активно участвует в глобальных процессах, связанных с ИКТ и их использованием.

Российская Федерация является автором и главным сторонником концепции международной информационной безопасности (МИБ), которую продвигает на мировой арене вот уже полтора десятилетия с переменным успехом. 2011 г. внес существенные коррективы в эту политику; арабские революции были восприняты Россией и ее союзниками прежде всего как свидетельство целенаправленного использования интернета для подрыва социально-политической стабильности. Недопущение подобных событий впредь стало одной из новых ключевых задач России в сфере МИБ, что отразилось в проектах глобальных конвенций и других документов, которые были выдвинуты российской дипломатией на международной арене в 2011–2013 гг. Не менее активная дискуссия с российским участием ведется вокруг вопроса о том, кто же все-таки должен управлять интернетом – малопонятные и сложнопереводимые на русский язык, но эффективные стейкхолдеры (*stakeholders*), Корпорация интернета по распределению имен и адресов (*Internet Corporation for Assigned Names and Numbers*, *ICANN*), Международный союз электросвязи (МСЭ), Китай, Иран и другие государства?

Особенность сегодняшнего момента состоит в том, что вопросы в сфере ИКТ как составляющей глобальных процессов возникают быстрее, чем формулируются внятные ответы на них, а тем более их правовое регулирование. Особенно ярко это ощущается в сфере безопасности – если электронное правительство можно отложить на несколько лет (уже по *старой* российской привычке), то трансграничные киберугрозы не оставляют такого временного лага. Этот урок хорошо усвоил Иран, столкнувшись со *Stuxnet*. Вопросы и вызовы, связанные с трансформацией международной безопасности под влиянием ИКТ, множатся буквально ежечасно. К примеру, Эстония, пострадав от атак в разгар кризиса с *Бронзовым солдатом* в 2008 г., призывает НАТО прибегнуть к ст. 6 Североатлантического договора и отреагировать на якобы «российскую агрессию» в формате совместной обороны. НАТО не решается на конфликт с РФ, но зерна размышления о том, когда кибератака переходит грань агрессии и может быть приравнена к вооруженному нападению, посеяны. И пять лет спустя из них вырастает Таллиннское руководство Центра совместной обороны НАТО (*CCD COE)* – противоречивый, но чрезвычайно важный документ, авторы которого пытаются очертить «правила ведения кибервойны». В России этот документ, увы, пока недооценен, хотя реальность подталкивает и нас, и наших партнеров к обсуждению тех же самых вопросов – где заканчивается мир и начинается война в Сети и как международное право, включая *jus in bello* и *jus ad bellum,* должно к ней применяться.

Любопытно, что российская дипломатия сегодня приходит к обсуждению тех же самых вопросов в формате Группы правительственных экспертов (ГПЭ) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности ООН.

Несомненный контекст дня сегодняшнего – интернет после разоблачений Сноудена. Сейчас, из ноября 2013 г., кажется, что Сноудена следовало изобрести, если бы он не появился сам. Для многих субъектов и процессов его действия стали катализатором для перемен, а то и *casus belli* для объявления войны сложившимся порядкам. Президент *ICANN* Фади Шехаде, представитель нового поколения глобального интернет-сообщества, использовал разоблачения Эдварда Сноудена как предлог объявить о том, что Корпорации интернета пора покинуть американскую гавань и уйти в свободное плавание под флагом международной организации. Куда выведет капитан Шехаде свой корабль, пока неизвестно, и особенно интересна в этом смысле позиция России: если *ICANN* больше не проводник американских интересов, как менять стратегию взаимодействия с ней? Участвовать, дружить или по-прежнему пытаться перекроить систему глобального управления интернетом под принятие решений исключительно на площадках межправительственных организаций? А ведь помимо официальной позиции России есть интересы частного сектора и интернет-сообщества, которые также немало озадачены происходящим. И впереди – Полномочная конференция МСЭ 2014 г. в корейском Пусане, ожидаемый *второй раунд* борьбы за наделение МСЭ контролем над управлением интернетом после ВКМЭ 2012 г. в Дубае.

Выше обозначены лишь некоторые вопросы и проблемы из числа тех, что занимают умы дипломатов, политиков, экспертов в области ИКТ. Регулирование отношений, связанных с интернетом, его управлением, безопасностью интернета, отражается в различного рода законодательных актах, неформальных инициативах, национальных и международных, правительственных и общественных, мультистейкхолдерских и частных проектах и актах в сфере информационной безопасности, кибербезопасности и управления интернетом.

Настоящее издание обобщает и систематизирует основные материалы и документы, разработанные за последние годы на международно-правовом и национальном уровне различными заинтересованными сторонами (*stakeholders*), а именно техническим сообществом, гражданским обществом, государствами, международными организациями. Безусловно, представленные материалы и документы не являются исчерпывающими, однозначно репрезентативными по своему охвату

в части проблематики управления интернетом и информационной безопасности – подобные задачи в принципе не могут решаться в рамках одного издания. Вместе с тем авторы-составители попытались в рамках настоящего издания обозначить приоритетные области регулирования и систематизацией документов и материалов дать целостное представление о существующей и формирующейся источниковедческой, нормативно-правовой базе управления интернетом и решения вопросов его безопасного использования, показать читателю в структурированном виде все существующее *многообразие* подходов, субъектного состава и уровней принятия решений в обозначенных сферах.

В настоящем издании приведены, на наш взгляд, материалы самого различного статуса и уровня. Некоторые из них, такие как национальные стратегии кибербезопасности ЕС, Финляндии, Национальная политика кибербезопасности Индии, впервые переведены на русский язык, чтобы быть более доступными для российских экспертов, лиц, принимающих решения, и иных стейкхолдеров. Другие, такие как двустороннее российско-бразильское соглашение о сотрудничестве в сфере обеспечения МИБ от 2010 г., интересны тем, что выпали – незаслуженно, как представляется, – из фокуса экспертного внимания и почти не освещаются. Наконец, в сборнике присутствуют попросту наиболее значимые и ключевые для российской и международной динамики в сфере информационной безопасности документы, такие как Основы государственной политики РФ в области МИБ на период до 2020 г., а также документы ООН.

Одна из основных целей настоящего издания – дать лицам, принимающим решения в России по вопросам информационной безопасности и управления интернетом, систематизированную и концентрированную подборку материалов, обобщающую ключевые тенденции в обозначенных сферах за последние годы и предоставляющую им экспертную базу и ориентиры в части подходов, лучших практик и приоритетных вопросов для принятия дальнейших решений. Во многом эта цель включает в себя доведение до российских представителей профильных государственных органов эффективных зарубежных и международных примеров регулирования в области ИКТ, которые могут ускользать от их внимания, недооцениваться и игнорироваться. Еще одно назначение настоящего издания – стимулирование интереса к проблематике ИКТ в политико-правовой плоскости и развитие дискуссии в российском сообществе технических и академических экспертов. Нельзя сказать, что проблемы глобального управления интернетом и кибербезопасности получили в России полное отраже-

ние в работах экспертов, а подготовка специалистов в этой области заложена в сегодняшнюю систему российского высшего образования. Вместе с тем объективная потребность в этом существует, и мы надеемся, что настоящее издание будет в той или иной мере способствовать ее удовлетворению, стимулировать рост интереса к данной проблематике.

В общем плане развитие информационных и коммуникационных технологий опережает их правовое регулирование и не исключено, что выявятся новые аспекты их развития, которые потребуют своего регулирования на национальном и на международно-правовом уровне, тем не менее любые возникающие вопросы так или иначе будут связаны с проблематикой трансграничного управления интернетом, его безопасного использования и принятия мер против противоправного использования интернета.

***

Настоящее издание подготовлено при поддержке Фонда содействия развитию интернета «Фонд поддержки интернет».

РАЗДЕЛ I
КИБЕРБЕЗОПАСНОСТЬ И УПРАВЛЕНИЕ ИНТЕРНЕТОМ

Мадина Касенова,
заведующая кафедрой
международного частного права
Дипломатической академии МИД России,
к.ю.н., профессор

Основы трансграничного управления интернетом

1. Общие вопросы и основные понятия

История знает целый ряд открытий и изобретений, которые коренным образом изменили существование человека, например бумага, порох, телеграф, радио, телевидение. К числу величайших изобретений прошлого столетия, несомненно, относится интернет. Интернет первоначально был предназначен для военных целей, и исторически одной из основных причин его возникновения стало военное противостояние 60-х годов XX в. и угроза нанесения ракетно-ядерного удара. Правительство США инициировало научно-исследовательский проект Пентагона в целях создания системы управления стратегическими ядерными силами. Была поставлена задача создания системы управления, способной сохранять устойчивость и функционировать даже при нанесении ракетно-ядерного удара и уничтожении части компонентов такой системы. Интернет создавался и развивался как технологическая система информационного обмена между лицами, передающими и получающими информацию, по произвольным маршрутам через узловые соединения. При этом базовая технологическая архитектура интернета изначально зиждилась на саморегулировании, децентрализованной «сетевой» организационной модели, не предполагающей иерархии управления и идентификации лиц, получающих и передающих информацию, включая определение статуса таких лиц.

За более чем 45-летнюю историю своего развития интернет превратился в глобальную коммерческую инфраструктуру трансграничного информационного обмена, но базовые технологические особенности интернета остались неизменными и лишь модифицировались для удобства пользования интенсивно расширяющимся числом пользователей. Несомненно, что именно базовая технологическая структура интернета стала ключевым фактором развития и распространения интернета во всем мире.

В 1985 г. в мире насчитывалось приблизительно 20 тыс. интернет-пользователей, жители США составляли 90%. Через 20 лет, в 2005 г., число пользователей интернета по всему миру приблизилось к 1,1 млрд, среди них – более 200 млн американцев (около 17 %)[1]. По данным на середину 2013 г. 2,26 млрд человек в мире имеют доступ к интернету с различной степенью охвата населения всемирной паутиной в государствах. Например, в Исландии интернетом пользуется 95% населения, в Германии – 83%, в США – 77,9, в России – 49, в Китае – 38,3%. Несколько иная картина в государствах бывшего СССР. Так, в Эстонии, Латвии и Литве 76,5, 71,7 и 65,1% населения соответственно имеют доступ к интернету; в Азербайджане интернетом охвачены 50% населения, в Казахстане – 45, в Беларуси – 39,6, в Молдове – 38, в Грузии – 36,6, в Украине – 30,6, в Узбекистане – 30,2, в Киргизии – 20, в Таджикистане – 13, в Туркменистане – 5%.

Распространению интернета способствует то, что он «становится многоязычным». При этом доля англоязычных пользователей интернета падает, к примеру, если в 90-е годы XX в. она составляла 80%, то к 2013 г. – 27%. Значительно растет доля пользователей, использующих китайский, испанский, немецкий, арабский, французский языки. Русский язык входит в первую десятку наиболее используемых в интернете языков[2]. В настоящее время в мире насчитывается свыше 4 млрд цифровых телекоммуникационных устройств, к которым подключено более 1,7 млрд пользователей.

Вопросы регулирования информационных и коммуникационных технологий приобретают актуальность не только в связи с тем, что их использование стало концентрированным отражением происходящей глобализации. Феноменальный успех интернета приводит к «интерне-

[1] См. данные издания «eTForescasts» – «Прогноз в отношении числа интернет-пользователей по странам» (*eTForecasts, Internet User Forecast by Country*) (URL: http://www.etforecasts.com/products/ES_intusersv2.htm), а также: Internet World Stats. Usage and population statistics // URL: http://www.internetworldstats.org; Интернет в цифрах. 2013. № 2 (14). С. 4–13.

[2] Интернет в цифрах. 2013. № 3 (15). С. 4–6.

тизации» значительного числа государств, что, с одной стороны, расширяет и изменяет географию и аудиторию интернет-пользователей, а с другой – ввергает государства в своеобразную «технологическую гонку вооружений». Развитие информационных и коммуникационных технологий передачи и обработки информации влияет даже на лексический состав и орфографические правила многих языков мира. Стали появляться и все чаще использоваться слова-неологизмы с приставкой «кибер-» (англ. *cyber-*): киберпространство, кибербезопасность, киберпреступность, кибертерроризм, кибератака, кибервойска, кибероружие, киберсотрудничество и т.д. Эти слова используются в различных нормативных актах внутригосударственного законодательства, политических декларациях, документах международных организаций и иных документах правового характера. Терминологическое значение и содержание этих понятий формируется и пока однозначно не определено, поэтому они получают различную интерпретацию и применение в документах международных межправительственных организаций, в первую очередь ООН, Международного союза электросвязи (МСЭ), а также в национальных «стратегиях киберпространства» (например, США) или «стратегиях кибербезопасности» (например, Финляндии, Индии, Европейского Союза[1] и др.). Так, в документах Международного союза электросвязи под *киберпространством* (*cyberspace*), понимается «среда с подключенными компьютерными устройствами, пользователями, инфраструктурой, приложениями, сервисами, телекоммуникационными системами, а также совокупность передаваемой и (или) хранящейся в этой среде информации». Вместе с тем во внутригосударственном праве многих стран термин «киберпространство» используется в ином содержательном значении.

На повестку дня все настоятельнее выдвигается вопрос о единообразии применяемых терминов и понятий, правовой квалификации используемых понятий, а также адекватности переводов этих понятий на другие языки, включая русский. Смысловые, содержательные различия употребления тех или иных терминов зависят и от вариантов перевода терминов и понятий. Например, слово *cybersecurity* с английского языка буквально переводится как «*кибербезопасность*», но в силу определенной политической мотивации может переводиться на русский язык как «информационная безопасность» или даже «безопасность применения информационных технологий». Примечательно, что в ряде документов Генеральной Ассамблеи ООН

[1] См. раздел II настоящего издания.

(русскоязычная версия) стал использоваться термин «информационная безопасность»[1].

Применительно к терминам более общего характера также можно заметить различия в написании и применении слов, словосочетаний и аббревиатур, используемых правовыми системами и законодательными актами разных государств. В документах международных организаций, в частности Организации Объединенных Наций, используется словосочетание *Information and Telecommunication Technologies*, которое на русский язык переводится по-разному: «информационно-коммуникационные технологии», «информационные и коммуникационные технологии». Употребление в этом словосочетании дефиса либо использование союза «и», несомненно, меняет смысловые характеристики и контекст их применения. Так, использование дефиса в русском переводе термина «информационно-коммуникационные технологии» дает возможность отнести международно-правовое регулирование телекоммуникаций к сфере деятельности Международного союза электросвязи и выделять при этом информационные технологии как отдельную сферу международно-правового регулирования, в значительной степени совпадающую со сферой «трансграничного управления» интернетом.

В правовой системе США, относящейся к англо-американской правовой семье, в которой судебный прецедент имеет регулирующее значение, принципиальным стало то, что Верховный суд США в 2005 г. вынес решение о различии классификаций «информационные услуги» и «телекоммуникации», что повлияло на различия в их правовом регулировании и использовании в правоприменительной практике США. Обсуждение вопроса о квалификации названных категорий происходит в драматичном ключе и в настоящее время активно продолжается.

Сама орфографическая норма написания слова «интернет» отражает эволюцию его применения и изменение его значения. В российском законодательстве слово «интернет» употребляется в различном контексте и сочетаниях, но предпочтение отдается использованию его эвфемизма – «информационно-коммуникационная сеть», который пишется через дефис. Интересно, что в настоящее время при написании слова «интернет» все чаще используется строчная буква, что знаменует переход этого понятия из категории имен собственных, как обозначения названия некой международной компьютерной сети, в категорию имен нарицательных, как обозначения инфраструктуры,

[1] Резолюция Генеральной Ассамблеи ООН A/C.1/68/L.37.

обеспечивающей определенную технологию обмена информацией. Это является свидетельством того факта, что интернет стал частью повседневной жизни и перестал быть чем-то уникальным, «разделив участь» таких изобретений, как телеграф, телефон, радио, телевидение, написание которых тоже когда-то было с прописной буквы. Тем самым окончательно ликвидируется возможность отношения к этой международной информационной сети как к некоему объекту регулирования, который: а) кому-то принадлежит; б) носит в этой связи присвоенное фактическим или формальным владельцем имя или название; в) сосуществует с некими иными объектами, сходными с ним по принципам функционирования и принципам развития[1].

Ключевым в дискуссиях относительно правового регулирования информационных и коммуникационных технологий являлся – и до сих пор остается таковым – вопрос об управлении интернетом. Эта проблема в настоящее время не только не имеет однозначного решения, но и сами теоретические (доктринальные) подходы к ее разрешению весьма разнообразны. Во многом это объясняется тем, что интернет – это инфраструктурно сложная технологически многоуровневая информационная сеть, функционирование которой осуществляется в трансграничном масштабе. Технологически «инфраструктурные уровни» интернета объединяют: физические каналы связи и компьютерное оборудование; программные и технические средства, обеспечивающие связность различных сегментов информационной сети в разных странах, через систему корневых серверов (*root servers*), маршрутизирующих основные информационные потоки интернета; технические стандарты и способы их практической реализации, относящиеся к системе сетевой адресации; собственно сами интернет-ресурсы в виде веб-сайтов, социальных сетей, служб электронной почты, систем поиска информации и т.д. Интернет, таким образом, – «техническое изобретение» и, как таковое, объективно требует технической поддержки и технологического обеспечения функционирования его инфраструктуры. Для обеспечения трансграничного функционирования интернета в этом контексте наряду с правовыми нормами специальное регулирующее значение имеют «организационно-технические» нормы, такие как стандарты и протоколы интернета (*Internet Protocol Standards*), создаваемые, например, организациями, входящими в Общество интернета (*Internet Society, ISOC*), Консор-

[1] См. об этом: *Якушев М.В.* Интернет 2012 и международная политика // Индекс безопасности. 2013. № 1 (104). С. 29–42.

циумом Всемирной сети (*World Wide Web Consortium, 3WC*) и другими организациями.

Вместе с тем интернет следует рассматривать не только как «техническое изобретение», поскольку его использование влияет на внутригосударственное экономическое и социальное развитие государств, обеспечивает коммуникационные связи государств, организаций, людей в международном масштабе; безопасное использование интернета все чаще принимается в международно-правовом сотрудничестве государств и т.д. В этом контексте на доктринальном и правоприменительном уровне обсуждается необходимость концептуального разграничения собственно *интернета*, рассматриваемого в качестве технического изобретения, которое главным образом связано со сферой телекоммуникаций, и *доступа к интернету* – использование технологических возможностей интернета для получения информации, т.е. использование интернета, рассматриваемое как «информационная услуга». Такое концептуальное разграничение позволяет понять суть управления интернетом и обозначить, с одной стороны, управление многоуровневым процессом технической координации базовых компонентов технологической инфраструктуры Интернета (архитектурные принципы интернета, *IP*-адреса, система доменных имен, разработка стандартов и протоколов интернета, корневые серверы), т.е. технологические компоненты, без технического обеспечения и координации функционирования которых трансграничное управление интернетом невозможно; с другой стороны – определить иные измерения или ипостаси управления интернетом: политические, социальные, экономические, правовые и проч.

Термин *управление интернетом* в его традиционном в настоящее время понимании появился в начале 2000-х годов, явившись достаточно условным переводом английского эквивалента *Internet Governance*. Действительно, слову *governance*, подобно многим другим отвлеченным понятиям, выраженным по-английски, нелегко подобрать однозначные соответствия в большинстве других языков мира. В доктрине и в практике используются разнообразные переводы понятия *Internet Governance* на русский язык, в том числе «регулирование интернета», «управление использованием интернета» и т.д. Представляется, что из всего многообразия предложенных терминов именно «управление Интернетом» наиболее адекватен, хотя и не вполне отражает суть описываемого явления, фактически сводящегося к установлению и соблюдению правил и процедур, регламентирующих порядок функционирования и развития глобальной информационной сети.

Обсуждение проблематики управления интернетом началось в 2000-х годах и происходило в контексте двух подходов. Узкий подход, *strictu sensu,* ограничивал управление интернетом технико-организационными вопросами построения сети, сетевой адресации и нумерации, стандартизации, и т.д. «Широкий» подход, *sensu lato*, подразумевал необходимость включения в управление интернетом наряду с техническими также социальных, экономических, политических, правовых и проч. вопросов и содержательно в понятие «управление интернетом» включались проблемы коммутации международных сетей электросвязи, обеспечение «сбалансированности» тарифов за пропуск сетевого трафика и т.д. Проблематика управления интернетом при широком подходе фактически совпадала с проблематикой «построения информационного общества», впервые обозначенной на международном уровне в Окинавской хартии глобального информационного общества группы стран «Большой восьмерки» 2000 г.[1]

Представляется целесообразным использовать «широкий подход» управления интернетом и включать в проблематику управления интернетом организационно-технические, технологические, общественно-политические, социально-экономические и проч. аспекты. Широкий подход получил закрепление в целом ряде документов международных организаций и форумов, связанных с управлением интернетом, и позволил разграничить сферы сотрудничества и взаимодействия, а именно сферу, относящуюся к «повседневной деятельности технического и эксплуатационного характера», и сферу, связанную с «деятельностью правительств и их ролью в выполнении своих обязательств в решении международных вопросов государственной политики, касающихся интернета». Сошлемся в качестве примера на резолюцию Экономического и социального совета ООН (ЭКОСОС) от 26 июля 2011 г. 2011/16. Резолюция (п. 22, 24) разделяет вопросы, связанные с интернетом, на вопросы, относящиеся к «повседневной деятельности технического и эксплуатационного характера», и вопросы, связанные с «деятельностью правительств и их ролью в выполнении своих обязательств в решении международных вопросов государственной политики, касающихся интернета»[2].

Управление интернетом в сфере «повседневной деятельности технического и эксплуатационного характера» в целом сформировалось и в самом общем плане представляет собой исторически сложившуюся

[1] См. об этом: *Касенова М.Б., Якушев М.В.* Управление интернетом: Документы и материалы. СПб., 2013. С. 323–329

[2] См. E/2011/INF/2

«многостороннюю» модель (*Multistakeholder Model*), основанную на саморегулировании и многостороннем партнерстве, включающем все заинтересованные стороны[1], а именно частный сектор, гражданское общество, бизнес, техническое и академическое сообщество, правительства, международные организации. Такая многосторонняя модель оказалась эффективной для обеспечения стабильности, безопасности и доступности трансграничной инфраструктуры интернета, явилась ключевым фактором захватывающего революционного развития и глобального распространения интернета. Несомненно, организационно-техническое функционирование интернета будет развиваться, совершенствоваться и дальше.

Сфера управления интернетом, «связанная с деятельностью правительств и их ролью в выполнении своих обязательств в решении международных вопросов государственной политики, касающихся интернета», прежде всего связана с государствами как субъектами международного права. В этой связи целесообразно отметить следующее. Во-первых, специфика организационно-технического функционирования интернета заключается в том, что интернет никому не принадлежит, ни одно государство не обладает монопольной властью над ним и интернет никто не может «выключить». Вместе с тем технологические компоненты интернета подпадают под многочисленные национальные и государственные юрисдикции, в рамках которых могут быть установлены те или иные ограничения на передачу информации, что является суверенным правом государств. Во-вторых, именно государствам принадлежит ведущая роль *и* в решении вопросов, связанных с политикой в сфере интернета, *и* в формировании международно-правовой модели управления интернетом. В-третьих, в более чем 45-летней истории развития интернета решение проблем, связанных с государственной политикой в сфере интернета, насчитывает немногим более десятилетия и на формирование международно-правовой модели управления интернетом влияет сложившаяся многосторонняя модель управления интернетом, которая предусматривает взаимодействие всех заинтересованных сторон: правительств, международных организаций, гражданского общества, частного сектора, технического и академического сообщества. Именно многосторонняя модель дает суверенным государствам возможность регулировать использование интернета в пределах своей юрисдикции.

[1] Английское слово *multistakeholders* переводится как «заинтересованные стороны». В доктрине используются термины, которые являются «калькой» этого слова: «мультистейкхолдеризм», «мультистейкхолдерская модель» и т.д.

2. Всемирная встреча на высшем уровне по вопросам информационного общества и управление интернетом

Проблематика управления интернетом и вопрос формирования международно-правовой модели управления интернетом исторически тесно связаны с процессом проведения Всемирной встречи на высшем уровне по вопросам информационного общества и последующих шагов в реализации принятых решений[1]. Всемирная встреча на высшем уровне по вопросам информационного общества (*World Summit on the Information Society, WSIS*; далее – Всемирная встреча *WSIS*) проходила под эгидой Организации Объединенных Наций (первый этап – Женева, декабрь 2003 г.; второй этап – Тунис, 2005 г.). Одним из важных итогов первого этапа Всемирной встречи *WSIS* было учреждение Рабочей группы по управлению интернетом (*Working Group on Internet Governance*; далее –Рабочая группа *WGIG*)[2].

Рабочая группа *WGIG* с учетом всестороннего обсуждения выработала определение понятия «управление интернетом»: *управление интернетом представляет собой разработку и применение правительствами, частным сектором и гражданским обществом, при выполнении ими своей соответствующей роли, общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение интернета.* Это определение не является исчерпывающим, вызывало и вызывает ряд критических замечаний, но в настоящее время считается общепризнанным и «рабочим». Важно обратить внимание на то, что разработанное рабочее определение зиждется на концепции участия всех заинтересованных сторон (*Stakeholders*) в управлении интернетом.

Определение управления интернетом исходит из признания того, что в конкретных вопросах управления интернетом каждая заинтересованная сторона имеет свои различные интересы, играет различную роль и принимает участие в различных формах, которые зачастую могут дублировать друг друга.

К числу заинтересованных сторон – участников управления интернетом относятся правительства, частный сектор и гражданское общество. (В последнее время к их числу относят международные межправительственные организации, образовательные и научные ор-

[1] Документ ООН: A/RES/59/220. Декларация принципов и План действий ВСИС — WSIS-03/Geneva/DOC/0004 // URL: http://www.itu.int/wsis/

[2] Рабочая группа *WGIG* рассматривала как тождественные понятия «управление интернетом» и «управление использования интернета» (см. об этом подробнее: URL: http://www.itu.int/wsis/basic/about.html).

ганизации, экспертные сообщества так называемого «некоммерческого сектора».) В управлении интернетом заинтересованные стороны (*Stakeholders*) выполняют свои «соответствующие роли»[1].

Так, роль и обязанности правительств связаны с такими аспектами деятельности, как разработка, координация и осуществление государственной политики на национальном уровне, координация политики на региональном и международном уровнях; создание благоприятных условий для развития информационных и коммуникационных технологий (ИКТ); надзорные функции; разработка и принятие законов, положений и стандартов; разработка международных договоров и правил; развитие передового опыта; содействие созданию потенциала в сфере ИКТ и с их помощью; борьба с киберпреступностью; содействие международному и региональному сотрудничеству; решение общих вопросов развития; поощрение многоязычия и культурного разнообразия и др.

В сферу ответственности частного сектора относятся вопросы саморегулирования информационной индустрии; развития передового опыта; разработки стратегических предложений, руководящих принципов и инструментария для директивных органов и других заинтересованных сторон; научных исследований и опытно-конструкторских разработок в области технологий, стандартов и процессов; участия в разработке национального законодательства и национальной и международной политики; содействия инновационной деятельности и др.

Роль и функции гражданского общества включают расширение информированности общественности и создание потенциала (знания, подготовка кадров, обмен опытом); предоставление экспертов, специалистов, обмен опытом и знаниями по вопросам политики в области ИКТ; научные исследования и опытно-конструкторские разработки в области технологий и стандартов; содействие в обеспечении соответствия политических и рыночных факторов потребностям всех членов общества; содействие формированию концепций информационного общества, ориентированного на человека, и др.

Рабочая группа *WGIG* сформулировала важнейшие проблемы, требующие закрепления и решения на международном уровне, а именно:

– административное управление корневой зоной интернета и корневыми серверами системы доменных имен (*DNS*)[2];

[1] См. подробнее: Декларация принципов *WSIS*, п. 49 (WSIS-03/GENEVA/DOC/0004).

[2] Доменное имя – это символьное обозначение, зарегистрированное для сетевой адресации, в которой используется система доменных имен (*Domain Name System, DNS*). Система доменных имен *DNS* предназначена для удобства пользователей интернета

– порядок присвоения сетевых *IP*-адресов и распределения адресного пространства в условиях перехода на новый сетевой протокол *IPv*6;

– уточнение порядка присоединения информационных и телекоммуникационных сетей на международном уровне и их взаимодействие;

– стабильность и безопасность глобальной сети и ее пользователей;

– предотвращение противоправного распространения информации в интернете, включая спам;

– обеспечение основных прав и свобод человека при использовании интернета, включая в первую очередь свободу слова и выражения своего мнения;

– обеспечение конструктивного участия каждого желающего в разработке государственной политики управления интернетом;

– защита информации и права на неприкосновенность частной жизни;

– соблюдение прав потребителей при оказании сетевых услуг;

– расширение практики многоязычия и политики мультикультурализма.

Принципиальным моментом являлось не только то, что итоговый доклад Рабочей группы *WGIG* исходил из признания многосторонней модели (*Multistakeholder's Model*) управления интернетом, но и то, что были предложены *четыре* возможные организационные модели управления интернетом. Следует подчеркнуть, что принципиальным моментом для всех четырех моделей управления интернетом являлось то, что все предложенные модели предусматривали осуществление функций Корпорации интернета по распределению имен и адресов (*Internet Corporation for Assigned Names and Numbers*, *ICANN*). Соответственно, логика изложения требует обозначить в общем плане роль и значение *ICANN* в трансграничном управлении интернетом[1].

Трансграничное функционирование интернета основано на саморегулировании, но требует «централизованного» осуществления как минимум трех функций: во-первых, разработки принципов распределения (выделения) блоков интернет-адресного пространства (*Internet Protocol Address)*; во-вторых, эксплуатации корневых серверов (*Operating Root Servers*), позволяющих подключенным к интернету устройствам находить друг друга, а пакетам данных перемещаться

и обеспечивает соответствие между сетевыми адресами, *IP*-адресами. В сети Интернет требуется глобальная уникальность адреса. *IP*-адрес (*Internet Protocol Address, IP-Address*) – уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу *IP* (см. подробнее об этом: URL: http://cctld.ru/ru/docs/legals/domainsite.php/).

[1] См. подробнее об *ICANN:* http://www.icann.org/

от отправителя к получателю по всей Сети, включая осуществление функции назначения параметров протокола *http*-адреса; в-третьих, создания и администрированиясистемы доменных имен и адресов интернета (*Domain Name System*), без которых существование и функционирование целостного трансграничного интернета невозможно. Изложенное делает понятным, что управление интернетом прежде всего связано с деятельностью организаций, обеспечивающих осуществление обозначенных выше функций, а также технологическую поддержку трансграничного функционирования интернета, и именно *ICANN* принадлежит центральная роль.

ICANN была создана в соответствии с законами штата Калифорния (США) как некоммерческая организация, осуществляющая деятельность в качестве оператора доменного пространства интернета. До создания *ICANN* вопросами распределения имен и адресов в интернете и осуществлением надзора за всей системой доменных имен, занималось Правительство США в лице Министерства торговли США. Созданием *ICANN* в 1998 г. процесс передачи создания и администрирования системы доменных имен и адресов интернета (*DNS*) от Правительства США к *ICANN* был формально завершен. Вместе с тем Правительство США продолжало сохранять фактический контроль, а именно: деятельность *ICANN* как организации, являющейся юридическим лицом штата Калифорния (США) и представляющей «частный сектор», зиждилась на договорных отношениях с Правительством США.

ICANN «централизованно и единолично» осуществляет трансграничную координацию системы присвоения доменных имен и адресов в интернете, контролирует выполнение базовых принципов. Вместе с тем *ICANN* не управляет «содержимым интернета», не осуществляет фильтрацию нежелательного контента, не предоставляет доступа к интернету. Но именно *ICANN* поддерживает безопасность, стабильность и взаимодействие Сети, решает, какие устройства могут быть подключены к интернету и какие у них будут доменные имена. Именно *ICANN* принимает решение об утверждении и вводе в эксплуатацию новых доменов верхнего уровня, о регистрации доменных имен для государств, географических регионов. Система доменных имен и адресов интернета (*DNS*) координируется *ICANN* путем заключения соответствующего соглашения с юридическим или физическим лицом (оператором, организацией-регистратором и др.), которое поддерживает адреса доменов. Принципиальным моментом является то, что система доменных имен и адресов интернета (*DNS*) является ключевым вопросом управления интернетом. Следует отметить, что долгое

время вопрос управления интернетом рассматривался исключительно в контексте борьбы за контроль над системой распределения доменных имен, и в настоящее время этот контекст не только не теряет актуальности, более того – он приобретает новый импульс развития в связи с расширением зоны доменов верхнего уровня[1].

ICANN, таким образом, *de facto* осуществляет трансграничную координацию системы присвоения доменных имен и адресов в интернете, контролирует выполнение базовых принципов, т.е. является центральным звеном решения вопросов интернета, относящихся к «повседневной деятельности технического и эксплуатационного характера». Вместе с тем именно правовое положение *ICANN* как юридического лица права штата Калифорния (США) дает основание многим государствам утверждать, что США, а не международное сообщество государств, распределяют доменные имена и *IP*-адреса для всех стран мира и осуществляют надзор за этими процессами, что является нарушением основ многостороннего сотрудничества государств.

Предлагая организационные модели управления интернетом, Рабочая группа *WGIG* исходила из необходимости того, чтобы они, во-первых, отражали все элементы многостороннего управления интернетом, во-вторых, учитывали потребность интернационализации механизма управления интернетом; в-третьих, закрепляли институциональную координацию на универсальном, региональном и национальном уровнях.

Первая организационная модель. В этой модели предполагалось создание Глобального совета по интернету (*The Global Internet Council*), состоящего из членов, назначаемых правительствами с надлежащим учетом представительства каждого региона и при участии других заинтересованных сторон. Глобальный совет осуществлял бы функции международного управления интернетом, которые в настоящее время фактически осуществляет Министерство торговли США. Глобальный совет рассматривался как орган, который может заменить Правительственный консультативный комитет (*Government Advisory Committee, GAC*), *ICANN*[2].

[1] См. об этом подробнее, например: URL: http://newgtlds.icann.org/en/

[2] Правительственный консультативный комитет – *Governmental Advisory Committee, GAC*. В настоящее время членами Правительственного консультативного комитета (*GAC*) являются более 100 государств. На регулярной основе в работе *GAC* принимают участие также представители ряда международных межправительственных организаций, например Международного союза электросвязи (МСЭ), Всемирной организации интеллектуальной собственности (ВОИС) и др. Российская Федерация участвует в Правительственном консультативном совете *ICANN* с 2009 г. В настоящее время Россию в Правительственном консультативном совете *ICANN* представляют официальные лица

Предложение такой модели было связано с целью «интернационализировать» *ICANN*, которая «*централизованно и единолично*» осуществляет трансграничную координацию системы присвоения доменных имен и адресов в интернете и контролирует выполнение базовых принципов трансграничного функционирования интернета. Первая организационная модель предусматривала необходимость отчетности *ICANN* правительствам и Глобальному совету. Принципиальным моментом в предложенной модели являлось то, что Глобальный совет должен был функционировать совместно с ООН.

Функции Глобального совета по интернету должны были включать в себя следующее:

– определение международной государственной политики в отношении интернета и обеспечение надлежащего надзора за управлением ресурсами интернета, например за включением или исключением из файла корневой зоны, управлением *IP*-адресами, введением новых региональных доменов высшего уровня *TLD*, «перераспределяемых» в рамках общих доменов высшего уровня, *gTLD*;

– определение международной государственной политики и координация решений других ключевых вопросов, связанных с интернетом, например спам, персональные данные, кибербезопасность, киберпреступность, которые «системно» фактически не регулируются существующими межправительственными организациями;

– содействие переговорам по заключению договоров, конвенций и соглашений по вопросам взаимоотношений государств и их политики, касающейся интернета;

– формулирование и разработка руководящих принципов по широкому кругу вопросов для развития интернета, включая, в частности, возможности многоязычного использования интернета, справедливые расценки на подключение к международным сетям с учетом фактических расходов и справедливый доступ для всех;

– утверждение правил и процедур для механизмов урегулирования споров с выполнением функций арбитража.

Существенным вопросом для первой организационной модели являлось установление формально определенных официальных отношений между Глобальным советом по интернету, с одной стороны, и *ICANN* – с другой. В рамках первой модели *ICANN* рассматривался в качестве технической и операционной интернет-структуры, рефор-

Министерства связи и массовых коммуникаций (см. об этом: URL: https://gacweb.icann.org/display/gacweb/GAC+Representatives#GACRepresentatives-R, а также: URL: http://www.icann.org/general).

мированной, интернационализированной и подотчетной Глобальному совету.

Первая организационная модель предусматривала не только тесное взаимодействие Глобального совета по интернету с ООН, но и «приоритетное значение» государственного фактора при решении всех вопросов, рассматриваемых Глобальным советом. Частный сектор и гражданское общество в первой организационной модели осуществляли бы консультативную роль.

Вторая организационная модель предусматривала «трансформацию» *ICANN* в официальный международный орган – Форум по обсуждению вопросов интернета (далее – Форум). В организационном плане Форум мог бы осуществлять свою деятельность, в частности, на базе Правительственного консультативного комитета (*GAC*) *ICANN*. Форум рассматривался как площадка для проведения широких дискуссий по всем организационным вопросам функционирования интернета с равным участием правительств и всех заинтересованных сторон. Предлагалось закрепить за Форумом право принимать решения рекомендательного характера по вопросам управления интернетом. В этой организационной модели управления интернетом осуществление специальной надзорной функции за Форумом не предусматривалось. За создаваемым Форумом закреплялась бы функция координации работы всех заинтересованных сторон, а сам Форум рассматривался как структура, в которой могли бы открыто обсуждаться *все* вопросы управления интернетом *всеми* заинтересованными сторонами, включая организации, непосредственно участвующие в управлении интернетом. За Форумом закреплялось и право принимать решения рекомендательного характера по вопросам управления интернетом, в равной степени как и заинтересованные стороны вправе были бы принимать решения рекомендательного характера по конкретным вопросам управления интернетом для Форума.

Третья организационная модель. В этой модели управления интернетом предусматривалась необходимость создания Международного совета по интернету (*International Internet Council*, *IIC*) для управления наиболее важными аспектами интернета, включая решение политических вопросов, затрагивающих национальные интересы. В компетенцию Международного совета по интернету предлагалось включить вопросы международной государственной политики в отношении управления ресурсами интернета, а также вопросы международной государственной политики, не входящие в компетенцию других действующих межправительственных организаций. При решении этих воп-

росов правительствам отводилась ведущая роль. Роль частного сектора и гражданского общества в этой модели заключалась в выработке рекомендаций для правительств.

Третья организационная модель предполагала замену Правительственного консультативного комитета (*GAC*) *ICANN* Международным советом по интернету. При этом предлагалось сохранить *ICANN* в качестве организации, осуществляющей технические функции. В целях интернационализации механизма управления интернетом и минимизации контроля Правительства США над деятельностью *ICANN* организационные структуры *ICANN* следовало бы размещать в различных государствах. Правовым основанием функционирования структур *ICANN* стали бы соглашения с принимающим государством.

Четвертая организационная модель. Это некая комплексная модель, в которой предлагалось объединить три взаимосвязанных сферы: политику управления интернетом, надзорные функции и глобальную координацию. В этой модели предполагалось создание трех новых международных органов, в сферу ведения которых входили бы следующие вопросы:

– разработка государственной политики и принятие решений правительствами по вопросам международной государственной политики в отношении интернета;

– надзор за деятельностью органа, отвечающего на глобальном уровне за техническое и оперативное функционирование интернета, который находится в ведении частного сектора;

– глобальная координация развития интернета на основе равноправного диалога между правительствами, частным сектором и гражданским обществом.

Для решения указанных задач создавались бы соответственно: Совет по глобальной политике в отношении интернета (*The Global Policy Council*), Всемирная корпорация по присвоению имен и номеров в интернете (*The World Internet Corporation for Assigned Names and Numbers*) и Глобальный форум по управлению интернетом (*The Global Internet Governance Forum*).

В компетенцию *Совета по глобальной политике в отношении интернета* входили бы вопросы международной государственной политики в отношении Интернета и участие в разработке тех аспектов государственной политики, которые связаны с определением технических стандартов управления интернетом. Совет по глобальной политике в отношении интернета фактически должен был стать неким правительственным механизмом по вопросам, рассматриваемым существу-

ющими межправительственными организациями, а также по другим вопросам государственной политики, которыми в настоящее время не занимается какой-либо конкретный орган или которые относятся к компетенции целого ряда международных или межправительственных организаций. Частный сектор и гражданское общество принимали бы участие в работе Совета в качестве наблюдателей.

Организационной основой *Всемирной корпорации по присвоению имен и номеров в интернете* должна была стать реформированная и интернационализированная *ICANN*. Соответственно, Всемирная корпорация по присвоению имен и номеров в интернете была призвана отвечать за развитие интернета в технической и экономической областях. Предполагалось, что Всемирная корпорация по присвоению имен и номеров в интернете должна представлять интересы частного сектора. Вместе с тем в эту организацию были бы включены правительства, которые осуществляли бы две функции. Первая функция – надзорная. Эта функция закреплялась за Надзорным комитетом, назначаемым Советом по глобальной политике в отношении интернета. Если Совет по глобальной политике в отношении интернета должен нести ответственность на глобальном уровне за техническое и оперативное функционирование интернета, то функции Надзорного комитета не были бы связаны с оперативной деятельностью и управлением интернетом. Фактически речь шла о роли, которую в настоящее время осуществляет Министерство торговли США. Вторая функция – консультативная, аналогичная той функции, которую исполняет в настоящее время Правительственный консультативный комитет (*GAC*) *ICANN*.

Всемирная корпорация по присвоению имен и номеров в интернете заключала бы с принимающей ее страной соответствующее соглашение и осуществляла свою деятельность в тесном взаимодействии с ООН. Правительства и гражданское общество во Всемирной корпорации выступали бы в качестве наблюдателей-консультантов.

Третьим органом, предусмотренным четвертой организационной моделью, является *Глобальный форум по управлению интернетом,* который отвечал бы за содействие координации и обсуждению вопросов государственной политики, связанных с интернетом при равноправном участии правительств, частного сектора и гражданского общества.

Предложенные Рабочей группой *WGIG* организационные модели управления интернетом фактически представляли собой возможные варианты институционализации управления интернетом и явились отражением необходимости, во-первых, сотрудничества в управлении интернетом на многосторонней основе; во-вторых, интернационализа-

ции механизма управления интернетом; в-третьих, институциональной координации на универсальном, региональном и национальном уровнях и, в-четвертых, актуализировали постановку вопроса о создании глобального многостороннего форума для решения вопросов государственной политики в отношении управления интернетом.

На Всемирной встрече *WSIS*, в ходе проведения второго, тунисского, этапа (2005 г.), ряд государств инициировали обсуждение вопроса о необходимости участия правительств разных стран в присвоении имен и адресов в интернете и в придании большей степени интернационализации деятельности, связанной с управлением интернетом. Было высказано предложение о создании международной организации, которая стала бы основой интернационализации управления интернетом на межправительственной основе. Созданная международная организация смогла бы осуществлять репрезентативное управление интернетом, не зависящее от национальных и политических влияний, прежде всего со стороны Соединенных Штатов. При этом такая международная организация рассматривалась в качестве международной платформы сотрудничества государств для разработки общих принципов управления интернетом.

Предполагалось, что компетенция международной организации будет связана с разработкой основных принципов, обязательных для корпорации *ICANN,* но с сохранением за ней осуществления функций распределения имен и адресов интернета. Таким образом, *ICANN* сохраняла бы функции осуществления текущих задач по обеспечению и поддержанию работы интернета, связанной с повседневной деятельностью технического и эксплуатационного характера, а полномочия принятия политических решений от *ICANN* перешло бы к новой международной организации, все решения которой вырабатывались бы на основе Декларации принципов по вопросам информационного общества, принятой на женевском этапе Всемирной встречи на высшем уровне по вопросам информационного общества (2003 г.). Все предложенные меры должны были рассматриваться как своего рода гарантия для *ICANN*, что передача международной организации функций, связанных с выработкой политических решений, не повлечет за собой изменений для *ICANN* и позволит сохранить *status quo* управления интернетом в целом.

Предложение о создании международной организации не получило широкой поддержки главным образом из-за позиции США, представители которых выдвинули несколько причин, не позволяющих делегировать указанные полномочия международной организации.

Во-первых, наделение той или иной международной организации, например Международного союза электросвязи (МСЭ), полномочиями по управлению интернетом приведет, по их мнению, к краху Сети, поскольку такой орган не сможет обеспечить реализацию фундаментальных ценностей и принципов интернета. Во-вторых, даже если «международная бюрократия» и не приведет интернет к гибели, интернационализация управления интернетом даст возможность некоторым странам с недостаточно высоким уровнем демократии, открытости общения и свободомыслия оказывать негативное влияние на формирование политики развития интернета.

Важнейшим итогом тунисского этапа Всемирной встречи, было учреждение Форума по управлению интернетом (*Internet Governance Forum, IGF*; далее – Форум *IGF*). Форум *IGF* был создан под эгидой ООН для ведения многостороннего политического диалога по вопросам управления интернетом и его деятельность осуществлялась на основании мандата ООН. Мандат не предполагал жесткой организационной структуры и закреплял условия нейтральности, прозрачности, демократичности, децентрализованности Форума *IGF* с возможностью периодического пересмотра мандата. Предусматривалось, что Форум *IGF* в своей работе должен опираться на существующий институциональный механизм управления использованием интернета и особое внимание Форуму *IGF* следует уделять взаимодополняемости функций всех действующих организаций, обеспечивающих процесс функционирования интернета, а также заинтересованных сторон, принимающих участие в этом процессе. Форум *IGF* не осуществляет никаких надзорных функций и не подменяет существующие структуры, механизмы, институты или организации, но в то же время привлекает их к своей работе и использует их опыт. Принципиальным моментом является то, что Форум *IGF* не вмешивается в вопросы повседневной эксплуатации или технического обслуживания Интернета. Форум *IGF* действует на постоянной основе посредством регулярных всемирных встреч, совещаний, которые могут также проводиться одновременно с крупными конференциями ООН по соответствующим вопросам. Решения, принимаемые Форумом *IGF*, не имеют обязательной силы и носят характер рекомендаций. Материалы о его деятельности, а также рассматриваемые и принимаемые документы публикуются на регулярной основе и находятся в открытом доступе.

С 2006 г. до настоящего времени Форум *IGF* провел семь встреч, и за период его деятельности существенно изменился формат обсуждаемых вопросов, изменились как акценты в постановке самих вопросов,

так и их приоритетность. Например, если в 2006 г. вопросы открытости и безопасности обсуждались отдельно, то начиная с 2008 г. эти два вопроса, наряду с конфиденциальностью, стали рассматриваться в контексте с такими вопросами, как доступ к знаниям, свобода выражения мнений, права интеллектуальной собственности, преступность в интернете и государственная безопасность. Явно сместились акценты обсуждения «проблемных сфер»: если в 2006 г. вопросы безопасности были связаны со спамом, то в 2010 г. тема безопасности была расширена за счет включения вопроса о регулировании вредоносного интернет-контента.

В настоящее время Форум *IGF* по управлению интернетом действует как структурное звено системы ООН и служит площадкой для обсуждения разнообразных аспектов управления интернетом, включая ключевые вопросы государственной политики. Примечательно, что рекомендации Форума *IGF* по управлению интернетом находят отражение в международно-правовых документах международных организаций, например в декларациях Комитета министров Совета Европы, Организации экономического сотрудничества и развития (ОЭСР) и др.

После истечения пятилетнего мандата Форума *IGF* в 2010 г. по рекомендации Генерального секретаря ООН было принято решение продлить его мандат еще на пять лет и в 2015 г. проанализировать деятельность Форума *IGF* в контексте 10-летнего периода выполнений решений Всемирной встречи *WSIS*. Это решение было закреплено соответствующей резолюцией Генассамблеи ООН[1]. В настоящее время в рамках подготовки третьего этапа Всемирной встречи *WSIS*, проведение которой запланировано на 2015 г., решается вопрос о том, чтобы «регуляризировать бюджет Форума *IGF* в рамках ООН и превратить его в официальный орган межправительственного механизма ООН»[2]. Не будет преувеличением сказать, что Форум *IGF* представляет новую модель международного сотрудничества, функционирующую на многосторонней основе (*Multistakeholders Model*)[3].

Собственно, сама Всемирная встреча *WSIS* и формат ее проведения есть фактическое отражение мультистейкхолдерского подхода и свидетельство признания необходимости участия всех заинтересованных сторон в решении вопросов управления интернетом и, в общем плане, «построения информационного общества». Практически 10-летний

[1] См. резолюцию 65/141 ГА ООН: http://www.un.org/
[2] Раздел «B» резолюции ГА ООН A/65/78-E/2010/68.
[3] URL: http://www.itu.int/wsis

период реализации итоговых документов Всемирной встречи *WSIS*[1] подтверждает, что без взаимодействия всех заинтересованных сторон, без принятия согласованных между ними норм и принципов регулирования ни одно из решений или технических требований, связанных с управлением интернетом, не может быть эффективно реализовано. Мультистейкхолдеризм является эффективным способом трансграничного функционирования интернета, обеспечивает совместимость, стабильность, безопасность и доступность глобальной инфраструктуры интернета, в то же время предоставляет суверенным государствам возможность регулирования использования интернета в пределах национальной юрисдикции. Принцип участия всех заинтересованных сторон является основой дальнейшего развития интернета как глобальной Сети и важнейшим элементом управления интернетом.

3. Роль международных межправительственных организаций в управлении интернетом

С точки зрения международно-правового регулирования интернета важнейшее значение имеет Организация Объединенных Наций и ее специализированные учреждения, такие как Международный союз электросвязи (МСЭ), Всемирная организация по интеллектуальной собственности (ВОИС), Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО) и др.

Как говорилось ранее, обсуждение проблем международного сотрудничества управления интернетом было инициировано, развивалось и осуществляется в настоящее время в рамках международных межправительственных организаций. При этом особенностью деятельности международных межправительственных организаций, как универсальных, так и региональных, включенных в этот процесс, является то, что в ней принимают участие представители всех заинтересованных сторон: гражданского общества, частного сектора, международных неправительственных организаций, технического и академического сообщества. Другая особенность – то, что формат деятельности международных межправительственных организаций связан с реализацией задач и решений, закрепленных в документах двух этапов Всемирной встречи на высшем уровне по информационному обществу. Еще одной особенностью является то, что в рамках международных межправитель-

[1] См., например, резолюцию ГА ООН 58/201 (http://www.itu.int/wsis/documents//doc_multi.asp?lang=en&id=2167), а также информацию о Всемирном саммите Информационного общества (http://www.itu.int/wsis/basic/about.html).

ственных организаций создаются разнообразные структуры (рабочие группы, комиссии, программы, форумы, комитеты и др.), деятельность которых связана с той или иной сферой интернета. При этом такие структуры, во-первых, действуют на основании мандатов этих межправительственных организаций; во-вторых, в мандатах, как правило, определяется круг вопросов, а не организационные формы деятельности таких структур; в-третьих, в деятельности создаваемых структур принимают участие все заинтересованные стороны; в-четвертых, такие структуры могут действовать как на временной, так и на постоянной основе; в-пятых, все принимаемые такими структурами решения носят рекомендательный характер. Следует обратить внимание также на то, что широко обсуждаемая в настоящее время необходимость совершенствования механизма международного сотрудничества по вопросам управления интернетом осуществляется в рамках действующих международных межправительственных организаций, более того, сотрудничество по вопросам управления интернетом связывается с необходимостью использования действующей системы международных организаций.

Роль международных межправительственных организаций в развитии информационных и коммуникационных технологий в целом и в механизме управления интернетом в частности определена всеми итоговыми документами Всемирной встречи на высшем уровне по вопросам информационного общества. Напомним, что на первом, женевском, этапе Всемирной встречи на высшем уровне по вопросам информационного общества был принят основополагающий документ – Женевский план действий. В этом документе предусмотрено 11 направлений действий, реализация которых закреплена за конкретной международной межгосударственной организацией, международной неправительственной организацией, организацией частного сектора. Простое перечисление организаций, ответственных за реализацию соответствующего направления действий, дает общее представление об их месте, о роли и взаимодействии в общем процессе решения задач управления интернетом: Международный союз электросвязи, ЭКОСОС, Региональные комиссии ООН, Департамент ООН по экономическим и социальным вопросам, ВТО, ЮНЕСКО, ФАО, ЮНИДО, ЮНКТАД, ПРООН, Ассоциация по развитию коммуникаций (APC), Всемирный почтовый союз, ВОЗ, МОТ, ИКАО, Всемирная метеорологическая организация, Программа ООН по населенным пунктам (*UN Habitat*) и др. К примеру, реализация направления, связанного с «содействием применению информационных и коммуникационных технологий в целях развития», закреплена за Международным

союзом электросвязи, ЭКОСОС, Региональными комиссиями ООН, Департаментом ООН по экономическим и социальным вопросам; направление «доступ к информации и знаниям» – за Международным союзом электросвязи, ЮНЕСКО, ФАО, ЮНИДО и т.д.

Из шести главных органов ООН три, а именно Генеральная Ассамблея, Экономический и социальный совет и Секретариат, непосредственно участвуют в рассмотрении разнообразных аспектов управления интернетом и институционализацией этого процесса. По итогам Всемирной встречи на высшем уровне по информационному обществу Экономический и социальный совет ООН (ЭКОСОС) на основании мандата Генеральной Ассамблеи ООН выступает как общесистемный координатор реализации решений женевского и тунисского этапов Всемирной встречи на высшем уровне по вопросам информационного общества. Такая роль ЭКОСОС связана с тем, что он действует под общим руководством Генеральной Ассамблеи, координирует деятельность ООН и учреждений ее системы, специализированных учреждений, функциональных и региональных комиссий ООН в экономической и социальной областях, служит центральным форумом для обсуждения международных экономических и социальных проблем и выработки рекомендаций в отношении политики для государств-членов и системы ООН.

Значительная роль в решении вопросов управления интернетом принадлежит Генеральному секретарю ООН. Во-первых, в соответствии с положениями Тунисской программы Всемирной встречи по вопросам информационного общества Генеральный секретарь ООН периодически представляет государствам – членам ООН доклад о деятельности Форума по управлению интернетом и привлекает для обсуждения его деятельности все заинтересованные стороны с учетом сбалансированного географического представительства. Во-вторых, Генеральный секретарь координирует деятельность и содействует взаимодействию всех заинтересованных сторон, участвующих в решении вопросов управления интернетом. Так, в 2006 г. Генеральным секретарем были выбраны 10 организаций, представляющих все заинтересованные стороны, для дальнейшего выполнения задач, намеченных двумя этапами Всемирной встречи по информационному обществу. Наряду с международными межправительственными организациями были названы и организации, представляющие частный сектор и гражданское общество, а именно: *ICANN*, Консорциум «Всемирная паутина» (*W3C*), «Общество Интернета» (*ISOC*), Организация по ресурсам нумерации (*NRO*); в качестве организации, представляющей технические и ака-

демические круги, была обозначена Рабочая группа по интернет-инжинирингу (*Internet Engineering Task Force, IETF*).

В-третьих, Генеральный секретарь содействует активизации и расширению сотрудничества государств по вопросам политики в отношении интернета.

Группа ООН по информационному обществу (*UN Group on the Information Society, UN GIS*) была создана в 2006 г. в качестве специализированного подразделения ООН по вопросам информационных технологий, в качестве межучрежденческого механизма для координации политики деятельности организаций системы ООН в целях осуществления Женевского плана действий и Тунисской программы для информационного общества. Международные организации, входящие в состав Группы, имеют статус постоянных и непостоянных членов. Постоянными членами Группы являются МСЭ, ЮНЕСКО, ЮНКТАД, Экономическая комиссия ООН для Африки, ЭКАООН, а также Программа развития ООН (ПРООН). Группа имеет также широкий членский состав непостоянных членов, включающий организации ВТО, МАГАТЭ, МОТ, ОЭСР и др.

Названные выше международные организации, иные специализированные учреждения системы ООН, международные неправительственные организации взаимодействуют с государствами и всеми заинтересованными сторонами в решении вопросов управления интернетом. В этом процессе особое положение занимает Международный союз электросвязи (МСЭ), деятельность которого наиболее тесно связана с информационно-коммуникационными технологиями. Все 11 направлений действий в реализации общего процесса управления иинтернетом, включая вопросы институционализации процесса управления интернетом, которые были определены в Женевском плане действий, предусматривают участие Международного союза электросвязи. МСЭ принимает участие в решении вопросов всех 11 направлений действий либо самостоятельно, либо совместно с другими международными правительственными и неправительственными организациями.

Следует отметить, что многие развивающиеся страны, Россия, Китай, Бразилия, Иран, Пакистан и другие рассматривают Международный союз электросвязи в качестве межправительственной основы для наблюдения за различными аспектами управления интернетом и институционализации механизма управления интернетом. Призывы к расширению компетенции МСЭ поддерживаются не всеми государствами, включая развитые страны, а также не поддерживаются представителями заинтересованных сторон (S*takeholders*), которые участвуют

в решении вопросов управления интернетом. Высказываются вполне обоснованные опасения, что при таком подходе существует реальная опасность «слияния» традиционных телекоммуникационных сетей и интернета, что в свою очередь может повлиять на весь механизм трансграничного функционирования интернета. Кроме того, расширение полномочий МСЭ может радикально изменить сложившийся многосторонний механизм управления интернетом ((*Multistakeholder's Model*), включающий все заинтересованные стороны, который сформировался эволюционным путем и оказался эффективным для обеспечения его стабильности, безопасности и доступности трансграничной инфраструктуры интернета, в то же время предоставляя суверенным государствам возможность регулирования использования интернета в пределах своей юрисдикции.

Международный союз электросвязи – специализированное учреждение ООН, основными документами которого являются Устав международного союза электросвязи, Конвенция международного союза электросвязи и Административные регламенты. В соответствии с Уставом высшим органом Международного союза электросвязи является Полномочная конференция, которая проводится один раз в четыре года. В этой связи следует отметить, что в декабре 2012 г. в Дубае (ОАЭ) состоялась очередная Полномочная конференция МСЭ. Особое внимание со стороны мирового сообщества к этой Полномочной конференции было связано главным образом с тем, что на ней обсуждались вопросы международно-правовой регламентации информационных и коммуникационных технологий, включая интернет. На Полномочной конференции обсуждался и один из основных договоров МСЭ – Административный регламент международной электросвязи (*International Telecommunication Regulations*, *ITRs*), принятый на Всемирной административной конференции по вопросам телефонной и телеграфной связи в 1988 г. (*World Administrative Telegraph and Telephone Conference, WATTC*-88). Необходимость обсуждения Административного регламента международной электросвязи была связана с тем, что этот международный договор был принят в 1988 г., в «доинтернетовскую» эпоху, в период существования государственной телекоммуникационной монополии. Почти за четверть века действия Административного регламента международной электросвязи условия и порядок осуществления телекоммуникационной связи существенно изменились. Функционирование информационных и коммуникационных технологий, включая интернет, основывается на *IP*-протоколах – наборе правил, обеспечивающих соединение и обмен данными между

компьютерами, подключенными к сети, а для интернета существенная роль принадлежит протоколам *TCP/IP* и *HTTP*. В связи с необходимостью «адаптации» регулирования технических, операционных и прочих вопросов информационных и коммуникационных технологий Полномочная конференция в Дубае приняла решение о частичном пересмотре Административного регламента международной электросвязи. Итогом Полномочной конференции стало подписание новой редакции Административного регламента международной электросвязи. Из 193 государств, принимавших участие в Полномочной конференции МСЭ, этот документ подписали 89 государств (Россия, Китай, Бразилия, Иран, Куба, ряд развивающихся стран Азии и Африки), 55 государств (США, Канада, страны – члены ЕС, Индия и др.) выступили против этого договора, ряд государств воздержались от его подписания.

4. Международное сотрудничество государств в управлении интернетом

Разнообразие подходов суверенных государств в контексте международного сотрудничества в сфере управления интернетом в самом общем плане могут быть обобщены следующим образом. Во-первых, ряд государств придерживаются позиции сохранения *status quo*, а именно: сохранение роли *ICANN* в управлении интернетом; поддержка деятельности Форума *IGF* как международной платформы сотрудничества всех заинтересованных сторон; обсуждение всех вопросов управления интернетом в рамках существующей системы международных межправительственных организаций. Во-вторых, некоторые государства поддерживают идею создания новой международной межправительственной организации, которая должна либо заменить Форум *IGF*, либо действовать наряду с ним, однако принципиальным моментом является то, что созданная международная организация должна действовать под эгидой ООН. В-третьих, ряд государств рассматривают Международный союз электросвязи как международную организацию, которая должна стать центральным звеном управления интернетом.

В этой связи представляют интерес конкретные предложения, выдвигавшиеся государствами в течение 2010–2012 гг. Так, в июле 2011 г. в рамках ЭКОСОС группа государств *IBSA* (Индия, Бразилия, ЮАР) выступила с совместным заявлением (далее – Предложение *IBSA*), в котором содержался призыв создать межправительственный механизм для расширения сотрудничества государств в решении проблем

управления интернетом и дополнения деятельности Форума *IGF*. Коалиция государств *IBSA* была создана в 2003 г. в целях координации, сотрудничества и обмена знаниями по актуальным глобальным проблемам, а также создания условий вклада этих стран в процесс формирования так называемого нового международного порядка, поскольку эти страны имеют близкие позиции относительно роли и развития международного права. Управление интернетом является одним из тех вопросов, по которому эти государства занимают близкие позиции.

Предложение *IBSA* исходит из того, что помимо технических аспектов управления интернетом есть ряд сфер, связанных с государственной политикой, которые требуют участия правительства. Они затрагивают, среди прочего, такие вопросы, как стабильность (*stability*) интернета; совместимость (*interoperability*); доступность (*accessibility*); открытость *(openness*); нейтральность Сети (*Network neutrality*); доступ к информации и знаниям; конфиденциальность; кибербезопасность и развитие информационно-коммуникационных технологий в контексте функционирования интернета.

В Предложении *IBSA* подчеркивается, что центральным вопросом управления Интернетом является управление «критическими ресурсами интернета», но при этом только *ICANN* распределяет доменные имена и *IP*-адреса для всех стран мира и осуществляет надзор за этими процессами. Несмотря на то, что деятельность *ICANN* носит открытый характер и подотчетна международному интернет-сообществу, она остается юридическим лицом права США, и, таким образом, только единственная страна, а не международное сообщество государств управляет «критическими ресурсами интернета», что является нарушением основ многостороннего сотрудничества государств. Вопросы сотрудничества государств по вопросам управления интернетом нуждаются в обсуждении между государствами – членами ООН, и государствам следует рассматривать именно ООН как формальную платформу обсуждения таких вопросов. Более того, формирование межправительственной платформы следует не только обсуждать в рамках ООН, но необходимо, чтобы это было оформлено соответствующим мандатом ООН. Межправительственная платформа должна также дополнять деятельность Форума по управлению интернетом, поскольку он является многосторонней площадкой для всех заинтересованных сторон.

Предложение *IBSA* исходит из того, что платформа ООН позволит международному сообществу достигнуть целей развития, закрепленных в Тунисской программе, а практическое расширение международного

сотрудничества обеспечит реализацию положений Целей развития, закрепленных Декларацией тысячелетия ООН от 8 сентября 2000 г.[1] В Предложении *IBSA* выдвигается идея создания под эгидой ООН Межправительственной рабочей группы Комиссии по науке и технике в целях развития в качестве координационного центра в системе ООН. Межправительственная рабочая группа должна обладать мандатом ООН на подготовку доклада о возможных институциональных механизмах для улучшения сотрудничества на основе консультаций со всеми заинтересованными сторонами, включая все международные организации. Свой доклад Межправительственная рабочая группа должна представить Генеральной Ассамблее ООН. Межправительственная рабочая группа в своем докладе должна либо предложить расширение механизма международного сотрудничества в рамках существующих международных организаций, либо рекомендовать создать новый международный орган для такого сотрудничества.

Предложение *IBSA* призывает Генерального секретаря ООН осуществлять процесс консультаций с государствами-членами и всеми заинтересованными сторонами с целью содействия расширению международного сотрудничества по вопросам управления интернетом. В Предложении *IBSA* отмечается, что оно не является «планом захвата управления интернетом Организацией Объединенных Наций» *(«UN Takeover» of Internet Governance*), его основной целью является сохранение стабильности и безопасности интернета как глобального средства на основе широкого участия всех заинтересованных сторон.

Анализ содержания Предложения *IBSA* позволяет сделать вывод о том, что создание нового международного межправительственного органа в рамках ООН, которому следует «поручить разработку и установление международной государственной политики с целью обеспечения координации и согласованности междисциплинарных глобальных проблем интернета», а также «интегрировать и контролировать органы, ответственные за техническое и оперативное функционирование интернета», рассматривается в качестве одного из возможных вариантов. При этом если Межправительственная рабочая группа предложит сохранить механизм международного сотрудничества «в рамках существующих международных организаций», вопрос о создании нового международного межправительственного органа в рамках ООН может быть снят.

В октябре 2011 г. на 66-й сессии Генеральной Ассамблеи ООН Индия сделала заявление о международном механизме управления

[1] URL: http://www.un.org/ru/documents/decl_conv/declarations/summitdecl.shtml

интернетом (далее – Инициатива Индии)[1]. Инициативу Индии, по-видимому, следует рассматривать как некое развитие идей, закрепленных в Предложении *IBSA*, поскольку она была выдвинута через три месяца после Предложения *IBSA* и Индия входит в коалицию *IBSA*. Вместе с тем следует обратить внимание на то, что, во-первых, Инициатива Индии идет дальше, развивая в практической плоскости решения Тунисской программы для информационного общества. Во-вторых, если в Предложении *IBSA* расширение механизма международного сотрудничества формулировалось альтернативно – либо в рамках существующих международных организаций, либо в рамках нового международного органа, – в Инициативе Индии создание международного межправительственного органа рассматривается как необходимость, а не как «вопрос дискуссии для международного сообщества».

Инициатива Индии исходит из необходимости сохранения интернета как неограниченной, открытой и свободной глобальной среды, которая развивается за счет частных инноваций и индивидуального творчества и служит инструментом для открытого общения, доступа к культуре, знаниям, для демократизации и развития; признает роль различных участников и заинтересованных сторон в разработке и продолжении обогащения в интернете; привержена модели многостороннего управления интернетом как на национальном, так и на глобальном уровне; отмечает, что глобальное управление интернетом может быть функциональным, эффективным и надежным, если все соответствующие заинтересованные стороны будут способствовать процессу управления и участвовать в нем. Для разработки глобальной интернет-политики в Инициативе Индии предлагается создать международный межправительственный орган в рамках ООН, который мог бы быть назван «Комитет Организации Объединенных Наций по вопросам политики интернета» (*United Nations Committee for Internet-Related Policies, CIRP*). Целью создания такого международного органа является формирование многостороннего механизма, не «контролирующего» интернет, а *дающего возможность* избежать ситуаций, при которых за правительствами не оставалось бы «последнее слово в регулировании интернета», и сделать возможным, чтобы интернет регулировался не в одностороннем порядке, а в процессе открытого, демократического, общенародного обсуждения с участием всех заинтересованных сторон. Инициатива Индии подробно формулирует цели, задачи, организационную структуру, порядок функционирования создаваемого международного межправительственного органа,

[1] См. подробнее: http://igfwatch.org/discussion-board

при этом предусматривается участие всех заинтересованных сторон в работе международного органа, а также организационные формы такого участия. Инициатива Индии решает вопрос бюджета нового международного органа, вопросы координации деятельности с другими международными межправительственными и неправительственными организациями.

Инициативы, подобные Предложению *IBSA* или Инициативе Индии, можно приветствовать; их реализация может в определенной мере демократизировать процесс принятия решений по вопросам управления интернетом, а также способствовать продвижению по пути интернационализации механизма управления интернетом. В этом случае высока вероятность возникновения условий для возможности разработки и принятия адекватных международно-правовых норм для управления интернетом. Однако в настоящее время ключевой вопрос о широком международном консенсусе относительно создания такого органа остается по-прежнему открытым.

5. Вопросы безопасности управления интернетом

Одним из важнейших аспектов управления интернетом и обеспечения его трансграничного функционирования является обеспечение его безопасного использования и противодействие попыткам противоправного использования интернета. Принципиальным тезисом является то, что безопасность интернета важна не сама по себе, безопасность интернета важна для его функционирования и применения. С развитием современных информационных технологий человечество столкнулось с новыми типами угроз: возможностями силового противостояния государств в киберпространстве («кибервойны»), использования информационных технологий террористическими организациями либо с террористическими целями («кибертерроризм»), а также использования интернета в иных противоправных целях, с нарушением установленного правопорядка, преследуемым уголовным законодательством национальных государств («киберпреступность»), и т.д. Терминологическое и понятийное разнообразие, о котором говорилось выше, получает конкретное выражение, в частности в том, что в национальном праве ряда государств понятие «киберпреступность» не используется. Например, в российском уголовном праве соответствующие составы преступлений названы как «преступления в сфере компьютерной информации». Примечательно, что государствам в рамках такой международной организации, как Совет Европы, удалось

разработать и принять Конвенцию о киберпреступности (Будапешт, 2001 г.). В английской версии эта Конвенция называется *Convention on Cybercrime*, однако в переводе на русский язык (неофициальный перевод) этот документ получил название «Конвенция о преступности в сфере компьютерной информации», хотя в российской доктрине, в деловой лексике и проч. этот документ часто называется Конвенцией о киберпреступности или Будапештской конвенцией.

Следует отметить, что в настоящее время Будапештская конвенция о киберпреступности – единственный международный договор, участниками которого являются не только страны – члены Совета Европы, но и такие государства, как Аргентина, Австралия, Канада, США, Япония и др.[1] Вместе с тем несмотря на то, что участниками этой Конвенции являются не только европейские страны, ее нельзя назвать универсальным международно-правовым договором. Российская Федерация не является участницей Будапештской конвенции, хотя она принимала участие в ее разработке, в 2005 г. подписала эту Конвенцию, но затем отозвала свою подпись. Отметим, что данная Конвенция не предусматривает возможность для стран-участниц делать оговорки при присоединении к Конвенции. В ряде статей Конвенции содержатся положения, которые можно рассматривать как нарушение суверенных прав стран-участниц. Так, ст. 32 (*b*) Конвенции позволяет получать без согласия страны-участницы доступ к хранящимся на ее территории компьютерным данным, т.е. проводить трансграничные расследования и следственно-оперативные мероприятия. Закрепление такой конвенционной нормы вызывает категорическое несогласие Российской Федерации.

Российская Федерация по вопросам управления интернетом свою позицию не сформулировала. В настоящее время существует настоятельная необходимость корреляции усилий всех «российских» заинтересованных сторон. Представители некоммерческого сектора (экспертного сообщества) российского интернета достаточно активно участвуют в деятельности международных организаций и форумов, связанных с трансграничным управлением интернета[2]. Принцип участия всех заинтересованных сторон не всегда соблюдается в законотворческом процессе применительно к регулированию интернет-технологий

[1] В 2012 г. Белоруссия выразила желание присоединиться к Конвенции.

[2] Например, проекты Координационного центра национального домена сети Интернет (URL: http://cctld.ru/ru/activities/actions_archive.php); Центра политических исследований России («ПИР-Центр») (URL: http://www.pircenter.org/projects/10-international-information-security-and-global-internet-governance).

на национальном уровне. Так, крупнейшие российские интернет-компании «Яндекс» и «Мэйл.Ру» неоднократно выступали против поспешных и непродуманных, с их точки зрения, законотворческих инициатив, в ускоренном порядке принимавшихся Государственной Думой в 2012–2013 гг.[1] Аналогичные позиции занимали представители экспертного сообщества российской индустрии, объединенные в Российской ассоциации электронных коммуникаций (РАЭК)[2].

Примечательно, что в Российской Федерации вопросы «информационной безопасности» «сетевой безопасности на глобальном уровне» не только являются предметом системного и последовательного изучения, но и получают закрепление как в актах национального законодательства, так и в международно-правовых инициативах Российской Федерации. Например, в конце 2013 г. был принят такой документ, как «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года»[3].

Российская Федерация в 2011 г. в рамках ООН инициировала рассмотрение документов, связанных с международно-правовым регулированием вопросов информационной безопасности, – в сентябре 2011 г., на 66-й сессии Генеральной Ассамблеи ООН, на имя Генерального секретаря ООН было направлено письмо Постоянных представителей при ООН Китая, Российской Федерации, Таджикистана и Узбекистана. Четыре государства – члена ООН предложили к рассмотрению Правила поведения в области обеспечения международной информационной безопасности (далее – Кодекс информационной безопасности)[4]. Необходимость принятия Кодекса информационной безопасности эти государства связывали с тем, что вопросы интернет-безопасности имеют большое значение и их следует рассматривать в рамках международного сотрудничества и в духе взаимного уважения. Кодекс призван защищать интернет и другие информационно-коммуникационные сетевые технологии от угроз и «уязвимости».

Кодекс информационной безопасности был вынесен на обсуждение международного сообщества. В концентрированном виде параметры обсуждений нашли отражение в документе, представленном Советом гражданского сообщества по управлению интернетом (*Civil Society Internet Governance Caucus*), который является открытым фору-

[1] См., например: URL: http://www.therunet.com/news/1089-lidery-rossiyskogo-rynka-protiv-antipiratskogo-zakona

[2] URL: http://raec.ru/right/position/

[3] URL: http://www.scrf.gov.ru/documents/6/114.html

[4] См. текст документа A66/356: URL: http://www.un.org/en/ga/

мом для организаций, различных групп гражданского общества и обсуждающих вопросы управления интернетом[1]. Три тезиса, которые касаются ключевых вопросов управления интернетом и прав человека, являются принципиальными. Первый тезис – обсуждение проблем, связанных с управлением интернетом, включая вопросы стабильного и безопасного функционирования интернета, не может происходить только на уровне государств. Все вопросы политики управления интернетом могут решаться только путем вовлечения всех заинтересованных сторон: гражданского общества, частного сектора, технического и академического сообщества, правительств. При этом игнорирование такого условия противоречит положениям, закрепленным итоговыми документами двух этапов Всемирной встречи на высшем уровне по информационному обществу. В предлагаемом Кодексе информационной безопасности отсутствуют ссылки на многосторонний подход к определению политики интернета. Второй тезис – содержание терминов и понятий, которые закрепляются в Кодексе информационной безопасности, – применительно к правам человека вызывают ряд вопросов. В частности, содержащееся в тексте Кодекса информационной безопасности положение об «уважении прав человека и основных свобод» бесспорно. Вместе с тем Кодекс содержит призыв к уважению «разнообразия истории, культуры и социальных систем всех стран», что может быть истолковано как ограничение приверженности к универсальному характеру прав человека. Третий тезис – Кодекс информационной безопасности предусматривает сотрудничество в «борьбе с преступной или террористической деятельностью с использованием информационно-коммуникационных технологий, включая *сети*» и сдерживание «распространения информации террористического, экстремистского и сепаратистского характера, а также подрывающей политическую, экономическую и социальную стабильность государств, их культурный и духовный уклад». Такое широкое толкование противоречит «допустимым ограничениям на свободу выражения мнений», закрепленным ст. 19 (3) Международного пакта о гражданских и политических правах 1966 г., и может быть «расширительно интерпретировано» со стороны правительств, позволяя им существенно ограничивать права на свободу выражения мнений.

Несмотря на то, что Кодекс информационной безопасности не получил широкой международной поддержки, он был представлен в ка-

[1] См. подробнее: URL: http://www.igcaucus.org/. Документ был подготовлен от имени группы неправительственных организаций и гражданского общества (Найроби, 6-й Форум по управлению интернетом).

честве официального документа 66-й сессии Генеральной Ассамблеи ООН и его обсуждение государствами – членами ООН внесло определенный вклад в контекст «достижение консенсуса в отношении международных норм и правил поведения государств в киберпространстве».

В 2011 г. Российская Федерация подготовила и предложила для обсуждения в рамках ООН Конвенцию о международной информационной безопасности (концепция)[1]. Документ предлагает определить права и обязанности государств в информационном пространстве и закрепляет принцип государственного суверенитета над «национальными сегментами» интернета. Документ содержит призыв к государствам-участникам не применять информационные и телекоммуникационные технологии, в том числе интернет, для совершения враждебных действий или актов агрессии и создания угроз для международного мира и безопасности; не распространять информацию об оружии и связанных с ними технологиях, а также сотрудничать в борьбе с преступной и террористической деятельностью, в полной мере уважать права и свободы в информационном пространстве и содействовать созданию многостороннего, прозрачного и демократического международного управления интернетом.

Предлагаемый Российской Федерацией проект Конвенции о международной информационной безопасности рассматривался в рамках различных международных форумов. При всем разнообразии обсуждаемых аспектов проекта Конвенции два оказались основными. Первый аспект был связан с проблемой соотношения проекта Конвенции и действующей Будапештской конвенции о киберпреступности. Второй аспект был связан с тем, что «возможность ограничений контента в рамках юрисдикции государств» может привести к «фрагментации регулирования» интернета и негативно повлиять на его трансграничное функционирование.

Инициативы Российской Федерации по вопросам информационной безопасности в рамках ООН, бесспорно, важны, но постановка этих вопросов в контексте проблематики управления интернетом в целом и формирования международно-правовой модели управления интернетом в частности была бы целесообразнее.

Становится очевидным то, что международное сотрудничество по вопросам информационных и коммуникационных технологий, и в частности по вопросам управления интернетом, может быть успешным в условиях политического компромисса и только с участием «всех заинтересованных сторон». Одним из примеров системного

[1] См.: URL: http://www.scrf.gov.ru/documents/6/112.html

аналитического исследования с участием «всех заинтересованных сторон» является опубликованное в 2013 г. Таллиннское руководство по международному праву, применимому в случае кибервойны (далее – Таллиннское руководство)[1]. Этот документ является итогом трехлетней работы международной группы экспертов, приглашенных Центром передового опыта НАТО по совместной защите от киберугроз, размещенным в столице Эстонии г. Таллинне[2]. Таллиннское руководство нельзя рассматривать как официальный документ ни упомянутого Центра, ни государств-членов, спонсировавших это исследование, ни собственно НАТО. Таллиннское руководство выражает точку зрения международной группы независимых экспертов, действующих исключительно в личном качестве, и является своеобразным подтверждением того, что практические шаги в вопросах управления интернетом на международно-правовом уровне невозможно решать без «участия всех заинтересованных сторон», в данном случае «экспертного сообщества». Ряд аналитиков, однако, уже поспешили назвать документ «руководством по ведению кибервойн», «легитимизацией милитаризации» киберпространства и т.п.[3]

Таллиннское руководство представляет собой обширный документ объемом более 300 страниц и вызывает практический интерес по нескольким причинам. Во-первых, кибербезопасность важна не сама по себе и ее нельзя рассматривать вне контекста управления интернетом в целом и формирования международной модели управления интернетом в частности. Иной подход понимания кибербезопасности может привести как минимум к полицентризму и фрагментации интернета в территориальных рамках национальной юрисдикции государств, может разрушить глобальную Сеть, став препятствием трансграничного функционирования интернета, а также к доминированию государств

[1] URL: http://www. Cambridge.org/9781107024434.

Центр передового опыта НАТО по совместной защите от киберугроз (*The NATO Cooperative Cyber Defence Center of Excellence*), г. Таллин (Эстония).

[2] Центр передового опыта НАТО по совместной защите от киберугроз (*The NATO Cooperative Cyber Defence Center of Excellence, CCDCOE*), называемый иногда Объединенным центром передового опыта в сфере кибернетической защиты, создан в 2008 году в г. Таллине (Эстония) в целях повышения эффективности взаимодействия стран НАТО и расширения их возможностей в сфере кибербезопасности, аккредитован при НАТО и имеет статус международной военной организации. В его компетенцию входит предоставление экспертных заключений по вопросам совместной кибернетической и информационной безопасности для НАТО и стран – членов НАТО.

[3] См. например, материалы: URL: http://www.3dnews.ru/643092; http://www.securitylab.ru/blog/personal/tsarev/29130.php и др. Взвешенная оценка документа дана А. Лукацким, доступно: http://lukatsky.blogspot.ru/2013/05/blog-post.html

в многосторонней модели управления интернетом. Во-вторых, Таллиннское руководство подготовлено на основе многих нормативно-правовых источников: международных договоров, документов международных межправительственных организаций, решений (прецедентов) международных трибуналов и судов, обычаев и принципов международного права. Вся упоминаемая нормативная база призвана ответить на основной вопрос: применимы ли нормы современного международного права, как обычные, так и конвенционные, к новым киберугрозам, киберконфликтам, кибервойнам, и если применимы, то каким образом? В самом общем плане Таллиннское руководство положительно отвечает на этот вопрос и формулирует правила, применимые в условиях киберконфликтов[1]. Положительный ответ на вопрос о применимости международного права к киберпространству, данный в Таллиннском руководстве, имеет важное значение и в связи с особенностью формирования принципов и норм международного права. Поэтому, в-третьих, следует сказать о принципе *opinio juris*. Убежденность в правомерности (*opinio juris*) для международного права – убеждение субъектов международного права в юридической полноценности (действительности) нормы права, означающее признание государством определенного правила в качестве нормы международного права – обычной или конвенционной. Любая норма международного права, независимо от ее источника и применяемой процедуры, проходит стадию выработки содержания правила, а затем стадию признания этого правила в качестве обязательной нормы международного права. При создании конвенционных норм *opinio juris* имеет явно выраженный характер, а при квалификации обычных норм в качестве норм обычного международного права – молчаливый характер. Отсюда следует, что при квалификации норм обычного международного права доказательство *opinio juris* непосредственно связывается с кодификацией международного обычного права, в процессе которой *opinio juris* получает явно выраженный характер[2]. Таллиннское руководство следует рассматривать именно в контексте «стремления к нормативной определенности» применимости нормы современного международного права к «киберугрозам».

Структурно Таллиннское руководство состоит из 95 правил, причем вначале формулируется конкретное правило (норма), содержание

[1] URL: http://www. Cambridge.org/9781107024434;

Центр передового опыта НАТО по совместной защите от киберугроз (*The NATO Cooperative Cyber Defence Center of Excellence*), г. Таллин (Эстония).

[2] См., например, материалы: http://mirslovarei.com/content_eco/opinio-juris-49850.html#ixzz2YSq1YaOd

которого разъясняется в соответствующих комментариях, включая интерпретацию применимости правил, с указанием на существовавшие разногласия, возникшие среди экспертов по тому или иному правилу.

Приведем в качестве примера правило 1, изложенное в разд. 1 «Суверенитет, юрисдикция и контроль» гл. 1 «Государство и киберпространство». Оно звучит так: «Государство может осуществлять контроль над киберинфраструктурой и за деятельностью в рамках своей суверенной территории». В последующих 14 пунктах раскрывается содержания указанного правила и даются, к примеру, следующие комментарии: «Несмотря на то, что ни одно государство не обладает суверенитетом над киберпространством как таковым (*per se*), государство обладает исключительными суверенными правами над объектами киберинфраструктуры, находящимися на его территории. Государственный суверенитет над киберинфраструктурой в пределах суверенной территории означает то, что, во-первых, государство осуществляет нормативно-правовой контроль над объектами киберинфртаструктуры; во-вторых, государство осуществляет территориально-суверенную защиту объектов киберинфраструктуры. При этом такой контроль и защита осуществляются вне зависимости от того, принадлежат ли такие объекты самому государству, частным организациям или индивидам, и вне зависимости от целей использования таких объектов». Основной единодушный вывод, сделанный группой экспертов в Таллиннском руководстве, – общие принципы и нормы международного права применимы к регулированию киберпространства.

6. Перспективы трансграничного управления интернетом после 2015 г.

Формирование управления Интернетом в «широком смысле» находится на начальном этапе своего развития. Возможность разработки проектов универсальных международно-правовых документов, связанных с управлением интернетом на глобальном уровне, по-видимому, может появиться в 2015–2017 гг., и отчасти основанием для такого прогноза является ряд причин. В числе одной из причин следует назвать то, что в 2015 г. планируется проведение третьего этапа Всемирной встречи на высшем уровне по вопросам информационного общества.

Существует как минимум еще две причины глобального характера. Во-первых, Декларация тысячелетия ООН, принятая резолюцией 55/2 Генеральной Ассамблеи от 8 сентября 2000 г., предусмотрела 18 задач

и 8 целей, которые все государства – члены ООН обязуются достичь к 2015 г.[1] В их числе – обязательства сформировать новое глобальное партнерство в целях развития, включающее использование информационных и коммуникационных технологий. Обсуждение итогов достижения целей и задач Декларации тысячелетия в 2015 г. так или иначе будет иметь отношение к проблемам использования информационных и коммуникационных технологий, а значит, и к проблематике управления интернетом. Во-вторых, в 2015 г. вступает в действие новая редакция Административного регламента международной электросвязи в редакции 2012 г., о котором говорилось выше. Правовым следствием неоднозначной оценки новой редакции Административного регламента международной электросвязи (редакция 2012 г.) в контексте управления интернетом является то, что целый ряд государств будут применять Административный регламент международной электросвязи в редакции 1988 г., что неизбежно вызовет многочисленные коллизии в части правоприменения.

Темпы развития общественных отношений в сфере информационных и коммуникационных отношений опережают их правовое регулирование и не исключено, что выявятся новые аспекты развития информационных технологий, которые потребуют внутригосударственного и международно-правового регулирования, но любые вопросы данной проблематики так или иначе будут связаны со сферой трансграничного управления интернетом. В настоящее время довольно сложно предположить, в каком контексте будет развиваться решение проблематики управления интернетом; вместе с тем можно очертить круг вопросов, которые так или иначе будут обсуждаться как на национальном, так и на международно-правовом уровне. Во-первых, это разработка международно-правовых гарантий безопасного использования интернета. В этом плане инициативы Российской Федерации по вопросам информационной безопасности могут быть востребованы мировым сообществом. Во-вторых, существуют различия в порядке и методах регулирования национальным правом использования сетевых технологий в противоправных целях. В настоящее время становится очевидной необходимость гармонизации национального законодательства в сфере, связанной с сотрудничеством правоохранительных органов разных государств, с проведением соответствующих следственных мероприятий, привлечением к ответственности виновных лиц и проч.

[1] См. подробнее об этом: URL: http://www.un.org/millennium/declaration/ares552e.htm, а также доклад Яна Вандемуртеля (*Jan Vandemoortele*): URL: http://www.wssinfo.org/fileadmin/user_upload/resources/DESA---post-2015-paper---Vandemoortele.pdf

Международное сотрудничество государств в сфере управления интернетом, несомненно, должно учитывать практику применения Будапештской конвенции Совета Европы по борьбе с киберпреступностью. В-третьих, это разработка правил, принципов и норм защиты критически важной инфраструктуры интернета на международном уровне с учетом трансграничного функционирования интернета. Такие правила, принципы и нормы должны быть связаны с обязательствами государств обеспечивать стабильность и устойчивость функционирования объектов сетевой инфраструктуры интернета на своей территории, и защиту такой инфраструктуры. В-четвертых, в ближайшее десятилетие проблема идентификации пользователей интернета, владельцев интернет-ресурсов и операторов интернет-услуг потребует своего решения, что в свою очередь обусловит необходимость если не создания глобальной системы идентификации в интернете, то разработки принципов взаимного признания национальных систем идентификации и определения основных направлений их формирования[1]. Наконец, в-пятых, потребуется дальнейшее совершенствование нормативно-правового регулирования порядка оказания трансграничных услуг интернет-компаниями, являющимися национальными юридическими лицами конкретных государств, например, таких как *Google, Facebook* и т.п. В настоящее время пользователями услуг подобных компаний являются сотни миллионов человек во всех странах мира. Для сохранения единства и стабильности трансграничного функционирования интернета необходима корреляция регулирования на национальном и международно-правовом уровне вопросов, связанных с юрисдикцией государств.

С учетом достаточно радикальных изменений как на рынке интернет-технологий, так и на международной политической арене в настоящее время довольно сложно предположить, каким образом будет развиваться международное сотрудничество государств в сфере управления интернетом. Развитие общественных отношений в сфере информационных и коммуникационных технологий опережает их правовое регулирование, и не исключено, что выявятся и иные вопросы развития информационных технологий, которые потребуют регулирования.

[1] Например, «Национальная стратегия идентификации в киберпространстве» США (*National Strategy for Trusted Identities in Cyberspace*), названная *Identity Ecosystem* (URL: http://habrahabr.ru/blogs/infosecurity/111631/), а также см. об этом: URL: http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

О.В. Демидов,
директор программы ПИР-Центра
«Международная информационная безопасность
и глобальное управление интернетом»

Международная безопасность в области использования ИКТ: глобальные тенденции и национальные интересы России

Российская повестка дня в сфере кибербезопасности: вехи прогресса и нерешенные проблемы

Несмотря на то, что в публикуемом сборнике акцент сделан на недавно принятых или предложенных документах и их проектах, обзор российской позиции в области обеспечения безопасности киберпространства или, говоря официальным языком МИД России, международной информационной безопасности (МИБ) невозможен без краткого анализа истории политики РФ в данной области.

Прежде всего необходимо подчеркнуть, что Российская Федерация очень рано, одной из первых в мире стран, всерьез озаботилась вопросами предотвращения и отражения угроз международной безопасности, связанных с использованием ИКТ.

Как отмечает в своей статье А.В. Крутских – специальный координатор МИД России по вопросам использования ИКТ в политических целях, «с 1998 г. Россия продвигает идею налаживания международного сотрудничества по укреплению МИБ», при этом с самого начала «работа по согласованию конкретных мер в интересах упрочения МИБ проводилась главным образом через механизм ООН»[1].

В течение ряда лет российской стороной на рассмотрение ГА ООН вносились проекты резолюций «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в которых содержались призывы к рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных мер по ограничению таковых угроз.

[1] *Крутских А.В.* К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. № 1 (13) (http://www.intertrends.ru/thirteen/003.htm (последнее посещение – 18 ноября 2013 г.)).

Первая из этих резолюций (A/RES/53/70) от 4 декабря 1998 г. была принята Генеральной Ассамблей без голосования, консенсусом[1]. Однако принятый текст резолюции не соответствовал изначальному варианту, который был направлен Генеральному секретарю ООН в письме от 23 сентября 1998 г. от постоянного представителя РФ при ООН министра иностранных дел России И.С. Иванова[2]. Уже на тот момент в приложенном к письму проекте резолюции были сформулированы ключевые цели, которые отечественная дипломатия пытается решить сегодня в рамках концепции Конвенции об обеспечении МИБ. Так, в проекте резолюции всем государствам – членам ООН предлагалось, в частности, информировать Генерального секретаря о своих взглядах на:

- использование информационных технологий в военных целях;
- определение понятий «информационное оружие» и «информационная война»;
- целесообразность строительства международно-правовых режимов с целью запрещения разработки особо опасных форм информационного оружия.

В итоговом варианте резолюции эти проблемы не были отражены. Несмотря на это, вносимые РФ резолюции принимались Генеральной Ассамблеей консенсусом в последующие годы вплоть до 2005 г.

Помимо усилий по внесению проектов резолюций на сессиях Генассамблеи ООН Россия активно использовала механизм Групп правительственных экспертов (ГПЭ) ООН для продвижения повестки МИБ. Впервые ГПЭ ООН была учреждена 8 декабря 2003 г. во исполнение резолюции ГА ООН от 29 ноября 2001 г. A/RES/56/19. Целью Группы была активизация международного рассмотрения существующих и потенциальных угроз в сфере информационной безопасности, возможных мер по ограничению таких угроз и изучение международных стратегий, направленных на укрепление безопасности глобальных

[1] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция, принятая Генеральной Ассамблеей A/RES/53/70 / Генеральная Ассамблея ООН. 4 января 1999 г. (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement (последнее посещение – 18 ноября 2013 г.)).

[2] См.: Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General. Role of science and technology in the context of international security, disarmament and other related fields. A/C.1/53/3 / United Nations General Assembly. 30 September 1998 (https://disarmament-library.un.org/UNODA/Library.nsf/1c90cfa42bbb0d6985257631004ff541/663e6453bdaa2e2285257650005502 77/$FILE/A-C1-53-3_russia.pdf (последнее посещение – 18 ноября 2013 г.)).

информационных и телекоммуникационных систем[1]. Первый проект доклада по итогам работы Группы был подготовлен в 2004 г., однако в изначальном виде не был принят консенсусом из-за серьезных разногласий между ее членами и, в частности, противодействия российскому подходу со стороны представителей США. В результате в 2005 г. удалось принять лишь процедурный доклад A/60/202, где констатировалось, что «с учетом сложного характера вопросов, о которых идет речь, не было достигнуто консенсуса относительно подготовки окончательного доклада»[2].

Противоречия между участниками ГПЭ касались прежде всего двух вопросов, имевших политическую окраску. Первый из них, принципиально важный для России, касался военно-политических аспектов ИКТ и влияния этих технологий на национальную безопасность и международный военно-политический баланс. Второе противоречие касалось вопроса о том, должны ли быть предметом рассмотрения Группы вопросы, связанные с содержанием информационных потоков, или же необходимо рассматривать лишь вопросы безопасности информационной инфраструктуры. Первую точку зрения можно с некоторыми оговорками назвать *российской*, вторую – *американской*. Один из конкретных вопросов в этой связи касался того, следует ли рассматривать передачу и распространение трансграничной информации через ИКТ-сети в качестве вопроса национальной безопасности и обеспечивать соответствующий контроль над ними.

Призыв к созданию следующей ГПЭ вновь прозвучал по инициативе России уже 8 декабря 2005 г., когда была принята очередная резолюция «Достижения в сфере информатизации...» (A/RES/60/45)[3].

По словам А.В. Крутских, возглавившего вторую ГПЭ, «несмотря на давление американской делегации», «российские предложения

[1] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция, принятая Генеральной Ассамблеей [по докладу Первого комитета (A/56/533)]. A/RES/56/19 / Генеральная Ассамблея ООН. 7 января 2002 г. (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf?OpenElement (последнее посещение – 18 ноября 2013 г.)).

[2] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: Доклад Генерального секретаря. A/60/202 / Генеральная Ассамблея ООН. 5 августа 2005 г. (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/453/65/PDF/N0545365.pdf?OpenElement (последнее посещение – 18 ноября 2013 г.)).

[3] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/RES/60/45 / Генеральная Ассамблея ООН. 6 января 2006 г. (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/490/32/PDF/N0549032.pdf?OpenElement (последнее посещение – 18 ноября 2013 г.)).

по вопросам МИБ поддержали Япония, Израиль, Южная Корея, Австралия и Канада»[1]. Группа из 15 экспертов – представителей стран была сформирована в 2009 г. и завершила свою деятельность в 2010 г. после серии из четырех сессий. В отличие от предыдущей ГПЭ итогом работы второй Группы стал принятый консенсусом и представленный на 65-й сессии Генеральной ассамблеи в июле 2010 г. доклад, который отразил некоторые ключевые вопросы и озабоченности российской стороны по поводу применения ИКТ в военно-политических целях. В частности, в докладе отмечалась опасность использования ИКТ «в целях создания угрозы международному миру и национальной безопасности»[2]. Кроме того, впервые в рамках ООН в документе было прямо отмечена угроза, связанная с разработкой государствами ИКТ в качестве инструментов ведения войны и разведки и для применения в политических целях. Наконец, в числе итоговых рекомендаций доклада фигурировал призыв к «принятию мер по укреплению доверия, обеспечению стабильности и уменьшению рисков в связи с последствиями государственного использования ИКТ, включая обмен мнениями стран по вопросу об использовании ИКТ в конфликтах»[3]. Таким образом, деятельность второй ГПЭ стала *прорывом* для России, сумевшей существенно продвинуть повестку дня в сфере ИКТ с учетом тех аспектов, которые являлись и до сих пор являются для нее центральными.

Очередная, третья по счету, ГПЭ была учреждена резолюцией Генассамблеи ООН от 2 декабря 2011 г. A/RES/66/24 с целью продолжить изучение существующих и потенциальных угроз в сфере информационной безопасности, а также возможных стратегий по рассмотрению таких угроз. Деятельность группы, в которую, как и в предыдущие ГПЭ, входят российские представители, включала три встречи. Первая из встреч Группы прошла 6–10 августа 2012 г. в Нью-Йорке, вторая – 14–18 января 2013 г. в Женеве, последняя встреча состоялась там же 3–7 июня 2013 г. 24 июня 2013 г. был принят консенсусом всех участников Группы доклад ГПЭ.

---

[1] *Крутских А.В.* Указ. соч.

[2] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/65/201. Записка Генерального секретаря / Генеральная Ассамблея ООН. 30 июля 2010 г. (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/469/59/PDF/N1046959.pdf?OpenElement (последнее посещение – 18 ноября 2013 г.)).

[3] Там же.

По сравнению с предыдущими докладами результат работы третьей ГПЭ выглядит гораздо более конкретным – вероятно, как следствие более узкой и практически ориентированной повестки дня Группы. В этот раз деятельность экспертов 15 стран была сфокусирована прежде всего на вопросах применения международного права «в отношении деятельности государств, связанной с использованием ИКТ»[1]. Все эксперты ГПЭ сошлись в положительном ответе на ключевой вопрос – согласно рекомендациям доклада, международное право применимо к деятельности в сфере использования ИКТ и самих ИКТ.

Одна из ключевых рекомендаций доклада сводится к необходимости «выработки общего понимания того, как нормы, основанные на положениях международного права, применяются к поведению государств и использованию государствами ИКТ»[2]. В докладе отмечается важная роль Устава ООН в поддержании мира и стабильности в информационной среде, а также подчеркивается, что принцип государственного суверенитета и вытекающие из него международные нормы и принципы распространяются на деятельность государств по использованию ИКТ, а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории.

Оценивая деятельность ГПЭ в целом, необходимо отметить, что она внесла большой вклад в продвижение проблематики ИКТ в контексте МИБ и в том числе российского видения этих вопросов. Любопытно, что с течением времени даже США перестали отрицать важность проблем, связанных с использованием ИКТ государствами в военно-политических целях. В докладе Генерального секретаря ООН от 15 июля 2011 г. (A/66/152), в ответе, полученном от Правительства США, среди мотивов деятельности, создающей угрозы работе глобальной сети и критических инфраструктур, упоминается «перенесение традиционных форм государственного конфликта в киберпространство»[3], а в число субъектов, создающих такие угрозы, включены государства.

---

[1] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/68/98 / Генеральная Ассамблея ООН. 24 июня 2013 г. (http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=http://www.un.org/disarmament/sgreports/68/&Lang=R (последнее посещение – 18 ноября 2013 г.)).

[2] Там же.

[3] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Доклад Генерального секретаря. A/66/152 / Генеральная Ассамблея ООН (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/416/93/PDF/N1141693.pdf?OpenElement (последнее посещение – 18 ноября 2013 г.)).

В том же докладе говорится, что «в ряде обстоятельств подрывная деятельность в киберпространстве может представлять собой вооруженное нападение»[1]. Вместе с тем Вашингтон по-прежнему отстаивает понимание проблем использования ИКТ прежде всего в плоскости безопасности информационной инфраструктуры и не рассматривает проблемы, связанные с контентом трансграничных информационных потоков в плоскости международной безопасности.

Кроме того, в контексте настоящей статьи немаловажно то, что дискуссии в ходе деятельности ГПЭ и обсуждения проектов вышеназванных резолюций позволили выработать некий вариант *нейтральной терминологии*. В тексте резолюций рассматриваемая проблематика формулируется вне рамок западной лексики кибербезопасности и, по большей части, не в терминах «обеспечения МИБ». Поиски участниками ГПЭ взаимоприемлемых формулировок с целью нахождения компромисса привели к тому, что тексты резолюций обращены к проблематике «ИКТ в контексте международной безопасности» – что корректно и нейтрально, хотя и довольно размыто, характеризует суть затрагиваемых вопросов. Потенциал использования официальной терминологии резолюций Генассамблеи ООН для сближения подходов РФ и ее зарубежных партнеров в настоящее время будет рассматриваться далее в данной статье.

Сегодня можно говорить о том что, несмотря на впечатляющую активность России в продвижении проблематики обеспечения МИБ за последние 15 лет, в 2011–2013 гг. усилия российской дипломатии вышли на принципиально новый уровень.

Подобная интегральная оценка распадается на три ключевые составляющие, из которых складывается прогресс российских регуляторов и дипломатов.

Первая из этих составляющих – выработка и активное продвижение на международной арене проектов международных документов, регулирующих глобальную политику в сфере использования ИКТ как за счет механизмов мягкого права, так и путем принятия юридически обязывающих конвенций ООН.

Ключевая инициатива в этом перечне – концепция Конвенции об обеспечении международной информационной безопасности (МИБ), представленная Россией международному сообществу два года

[1] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Доклад Генерального секретаря. A/66/152 / Генеральная Ассамблея ООН (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/416/93/PDF/N1141693.pdf?OpenElement (последнее посещение – 18 ноября 2013 г.)).

назад. Полноценная презентация документа прошла 1 ноября 2011 г. на первой международной Конференции по вопросам киберпространства в Лондоне. С речью, преимущественно посвященной концепции Конвенции, выступил И.О. Щеголев, на тот момент занимавший пост министра связи и массовых коммуникаций РФ. Незадолго до этого, 22 сентября 2011 г., документ был представлен главам спецслужб и силовых ведомств 52 стран на встрече в Екатеринбурге.

Представленный проект документа обладает рядом характеристик, которые позволяют считать его заявкой на серьезную международно-правовую новацию в плоскости регулирования ИКТ. Так, в числе прочего, концепция Конвенции[1]:

• претендует на всеобъемлющий характер и полный охват проблематики МИБ, предлагая принципы и меры для обеспечения комплексного предупреждения и противодействия всей *неделимой триаде угроз*, связанной с использованием ИКТ в области международной безопасности;

• должна в конечном счете через механизм ООН получить глобальный охват и распространить свое действие на все государства – члены ООН, т.е. де-факто на все международное сообщество;

• предполагает юридически обязывающий характер, не ограничиваясь декларативными заявлениями и формулированием общих принципов поведения государств в информационном пространстве;

• позиционируется не как жесткий завершенный механизм, а как «приглашение к диалогу» о соответствующем итоговом документе, который после доработки может превратиться в действующий международно-правовой инструмент ООН уже в ближайшие годы.

В рамках работы по последнему из перечисленных пунктов российский МИД и другие государственные органы предпринимают практические усилия по доработке текста концепции Конвенции с учетом отзывов экспертов и наиболее веских пунктов критики со стороны зарубежных партнеров. Такая работа в настоящее время ведется по большей части на площадке Совета Безопасности РФ. В частности, текст концепции Конвенции, перспективы его доработки и ключевые критические отзывы в адрес документа обсуждались 6–8 июня 2012 г. на третьей международной встрече высоких представителей, курирующих вопросы безопасности, в Санкт-Петербурге. По итогам встречи не было разработано нового окончательного варианта текста,

[1] Конвенция об обеспечении международной информационной безопасности (концепция) / Совет Безопасности РФ (http://www.scrf.gov.ru/documents/6/112.html (последнее посещение – 18 ноября 2013 г.)).

однако были учтены отдельные критические замечания и было принято решение продолжить работу в этом направлении. В преддверии мероприятия секретарь Совбеза Н.П. Патрушев отметил, что задача РФ состоит в том, чтобы сделать приемлемыми заложенные в концепции Конвенции правила «для большинства государств на начальном этапе», для того чтобы на конечном этапе обеспечить их принятие «в целом, в мире»[1].

Чуть ранее, 12 сентября 2011 г., Генеральному секретарю ООН было направлено письмо от Постоянных представителей в ООН четырех государств ШОС – России, Китая, Узбекистана и Таджикистана[2]. К письму прилагался проект Правил поведения в области обеспечения международной информационной безопасности. В отличие от концепции Конвенции Правила не носят юридически обязывающего характера, но в целом воспроизводят проблематику концепции Конвенции, хотя и без столь явного упора на военно-политическую составляющую информационной безопасности.

Вторая область, где Россия хорошо и значимо – как для себя, так и глобально – продвинулась вперед за последние два года – двустороннее сотрудничество по проблематике международной безопасности в области использования ИКТ.

Двусторонний трэк лишь недавно выдвинулся в число российских приоритетов в области обеспечения МИБ, а точнее вернулся в их перечень после того, как в уже упомянутом 1998 г. попытки работы в этом направлении в двустороннем формате с Вашингтоном дали отрицательный результат.

Тогда параллельно с включением России в разработку проектов резолюций ГА ООН по обеспечению МИБ стартовало российско-американское обсуждение этой проблематики. Его первым итогом стало *Совместное российско-американское заявление об общих вызовах безопасности на рубеже XXI века*, которое 2 сентября 1998 г. подписали президенты двух стран[3]. Но на том этапе добиться существенных

[1] РФ представит Совбезу ООН конвенцию по *IT*-безопасности: Проект РИА Новости *Digit*. 5 июня 2012 г. (http://digit.ru/state/20120605/392334876.html (последнее посещение – 18 ноября 2013 г.)).

[2] Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при ООН от 12 сентября 2011 г. на имя Генерального секретаря. A/66/359 / Генеральная Ассамблея ООН (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement (последнее посещение – 18 ноября 2013 г.)).

[3] Text: Common Security Challenges at Threshold of the 21st Century. USIS Washington File. 1998. September 2 ((последнее посещение – 18 ноября 2013 г.)).

успехов не удалось. «Ослабление действия негативных аспектов информационной технологии» признавалось в совместном заявлении «серьезной задачей в деле обеспечения стратегических интересов безопасности наших двух стран в будущем», однако документ не предлагал четкой программы международного сотрудничества. Основные акценты в заявлении были расставлены вокруг частной, хотя и актуальной на тот момент проблемы совместного преодоления «проблемы-2000», связанной со сменой компьютерных кодировок с наступлением новой календарной даты.

И хотя сам факт появления совместного заявления стал существенным шагом для признания проблематики МИБ как важной составляющей двусторонних отношений России и США, этого изначального импульса не хватило для вывода Москвы и Вашингтона на устойчивый диалог и сотрудничество. Позднее, по мере смены политической конъюнктуры и активного развития в США доктринального мышления в области стратегического и военного использования киберпространства, общая повестка дня стала выглядеть и вовсе исчерпанной.

Должное развитие этот трэк получил лишь спустя 13 лет, уже после того как мир увидел *Stuxnet*, мировой рынок киберпреступности стал измеряться многими миллиардами долларов США, а китайский кибершпионаж стал рассматриваться в качестве одной из приоритетных угроз национальной безопасности США. 28 июня 2011 г. было опубликовано совместное заявление заместителя Секретаря Совета Безопасности Российской Федерации Н.В. Климашина и координатора Белого дома по кибербезопасности Говарда Шмидта[1]. В совместном заявлении сторон упоминались такие перспективные форматы двустороннего сотрудничества, как регулярные обмены информацией между национальными *CERT*-центрами, а также обмен информацией по вопросам кибербезопасности по горячим линиям связи Москва – Вашингтон.

Потребовалось еще два года, чтобы достичь соглашения об этих мерах доверия в киберпространстве. Примечательно, что камнем преткновения все это время была терминология, за которой, конечно, скрывались концептуальные расхождения. Российская сторона настаивала на выстраивании текста соглашений вокруг понятия «угроз,

[1] Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin "U.S. and Russian Delegations Meet to Discuss Confidence-Building Measures in Cyberspace". The White House Official Website. June 2011 (http://www.whitehouse.gov/sites/default/files/uploads/2011_klimashin_schmidt_cyber_joint_statement.pdf (последнее посещение – 18 ноября 2013 г.)).

связанных с использованием информационно-коммуникационных технологий», тогда как американские партнеры усматривали в этой формулировке предлог к регулированию контента интернет-коммуникаций. В итоге стороны согласились на российской формулировке, достигнув консенсуса в том, что она не предполагает регулирования контента и цензуры интернет-коммуникаций, а лишь отражает позицию, согласно которой регулированию и запрещению подлежат не сами по себе технологии, а их использование в противоправных целях.

Пакет из трех соглашений был подписан в ходе встречи В.В. Путина и Барака Обамы на полях саммита *G8* в Дублине, Ирландия, 17 июня 2013 г.; подписание их сопровождалось совместным заявлением президентов двух стран, текст которого приводится в настоящем сборнике[1].

В рамках заключенных соглашений предполагается реализация ряда мер доверия в области использования ИКТ и прежде всего организация оперативного обмена данными через каналы национальных центров реагирования на компьютерные инциденты (*CERT*). Такой обмен направлен на предупреждение угроз «критически важной информационной инфраструктуре»[2]. Более примечателен еще один канал обмена информацией, прописанный в соглашениях, а именно российский и американский Центры по уменьшению ядерной опасности (НЦУЯО), посредством которых предполагается вести обмен сведениями, «которые могут снизить риск недопонимания, эскалации и конфликта».

Здесь уместно напомнить о том, что упомянутые центры изначально создавались в 1987 г. как часть политики разрядки в отношениях двух сверхдержав в эпоху М.С. Горбачева. И в конце биполярной эпохи, и после нее НЦУЯО выступали неким символом, *артефактом* стратегического партнерства России и США в критически важных для всего мира областях международной безопасности. В этой связи решение адаптировать их к задачам обмена срочными сообщениями о киберинцидентах можно рассматривать не только с практической точки зрения, но и как стремление подчеркнуть преемственность роли и зна-

[1] Совместное заявление президентов РФ и США о новой области сотрудничества в укреплении доверия // Официальный сайт Президента России. 17 июня 2013 г. (http://kremlin.ru/ref_notes/1479 (последнее посещение – 18 ноября 2013 г.)).

[2] См., например: Fadi Chehadé's Opening Speech, IGF 2013 // ICANN Website. 21 October 2013 (http://www.icann.org/en/news/presentations/chehade-speech-igf-bali-21oct13-en.pdf (последнее посещение – 18 ноября 2013 г.)); Fadi Chehadé Speaks at the 2013 IGF // ICANN Website. 5 November 2013 (http://www.icann.org/en/about/learning/podcasts/podcast-chehade-igf-bali-05nov13-en.htm (последнее посещение – 18 ноября 2013 г.)).

чимости вопросов кибербезопасности в повестке дня стратегического партнерства двух военных сверхдержав. Косвенным образом в пользу этого взгляда на использование НЦУЯО можно интерпретировать слова министра иностранных дел РФ С.В. Лаврова, произнесенные в ходе саммита АТЭС в Бали в октябре 2013 г.: «Настало время адаптировать их (НЦУЯО. – *О.Д.*) деятельность к нынешним реалиям»[1].

Наконец, третьим ключевым элементом соглашений стало создание устойчивого контакта между должностными лицами высокого уровня через организацию линии прямой связи по вопросам урегулирования потенциально опасных ситуаций в сфере использования ИКТ. Для этого в рамках Президентской комиссии РФ – США создается двусторонняя рабочая группа по вопросам угроз в сфере использования ИКТ и самим ИКТ в контексте международной безопасности. С российской стороны такую группу возглавил заместитель секретаря Совета Безопасности РФ Н.В. Климашин.

Подписанные соглашения можно считать прорывом в российско-американском сотрудничестве по вопросам киберпространства. Тем более любопытен тот факт, что их подписание произошло на фоне ясной нисходящей динамики в российско-американских отношениях. И особый интерес вызывает их судьба в данный момент – станет ли наметившееся двустороннее укрепление доверия жертвой российской реакции на разоблачения Эдварда Сноудена? Очень хотелось бы получить ответ «нет», учитывая потенциальную значимость такого сотрудничеств для глобальной безопасности.

За последние два года Россия проделала впечатляющий путь в части оформления и развития своего подхода к вопросам информационной безопасности (и де-факто включенной в нее кибербезопасности) на уровне национального, внутреннего законодательства.

Один из ключевых шагов в этом направлении был сделан совсем недавно и, опять же, являлся частью процесса кристаллизации российской концепции обеспечения международной информационной безопасности. Речь идет об «Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года»[2] (2013 г.) – доктринальном документе, впервые сводящем воедино российские инициативы и направления

[1] Лавров и Керри подписали соглашение о национальных центрах по уменьшению ядерной опасности // ИТАР ТАСС. 7 октября 2013 г. (http://www.itar-tass.com/politika/686923 (последнее посещение – 18 ноября 2013 г.)).

[2] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года / Совет Безопасности РФ (http://www.scrf.gov.ru/documents/6/114.html (последнее посещение – 18 ноября 2013 г.)).

деятельности по обеспечению МИБ. Появление этого продукта коллективного труда ряда российских ведомств под началом Совбеза РФ следует считать важной вехой во внутренней эволюции российского курса.

Во-первых, «Основы государственной политики...» систематизируют и упорядочивают доселе активную, но разнонаправленную деятельность России на международной арене по вопросам МИБ. До настоящего времени было не до конца ясно, как соотносятся между собой различные вышеперечисленные российские инициативы глобального уровня, а также региональный и двусторонний трэки, включая российско-американский. Что приоритетнее и должно быть реализовано в первую очередь, как согласовывается межведомственная работа по подготовке проектов юридически обязывающих документов и инструментов мягкого права? «Основы государственной политики...» действительно сводят все эти направления в единую упорядоченную иерархию и представляют первую в своем роде *матрицу* российской внешней политики по вопросам международной безопасности в области использования ИКТ.

Вместе с тем новый документ не следует считать прямым ответом и аналогом Международной стратегии для киберпространства США от 2011 г., прежде всего по той причине, что американская Стратегия наряду с вопросами безопасности охватывает гораздо более широкий круг вопросов с упором на свободу в интернете, экономическую функцию ИКТ и личную безопасность пользователей. Российские «Основы государственной политики...» – куда более узко сфокусированный документ, от которого неуместно было бы ждать как параграфов о роли интернета в обеспечении гражданских прав и свобод, так и параметров возможного военного ответа российских Вооруженных Сил (ВС) в случае международного конфликта в киберпространстве.

Для подобного рода норм в РФ предусмотрены отдельные документы, разработкой которых занимается прежде всего Минобороны России, которое в последнее время также резко активизировало работу по формированию видения своих задач в киберпространстве. В частности, начиная с 2012 г. в открытом доступе появились проекты новых доктринальных документов по вопросам роли ИКТ в военных конфликтах, активизировалась экспертная и ведомственная дискуссия о терминологии и подходе российских ВС в этой области.

В январе 2012 г. в открытом доступе появился документ оборонного ведомства под витиеватым названием ««Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в ин-

формационном пространстве» – по сути, первый прообраз доктрины действий ВС РФ в условиях современной информационной войны. В «Концептуальных взглядах...» отражен болезненный для России опыт *Пятидневной войны* в августе 2008 г., из которой военные постарались вынести определенные уроки, например как избежать имиджевого и информационного фиаско на фоне успешного решения непосредственных боевых задач.

В рамках решения задач по предотвращению конфликтов в информационном пространстве в «Концептуальных взглядах...» предлагается «публично, объективно и своевременно разъяснять мировой общественности причины и истоки конфликта»[1]. Отмечается, что такие меры позволяют создать в «глобальном информационном пространстве» климат, который бы удерживал «организаторов конфликта» от его дальнейшей эскалации. Авторы «Концептуальных взглядов...» отмечают важную роль информационной работы непосредственно в ходе конфликта. В частности, постоянное информирование СМИ и работа с общественным мнением в ходе конфликтной ситуации призваны «эффективнее влиять на ее деэскалационное развитие»[2]. Появление подобных наработок говорит о том, что российские силовые структуры начали активно восполнять тот пробел, который существовал ранее в теоретическом осмыслении информационной войны применительно к спектру задач вооруженных сил. Документ приводится в настоящем сборнике, и хотя он не был принят в качестве официального документа Минобороны, он представляется весьма интересным для изучения – как едва ли не первая попытка проработать новую сферу задач и приоритетов российских ВС (надо сказать, уже давно назревшая).

Однако работа над военно-стратегической повесткой дня в киберпространстве в России уже далеко не ограничена доктринальными и теоретическими аспектами, равно как и не ограничена она *внешнеполитической* проблематикой. Вопросы обеспечения национальной безопасности РФ в киберпространстве решаются и на институциональном уровне, в том числе в части кибероборонe.

В марте 2012 г. Дмитрий Рогозин, незадолго до этого назначенный вице-премьером РФ и куратором отечественного оборонного комплекса, объявил о скором создании в России собственного ки-

[1] Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве // Официальный сайт Министерства обороны РФ. 2011 г. (http://function.mil.ru/news_page/country/more.htm?id=10845074@cmsArticle (последнее посещение – 18 ноября 2013 г.)).

[2] Там же.

беркомандования[1], причем за образец для последнего предлагается взять именно *U.S. CYBERCOM*, что будет означать частичный отход от двух важных тенденций прежних лет. Первая – приоритет угроз, связанных с социально-политическими аспектами «информационной войны», т.е. угроз, связанных с контентом, при значительном отставании в оценке угроз безопасности компьютерных сетей и управляющих систем, т.е. кибербезопасности в узком смысле слова. Вторая тенденция – доминирование в вопросах информационной безопасности спецслужб (ФСБ, ФСО, ФСТЭК), притом что в число приоритетных задач Минобороны эти вопросы ранее не включались.

Последняя тенденция, впрочем, скорее развивается в сторону более или менее четкого разделения сфер ответственности с Минобороны, притом что защита гражданских объектов остается за спецслужбами. Важной вехой в этой области стал Указ Президента РФ от 15 января 2013 г. № 31с, текст которого приводится в настоящем сборнике[2]. Указ, который многие эксперты считают одной из ключевых вех в формировании российского внутригосударственного подхода к вопросам обеспечения кибербезопасности, возлагает на ФСБ России создание «государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

То есть впервые в РФ определяется ведомство, которое будет выстраивать систему обеспечения кибербезопасности общенационального масштаба, хотя за бортом ее пока остаются сети и системы частных пользователей и бизнеса. Так или иначе Указ свидетельствует о том, что по крайней мере на внутреннем уровне Россия вступает в этап консолидации своих усилий и политик в сфере кибербезопасности, – от решения точечных задач внутригосударственная повестка дня окончательно сместилась в плоскость интегральных, системных решений. Явно отрицательным симптомом в этой части выглядит лишь непропорционально слабое влияние частного сектора и экспертного сообщества на государственную и ведомственную политику. Впрочем, для российской повестки дня в сфере ИКТ эта проблема никак не является новой.

[1] В российской армии может появиться киберкомандование, заявил Рогозин // РИА Новости. 21 марта 2013 г. (http://ria.ru/defense_safety/20120321/601798789.html (последнее посещение – 18 ноября 2013 г.)).

[2] См. также: Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Интернет-портал «Российской газеты». 18 января 2013 г. (http://www.rg.ru/2013/01/18/komp-ataki-site-dok.html (последнее посещение – 18 ноября 2013 г.)).

В то же время инициатива конца 2012 г. по разработке концепции российской Стратегии кибербезопасности, выдвинутая и курируемая членом Совета Федерации РФ Р.У. Гаттаровым, являет пример активного вовлечения неправительственных экспертов в обсуждение и согласование доктринальных подходов в сфере кибербезопасности. С самого начала работы над проектом концепции Стратегии к консультациям привлекались эксперты Российской ассоциации электронных коммуникаций (РАЭК), представители ИБ-сектора, академического сообщества и других структур. До конца 2013 г. пройдут парламентские слушания по проекту документа, после чего он может быть направлен для комментариев и доработки в российские ведомства. Проблема, однако, состоит в том, что Совет Федерации ФС РФ как площадка не обладает достаточными компетенциями и влиянием для самостоятельного определения подходов в области информационной безопасности. По этой причине дальнейшее будущее прорабатываемого сейчас документа не выглядит в достаточной степени определенным, а сам он не слишком «рифмуется» с международными инициативами МИД России в области МИБ или тенденциями в сфере кибероборонны в России.

Адаптация международного права к киберпространству: опыт Таллиннского руководства и российские подходы

19 марта 2013 г. Центром совместной кибероборонны НАТО в Таллинне, Эстония (*CCD COE*), был опубликован окончательный вариант Таллиннского руководства по вопросам применения международного права к условиям конфликтов в киберпространстве[1]. Речь идет о почти 300-страничном документе, подготовленном группой экспертов Центра в результате трехлетней работы по обозначенным в документе вопросам. Несмотря на то, что Таллиннское руководство пока не имеет никакого официального статуса и неизвестно, получит ли оно такой статус в будущем, его появление вызвало бурный интерес как в самих странах НАТО, так и в РФ. Документ привлек к себе всеобщее внимание прежде всего в силу отдельных положений, вызвавших дискуссии в связи со своим новаторским с точки зрения международного права характером.

Положения Таллиннского руководства при определенных условиях санкционируют применение неограниченно широкого спектра кине-

[1] См.: *Michael N. Schmitt*. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2013.

тического оружия против источника киберугрозы, силовые действия военных в отношении гражданских лиц, причастных к кибератакам (за счет причисления их к статусу комбатантов), а также военные кибероперации, направленные против критической инфраструктуры, включая АЭС и дамбы плотин. Наличие подобных положений, основанных на далеко не единогласном консенсусе авторов документа, дает основание ряду экспертов и дипломатов различных стран утверждать, что Таллиннское руководство дает государствам международно-правовую базу для ведения наступательной кибервойны. То есть в тексте документа усматривается попытка легитимизации конфликтов в киберпространстве как формы поведения государств и действующих в их интересах посредников (англ. *proxy actors*) на мировой арене.

В частности, подобные соображения высказывались представителями российских Минобороны и Министерства иностранных дел, а также Генштаба ВС РФ и некоторыми авторитетными отечественными экспертами в вопросах кибероборонны в ходе круглого стола «*Новые рекомендации НАТО по войне в киберпространстве: приглашение к диалогу или провокация? Международные оценки и взгляд из России*», который прошел 31 мая 2013 г. в Москве[1]. Также участники дискуссии охарактеризовали документ как «катехизис по ведению информационных войн»[2]. Любопытно, что такая позиция в отношении Таллиннского руководства вызывает довольно острый интерес и ряд вопросов среди зарубежных и прежде всего западноевропейских экспертов.

Не претендуя на подробный анализ и окончательный характер оценок, хотелось бы сформулировать ряд кратких комментариев по ключевым вопросам, которые ставит этот документ перед Россией и международным сообществом.

Во-первых, Таллиннское руководство представляет собой первую серьезную попытку заполнить международно-правовой вакуум в части формулирования правил поведения государств как непосредственных участников конфликтов в киберпространстве. С этой точки зрения, речь идет о заделе на будущее, в отсутствие которого потенциально возможный конфликт в киберпространстве может столкнуть международную систему в ситуацию дезориентации, непропорциональной и неадекватной реакции на действия противоборствующей стороны. Не нужно специально пояснять, что подобная ситуация чревата не-

[1] См. подробнее: *Кранц Максим*. «Таллинское руководство» – апология кибервойны? // Портал ИнфоШОС. 4 июня 2013 г. (http://www.infoshos.ru/ru/?idn=11516 (последнее посещение – 18 ноября 2013 г.)).

[2] Там же.

управляемой эскалацией конфликта и его перетеканием из киберпространства в плоскость вооруженных столкновений.

Во-вторых, при всей своей неоднозначности Таллиннское руководство не является попыткой произвольного нормотворчества и отталкивается от утвердившейся и бесспорно признаваемой мировым сообществом системы норм международного гуманитарного права (МГП) и права вооруженных конфликтов. Таким образом, сама идея, лежащая в основе документа, представляет собой шаг в правильном и нужном направлении. Вопросы возникают в отношении особенностей избранного подхода и частично обусловливаются международно-политической конъюнктурой, влияющей на интерпретацию выводов и положений документа.

В-третьих, вопреки часто звучащему мнению, Таллиннское руководство не может рассматриваться в качестве манифеста подхода, полностью противоположного российским инициативам, направленным на подчинение поведения государств в информационном пространстве своду универсальных правил и (или) норм. Разница между двумя подходами преувеличивается за счет того, что они рассматриваются через призму разных установок и задач. Как уже отмечалось, Россия и ее союзники видят свою миссию в запрещении и предотвращении межгосударственных конфликтов в информационном пространстве и выведении таких явлений за рамки приемлемых действий на международной арене. Таллиннское руководство – документ, не несущий такой задачи и отвечающий скорее на вопрос «Что делать?», если *гром все же грянул*, правила оказались нарушены и государства вместе с акторами-посредниками и другими субъектами уже втянуты в конфликт в киберпространстве.

Таким образом, российские дипломаты и эксперты *CCD COE* в Таллинне действительно работают на разную постановку задачи. Однако при этом их подходы не являются взаимоисключающими по своей сути. Женевские и Гаагские конвенции, от которых отталкиваются авторы Таллиннского документа, возникли в свое время именно потому, что войны между государствами тогда были частым и неизбежным явлением и в ситуации, когда их нельзя было прекратить как таковые, государства выработали *правила* их ведения с тем, чтобы ограничить жертвы мирного населения и ущерб от военных конфликтов, гуманизировать войну. Был бы возможен полный запрет агрессивной войны в 1945 г. без принятия ранее Женевских и Гаагских конвенций – большой вопрос.

В этой связи важно отметить, что положения российской концепции Конвенции об обеспечении МИБ от 2011 г. содержат прямую

ссылку на подход, лежащий в основе Таллиннского документа. Речь идет о п. 2 Статьи 7, согласно которому «в случае любого международного конфликта право государств-участников... выбирать методы или средства ведения «информационной войны» ограничено применимыми нормами международного гуманитарного права»[1].

Кроме того, идентичный по смыслу параграф содержится и в другом упомянутом документе: «Концептуальных взглядах...» российского Минобороны. В частности, документ предлагает Вооруженным Силам РФ руководствоваться такими нормами международного гуманитарного права, как «ограничение неизбирательного применения информационного оружия; установление особой защиты для информационных объектов, являющихся потенциально опасными источниками техногенных катастроф, а также запрещение вероломных методов ведения информационной войны»[2].

Проблема состоит в том, что ни одному из названных пунктов не сопутствует некая инструкция, которая расшифровывала бы его содержание. К примеру, неясно, какие именно объекты входят в перечень «потенциально опасных источников техногенных катастроф», что следует понимать мерами их «особой защиты», какие методы ведения информационной войны причисляются к «вероломным» и есть ли вообще такие методы, которые к вероломным не могут быть причислены? Речь идет скорее о манифесте, формулирующем очертания подхода российских ВС, но не несущем задачи наполнения его конкретным содержанием. Между тем время для этого явно пришло, что показал еще пресловутый *Stuxnet* в 2010 г.

Таллиннское руководство и есть подробная инструкция на этот самый случай, и может быть, руководству России и НАТО скорее следует задуматься над тем, как постепенно выработать возможность взаимного дополнения и усиления двух подходов – ведь друг без друга оба они грешат неполнотой и однобокостью. Таллиннское руководство, не будучи подкреплено какими-либо международными нормами, сдерживающими государства от кибервойн, действительно может восприниматься как средство легитимизации конфликтов в киберпространстве, укоренения их в систему международных отношений в XXI в. в качестве

[1] Конвенция об обеспечении международной информационной безопасности (концепция) // Совет Безопасности РФ (http://www.scrf.gov.ru/documents/6/112.html (последнее посещение – 18 ноября 2013 г.)).

[2] Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве // Официальный сайт Министерства обороны РФ. 2011 г. (http://function.mil.ru/news_page/country/more.htm?id=10845074@cmsArticle (последнее посещение – 18 ноября 2013 г.)).

допустимого средства решения внешних задач и обеспечения национальных интересов. Нужен балансир в виде международно-правовых ограничений, в духе которых действует и Россия. Однако в условиях мер верификации, неразрешимой с правовой точки зрения проблемы атрибуции и невероятно низкого технологического и ресурсного порога создания и применения кибероружия российские инициативы пока напоминают попытку удержать в руках воду. И поэтому они лишь выиграют, если вберут в себя корпус норм и правил, дающих ответ на вопрос «Что делать, если запрет все же нарушен?».

Однако надо отдавать себе отчет в том, что сближение и гармонизация двух подходов – задача на отдаленную перспективу, полагать иначе в условиях дефицита взаимного доверия по вопросам киберпространства между Россией и НАТО, Россией и США, тем более после ситуации вокруг Сноудена, было бы наивно. А вот запуск процесса наработки капитала доверия, начиная с обмена технической информацией, – достойная и крайне своевременная задача. К тому же она начала решаться на двустороннем уровне с подписанием рассмотренного выше совместного заявления президентов России и США о сотрудничестве в укреплении доверия в области ИКТ на полях саммита *G8* в Северной Ирландии 17 июня 2013 г. И если разоблачения программ АНБ и других западных спецслужб не перечеркнут российско-американское сотрудничество в этой области, можно надеяться на то, что встречное движение начнется и по вопросам о применении международного права к конфликтам в киберпространстве.

Осторожный оптимизм в этом смысле внушает вышеупомянутый доклад третьей ГПЭ ООН, одним из ключевых достижений которого является положительный консенсус правительственных экспертов по поводу применимости международного права к информационному пространству.

Отметим, что в докладе речь не идет о вопросах конфликтов в киберпространстве и собственно о международном гуманитарном праве, но этот контекст явно читается между строк документа. Учитывая накал дискуссий в предыдущих ГПЭ и обусловленную ими размытость формулировок прежних итоговых докладов, столь четкая констатация необходимости диалога, зафиксированная прежде всего представителями России и США, которые традиционно задают тон дискуссии в Группе, свидетельствует о значительном прогрессе. Вполне вероятно, что уже в рамках встреч четвертой ГПЭ в 2014 г. вопросы, охваченные ранее Таллиннским руководством, встанут ребром и на ее площадке,

что выведет дискуссию по ним на новый, заслуженный уровень максимально предметного рассмотрения.

В то же время нельзя не отметить, что сама Россия позиционирует работу по проблематике применения международного права к киберпространству и конфликта в киберпространстве как альтернативу и оппозицию Таллиннскому руководству. Например, в выступлении В.И. Ермакова, замдиректора Департамента по вопросам безопасности и разоружения МИД России, и.о. главы делегации РФ в Первом комитете 68-й сессии Генеральной Ассамблеи ООН от 30 октября 2013 г., в качестве «главного достижения доклада» третьей ГПЭ фокусируется не легитимизация, а предотвращение межгосударственных конфликтов в информационном пространстве[1]. Именно в «легитимизации» конфликтов в киберпространстве МИД России видит главный порок Таллиннского руководства, которое, с точки зрения российской дипломатии, не несет в себе ключевого посыла о принципиальной недопустимости кибервойн, зато активно вплетает правила их ведения в ткань международного права, да еще и с акцентом на проактивные операции в киберпространстве.

Позиция США по отношению к Таллиннскому руководству вызывает отдельный интерес. Мнение, согласно которому документ прямо отражает позицию США как ведущей кибердержавы, чью стратегию определяет принцип проактивных действий и глобальное доминирование в киберпространстве, довольно плохо соотносится с некоторыми положениями руководства. В частности, с параграфом документа *CCD COE* о том, что государства несут прямую ответственность в соответствии с международным правом за любые действия отдельных лиц или групп, которые действуют по его непосредственному указанию. К примеру, этот принцип явно противоречит усилиям Киберкомандования США по привлечению в свои ряды американских хакеров для решения задач национальной безопасности и кибероборонs, которые были озвучены главой Киберкома Китом Александером в августе 2013 г.

В то же время многие положения Таллиннского руководства, в частности норма о допустимости применения военной силы против гражданских хактивистов в том случае, если те «являются непосредственными участниками враждебных действий в киберпространстве», а также

[1] Выступление В.И. Ермакова, заместителя директора Департамента по вопросам безопасности и разоружения МИД России, и.о. главы делегации РФ в Первом комитете 68-й сессии ГА ООН. Нью-Йорк, 30 октября 2013 г. // Официальный интернет-портал ООН (http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_30-Oct_ODMIS_Russian-Fed-(R).pdf (последнее посещение – 18 ноября 2013 г.)).

возможности использования кинетических средств в ответ на кибератаки при определенных условиях, позволяют противодействовать группам и лицам, чью связь с военными структурами государства доказать весьма затруднительно. Подобный подход – своего рода палка о двух концах. Например, он мог бы позволить США активно бороться с хакерами Сирийской электронной армии, а также иранскими хакерами, чьи продвинутые и масштабные *DDoS*-атаки в первой половине 2013 г. немало досаждали *Wells Fargo* и другим американским банкам. Однако можно ли исключать интерпретацию возможных действий американских военных против сирийских хакеров на территории третьей страны из контекста нарушения ее государственного суверенитета? Едва ли – грань слишком тонка, и если в сегодняшнем случае атак американских беспилотников на членов Аль-Каиды в Йемене и боевиков Талибана в Пакистане некоторые правовые рамки удается имитировать при помощи негласных двусторонних соглашений с этими государствами, то в случае конфликта в киберпространстве с участием негосударственных акторов такой вариант исключен. Государство может вообще не знать и верить в то, что такие акторы находятся на его территории или используют его инфраструктуру для осуществления кибератак на США и их союзников, а сами акторы могут быстро менять страну пребывания (если это трансграничная группа злоумышленников, то вопрос вообще теряет смысл), а тем более инфраструктуру, которую используют для маршрутизации атак и запутывания своих следов. В подобных случаях активные действия в отношении таких субъектов на территории третьих стран ведут к непросчитываемым результатам, включая втягивание этих государств в конфликт в киберпространстве.

Кроме того, если сравнивать подход экспертов *CCD COE* с теми заявлениями, которые можно считать в той или иной мере отражающими позицию Вашингтона по этим вопросам, то бросается в глаза явная общность по многим позициям. Наиболее авторитетным на сегодняшний день источником, освещающим подход США к применению международного права к киберпространству, является конспект выступления советника по правовым вопросам Госдепартамента США Харольда Коха на межведомственной конференции Киберкома 28 сентября 2012 г. В ходе своего выступления Х. Кох сформулировал ряд ключевых вопросов касательно применения международного государственного права к конфликтам в киберпространстве и предложил ряд ответов на них[1].

[1] *Koh H.H.* International Law in Cyberspace. Remarks at USCYBERCOM Inter-Agency Legal Conference. September 28, 2012 // U.S.Department of State Official Website (http://www.state.gov/s/l/releases/remarks/197924.htm (последнее посещение – 18 ноября 2013 г.)).

В главных пунктах эти ответы практически полностью совпадают с выводами экспертов *CCD COE*. Кох соглашается с тем, что кибератаки при определенных условиях подпадают под понятие «применение силы» в рамках Статьи 2 (4) Устава ООН; так, под это определение с большой вероятностью попадает деятельность в киберпространстве, влекущая «гибель, ранения, или значительные разрушения»[1]. В то же время авторы Таллиннского руководства в Правилах 11 и 13 замыкают определение кибератак, подпадающих под понятие «использование силы», на другое понятие, а именно «вооруженное нападение» (*armed attack*). В итоге Международная экспертная группа условилась считать вооруженным нападением в киберпространстве любую деятельность, которая «ведет к гибели людей или повреждению имущества»[2], – почти дословно повторяя Х. Коха. Аналогичный консенсус наблюдается и по вопросу о том, может ли кибератака задействовать право государства на индивидуальную и коллективную самооборону согласно Статье 51 Устава ООН, – да, в том случае, если такая атака отвечает критериям вооруженного нападения или его непосредственной угрозы. Наконец, и эксперты *CCD COE* и Х. Кох сходятся в том, что государства несут ответственность за действия акторов-посредников (*proxy actors*) в ситуации конфликта в киберпространстве. Любопытно, что наряду с этим пунктом обе стороны по существу оставляют без ответа вопрос об атрибуции кибератак, осуществляемых такими посредниками.

Основное опасение, которое возникает при анализе Таллиннского руководства как возможного прообраза стратегии поведения НАТО в условиях конфликтов в киберпространстве, связано с тем, что заложенный в документе подход оставляет слишком широкое пространство для интерпретаций международного права. Таллиннское руководство – и это принципиальный момент – является не универсальной адаптацией норм международного гуманитарного права, а лишь их *прочтением* группой экспертов. Поскольку речь идет о специфичной реальности киберпространства, положения Таллиннского руководства оказываются довольно далеки от исходных норм МГП и права вооруженных конфликтов, а само их прочтение оказывается сильно подверженным интерпретации. Нет никакой гарантии, что в скором будущем США, осуществляя уже собственное прочтение междуна-

[1] Устав ООН. Глава I: Цели и принципы. Статья 2 // Официальный интернет-портал ООН (http://www.un.org/ru/documents/charter/chapter1.shtml (последнее посещение – 18 ноября 2013 г.)).

[2] *Michael N. Schmitt*. Tallinn Manual on the International Law applicable to Cyber Warfare. Cambridge University Press, 2013. P. 45–47, 54–60.

родных норм, аналогично таллиннским экспертам определят границу для использования военной силы в ответ на кибератаки, порог перехода гражданских хактивистов в статус комбатантов и легитимных целей на поле боя и т.д.

Характерным примером здесь является Правило 80 Таллиннского руководства, которое включает в число легитимных целей в условиях конфликта в киберпространстве такие объекты, как атомные электростанции, дамбы и плотины гидроэлектростанций, а также объекты, расположенные в непосредственной близости от упомянутых[1]. Возможность нанесения кибердударов по этим объектам оговаривается специально, а именно при соблюдении «особой осторожности» при планировании и осуществлении таких атак, которые могут быть направлены лишь на отключение, но не на разрушение таких объектов. Как несложно заметить, предлагаемые формулировки весьма хрупки и неочевидны с правовой точки зрения. Что означает «особая осторожность» для военных и каким образом можно полностью отключить АЭС, не создавая угрозу расплавления корпуса реактора или утечки радиации? А теперь представим, что какая-либо страна, разрабатывая собственный подход к правовым рамкам конфликта в киберпространстве, идет иным путем и логично вносит АЭС и дамбы в число объектов, кибератака на которые полностью запрещена и приравнивается к вооруженной агрессии. Тогда в случае конфликта с государством, придерживающимся подхода Таллиннского руководства, эта страна встанет на путь эскалации конфликта и ответит на такую кибератаку, например, ракетным ударом. При этом она полностью останется в рамках международного права, а точнее его собственного понимания, не унифицированного с подходами других государств. Разность трактовки неизбежно создает потенциал эскалации. А эксперты *CCD COE* не случайно разошлись между собой по вопросу о том, стоит ли считать применение *Stuxnet* против объектов атомной отрасли в Иране видом вооруженного нападения, дающим Тегерану право прибегнуть к самообороне в соответствии со Статьей 51 Устава ООН.

В заключение следует подчеркнуть, что, пожалуй, наиболее принципиальный вопрос применительно к Таллиннскому руководству состоит именно в значительной степени свободы прочтения существующих норм МГП, заложенной в самом его подходе. Подобная *свобода интерпретации* потенциально оставляет для каждого отдельно взятого государства слишком большой люфт, чтобы сделать его поведение

[1] *Michael N. Schmitt*. Tallinn Manual on the International Law applicable to Cyber Warfare. Cambridge University Press, 2013. С. 223.

в киберпространстве предсказуемым для остальных государств. Отсюда возникают вопросы: что станет следующим шагом после Таллиннского руководства и насколько четкий и единообразный свод правил будет создан в итоге и будет ли? Однако даже если страны НАТО пройдут весь путь и разработают собственный единогласно признаваемый и единообразно интерпретируемый вариант адаптации международного гуманитарного права для киберпространства, последуют ли ему на национальном уровне США? Поймут ли его Россия, Китай, Индия и еще 150 стран?

В результате мы возвращаемся к тому принципу, на котором строится российская позиция по вопросам МИБ, начиная с 1998 г., – приоритета глобальных соглашений или по крайней мере глобальных общих принципов поведения в киберпространстве (информационном пространстве), которые охватывали бы все мировое сообщество сразу. Необходимо признать, что в части выработки правил поведения в условиях конфликтов в киберпространстве их глобальный характер – то условие, без которого трудно надеяться на успех инициатив, подобных Таллиннскому руководству.

В то же время важно подчеркнуть, что значение Таллиннского руководства для международного права в самой России представляется явно недооцененным. И дело даже не в тех ответах, которые формулируют его авторы, но в самом факте подробной, детальной проработки ими вопросов применения МГП к кибервойнам и киберпространству. Единственный способ для России и любой другой страны и организации определиться с собственным пониманием этой проблематики – это «просканировать» каждую норму из существующего корпуса гуманитарного права на предмет того, как именно и с какими оговорками она должна применяться в любой потенциально возможной ситуации конфликта в киберпространстве. При этом совершенно не обязательно ориентироваться на логику и выводы авторов документа *CCD COE*, но саму работу, весьма кропотливую и объемную, проделать необходимо, иначе в споре по поводу формулирования такого подхода на глобальном уровне мы не имеем фактической аргументации и едва ли сможем отстоять свою точку зрения. Для укоренения на международном уровне той системы взглядов на эти вопросы, которая будет отвечать российским национальным интересам, явно недостаточно формулирования общих принципов применения МГП в киберпространстве, нужна конкретика и как можно скорее.

С одной стороны, такая постановка задачи уже прорабатывается Россией, как и ее партнерами, в рамках формирования мандата

для следующей, четвертой ГПЭ ООН. Так, в упомянутом выступлении замдиректора ДВБР МИД России В.И. Ермакова на 68-й сессии ГА ООН отмечается, что «новая ГПЭ могла бы детально проработать совокупность политико-правовых вопросов обеспечения МИБ», а также предлагается «расширить мандат ГПЭ» для проработки «вопросов использования ИКТ в конфликтах и того, как международное право применяется к действиям государств в информационном пространстве»[1].

С другой стороны, данный формат не отменяет сказанного выше, так как в формате консенсуса с 15 другими государствами может формулироваться общее понимание принципов применения МГП к конфликтам в киберпространстве, но не детальная адаптация корпуса международно-правовых норм. Эту работу, как представляется, Россия должна проделать самостоятельно (что совсем не исключает ее синергии с работой в рамках ГПЭ), с привлечением неправительственных экспертов и как можно скорее.

Национальные стратегии кибербезопасности: пусть цветут сто цветов

Еще одна область, в которой в 2011–2013 гг. имел место колоссальный прогресс, – разработка и принятие различными государствами доктринальных документов по вопросам безопасности в области ИКТ, включая прежде всего национальные стратегии кибербезопасности.

В последние годы стратегии кибербезопасности появляются по всему миру как грибы после дождя или как *сто цветов* в старой китайской мудрости. Начало процессу, безусловно, положило принятие США Международной стратегии по действиям в киберпространстве, опубликованной Белым домом 16 мая 2011 г. Ее логическим развитием в военной плоскости стала Стратегия Министерства обороны по действиям в киберпространстве, которая была частично рассекречена и опубликована в июне 2011 г. Принятие этих документов, а также их содержание показало, что проблематика интернета выходит на принципиально новый уровень в повестке Белого дома и в первую очередь в плоскости безопасности. Именно в Стратегии по действиям

[1] Выступление В.И. Ермакова, заместителя директора Департамента по вопросам безопасности и разоружения МИД России, и.о. главы делегации РФ в Первом комитете 68-й сессии ГА ООН. Нью-Йорк, 30 октября 2013 г. // Официальный интернет-портал ООН (http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_30-Oct_ODMIS_Russian-Fed-(R).pdf (последнее посещение – 18 ноября 2013 г.)).

в киберпространстве Министерства обороны США от 2011 г. впервые было сформулировано понимание киберпространства как пятой нефизической среды, являющейся оперативным пространством ВС США наряду с сушей, морем, воздухом и космосом[1]. Однако этот документ и так продолжительное время находился в фокусе международного внимания, а потому в рамках настоящего обзора хотелось бы также уделить внимание менее известным и изученным, по крайней мере в России, документам.

В феврале 2013 г. свою стратегию кибербезопасности принял Евросоюз. Один из любопытных моментов в тексте документа – проработка впервые в практике ЕС военных аспектов кибербезопасности и задач кибероборонны, которые оказываются вписаны в контекст Общей политики в области безопасности и обороны (*CSDP*) ЕС[2]. В этой области Брюссель вынужден начинать хоть и не с нуля, но из близкой к нему стартовой точки: в документе указывается, что наряду с формированием технологического потенциала европейской кибероборонны еще только предстоит сформировать ее доктринальное видение.

Другой любопытный аспект европейской стратегии в части военных аспектов кибербезопасности – разведение функций ЕС и НАТО, и в этой части документ оставляет гораздо меньше ясности. Несмотря на то, что необходимость избежать дублирования функций неоднократно подчеркивается в тексте стратегии, способы решения в ней не намечены либо не относятся к числу открытых составляющих европейской стратегии.

Также стоит отметить, что документ содержит подробно проработанный раздел по международному сотрудничеству в сфере обеспечения кибербезопасности. С точки зрения Брюсселя, который вряд ли станет легким союзником для России в сфере МИБ, одним из приоритетных задач объединенной Европы в киберпространстве является продвижение прав и свобод человека в сети. Соответствующий принцип закреплен в стратегии в качестве одного из основополагающих, в пояснении к нему отмечается, что «должный уровень кибербезопасности

[1] Department of Defense Strategy for Operating in Cyberspace. July 2011 // U.S. Department of Defense (http://www.defense.gov/news/d20110714cyber.pdf (последнее посещение – 18 ноября 2013 г.)).

[2] См. подробнее: Joint Communication to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace. Brussels, 7.2.2013 JOIN(2013) 1 final // European Union External Action Website. February 2013 (http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (последнее посещение – 18 ноября 2013 г.)).

и ее эффективность могут быть достигнуты только в том случае, если они опираются на фундаментальные права и свободы, перечисленные в Хартии ЕС по правам человека»[1]. Кроме того, расширение доступа к интернету как средство продвижения демократических реформ фигурирует как одна из составляющих международной политики ЕС в киберпространстве.

Особый интерес в свете российских инициатив в области МИБ имеют положения стратегии кибербезопасности ЕС, связанные с выработкой общих норм поведения для государств в киберпространстве. Необходимость таких норм отмечается в документе, но вместе с тем специально подчеркивается, что «ЕС не призывает к созданию новых международно-правовых инструментов для регулирования вопросов, связанных с киберпространством»[2].

Однако, наряду с признанием важности упомянутых стратегий Европы и США, нужно подчеркнуть, что деятельность по выработке и принятию стратегических документов, задающих вектор национальной политике в киберпространстве, отнюдь не ограничивается трансатлантическим сообществом – на эту площадку с каждым годом выходит все больше и больше игроков. Интерес к международно-политическим аспектам кибербезопасности, и в том числе доктринальным вопросам, сегодня быстро растет, например в Индии. Свидетельством этого процесса стала ускорившаяся в 2013 г. работа по формированию национальной индийской политики в области безопасности киберпространства.

Ключевой результат этой работы на сегодня – документ «Национальная политика в сфере кибербезопасности» (*National Cyber Security Policy*, *NCSP*), принятый индийским правительством 2 июля 2013 г.[3] По своей значимости документ является условным аналогом российских «Основ государственной политики в области международной информационной безопасности на период до 2020 г.», которые были подписаны Президентом РФ всего на месяц позже – в конце июля 2013 г. Любопытное

[1] Joint Communication to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace. Brussels, 7.2.2013 JOIN(2013) 1 final // European Union External Action Website. February 2013 (http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (последнее посещение – 18 ноября 2013 г.)).

[2] Там же.

[3] National Cyber Security Policy-2013. Department of Electronic and Information Technology. Ministry of Communications&Information Technology, Government of India. August 2013 (http://deity.gov.in/content/national-cyber-security-policy-2013-1 (последнее посещение – 18 ноября 2013 г.)).

и достаточно принципиальное различие кроется в том, что индийский документ полностью сконцентрирован именно на вопросах национального уровня и не включает в себя международную составляющую. Национальная стратегия кибербезопасности Индии, вбирающая в себя подобные глобальные аспекты, прорабатывается в настоящее время и *NCSP* – одна из основных составляющих ее фундамента, задающая ей направление.

Среди ключевых норм *NCSP* – создание государственного агентства, которое будет координировать повестку дня в сфере кибербезопасности в национальном масштабе, взаимодействуя с другими государственными органами и частным сектором. Кроме того, на *CERT-In* возлагается ответственность за реагирование и разрешение компьютерных инцидентов, а также кризис-менеджмент – опять же, в общегосударственном масштабе. Также документ предусматривает учреждение Национального центра защиты критической информационной инфраструктуры (*NCIPC*) и делегирование ему соответствующих полномочий, а также разработку национального плана защиты критической информационной инфраструктуры. Наконец, в документе прописано стимулирование введения во всех частных и государственных организациях страны единообразной позиции Директора по информационной безопасности (*CISO*), отвечающего за все соответствующие вопросы на организационном уровне в качестве контактного и координирующего лица.

Что касается международной повестки дня в киберпространстве, она, не найдя содержательного отражения в *NCSP*, встает во весь рост перед Индией следующим большим вопросом, решение которого является необходимым условием для выработки полноценной индийской стратегии кибербезопасности. Центральной темой для южно-азиатского гиганта становится выбор между институциональными и правовыми форматами международного сотрудничества в киберпространстве – как уже существующими, так и перспективными. Пока индийцы не определились с выбором формата международного сотрудничества в борьбе с трансграничной киберпреступностью, однако сейчас весьма активно приглядываются к Конвенции Совета Европы о компьютерных преступлениях 2001 г. – той самой Будапештской конвенции, которую последовательно критикует Россия. Российские дипломаты предпринимают попытки заострить внимание индийских коллег на альтернативах Будапештской конвенции и на ее устаревании. Однако до тех пор пока проект универсальной Конвенции ООН о борьбе с трансграничной киберпреступностью не представлен международной

общественности, подобная альтернатива остается достаточно плохо знакомой как минимум индийскому интернет-сообществу.

На этом фоне очевидным выглядит тезис о том, что сейчас, в переломный момент становления индийского подхода к кибербезопасности и международному сотрудничеству в киберпространстве, российское руководство нуждается в активизации диалога с Индией по вопросам МИБ – и активизация действительно происходит. Своевременным шагом стали прошедшие 21 октября 2013 г. в Москве переговоры российского Президента В.В. Путина с премьер-министром Индии Манмоханом Сингхом, которые обернулись существенным прогрессом по вопросам сотрудничества в области обеспечения МИБ. В ходе переговоров, а также прошедшего параллельно саммита по укреплению стратегического партнерства между Россией и Индией было принято заявление, п. 38 которого посвящен сотрудничеству в области обеспечения МИБ. В документе, в частности, отмечается «необходимость принятия универсальных правил, норм или принципов ответственного поведения государств при использовании ИКТ»[1]. Также предлагается ускорить работу над межправительственным российско-индийским соглашением о сотрудничестве в области обеспечения МИБ; наконец, отмечается важность невмешательства во внутренние дела, а также соблюдения прав человека в интернете.

Несмотря на многообещающий характер формулировок в совместном заявлении, его принятие не гарантирует качественного прорыва в двусторонних отношениях по вопросам сотрудничества в киберпространстве. Манмохан Сингх сам по себе не представляет ни экспертное сообщество Индии, ни индийский частный интернет-сектор, который обладает впечатляющими размерами и аккумулирует значительное влияние на процесс принятия политических решений. Дело в том, что позиции индийской стороны по данным вопросам, включая конкретно кибербезопасность, в значительной степени формулируются и отстаиваются с учетом позиции частного сектора, которая может и не совпадать с пунктами вышеназванного заявления.

Необходимо отметить, что индийский частный ИТ-бизнес с его валовым доходом порядка 100 млрд долл. в год и лишь домашним рынком в 160 млн пользователей, не говоря уже о внешних рынках сбыта, обладает весьма ощутимым влиянием на формирование государственной политики в этой области. Возможно, именно здесь кроется ответ

[1] Совместное заявление по итогам российско-индийского саммита // ИА *Regnum*. 21 октября 2013 г. (http://www.regnum.ru/news/1722435.html (последнее посещение – 18 ноября 2013 г.)).

на вопрос, почему Индия до недавних пор демонстрировала определенную пассивность в международно-политических и международно-правовых аспектах регулирования киберпространства.

Обеспечение кибербезопасности ранее было отдано на откуп частному сектору, который в Индии был локомотивом информатизации и использовал инструменты саморегулирования. В то же время правительство находилось в догоняющем положении, а в формировании активной международной позиции по этим вопросам до некоторых пор не было острой необходимости. Сейчас ситуация меняется, но индийцы по-прежнему видят роль частного сектора в обеспечении национальной кибербезопасности не просто как важную, а как главную. Поэтому в индийских условиях маловероятно принятие аналога Указа Президента РФ от 15 января 2013 г. № 31с. Речь скорее идет об иной постановке задачи: как правительству возложить создание общенациональной системы компьютерных сетей на частный бизнес на взаимоприемлемых условиях с возможным вовлечением государства в формате государственно-частных партнерств (ГЧП).

В заключение стоит привести небольшой пример, демонстрирующий вовлечение индийского частного сектора в обеспечение кибербезопасности на уровне всего общества. 13 октября 2013 г. индийские СМИ распространили информацию о том, что крупнейший промышленный холдинг страны *Reliance Industries Ltd* (*RIL)* займется созданием «*корпоративной вертикали кибербезопасности*», которая впоследствии может предлагаться другим игрокам индийского рынка в качестве комплексного организационного и технологического решения[1]. Это хороший пример того, как частная отрасль отзывается на государственные инициативы и самостоятельно воплощает их на практике, не забывая при этом о собственных интересах. В этом плане уже Россия могла бы кое-чему поучиться у своего стратегического партнера.

Трансформация глобального управления интернетом: меняющиеся контуры мультистейкхолдеризма

До последнего времени вопросы, связанные с глобальным управлением интернетом и моделями принятия решений и выработки политик управления Сетью, носили в основном технический харак-

[1] As govt gears up against digital attacks, Mukesh Ambani's RIL bets big on cyber security sector // The Economic Times. 13 October 2013 (http://articles.economictimes.indiatimes.com/2013-10-13/news/42993130_1_ril-cyber-security-sector-homeland-security (последнее посещение – 18 ноября 2013 г.)).

тер. Исчерпание резерва *IP*-адресов в рамках *IPv4* и старт глобального перехода на *IPv6*, развитие широкополосного доступа в странах развивающегося мира, применение *DNSSEC* и, конечно, развитие и применение программы новых доменов верхнего уровня (*nGTLDs*), включая, например, такие противоречивые случаи, как домен .xxx, – вокруг этих проблем ломались копья и разыгрывались определенные интриги, но правила игры в целом оставались незыблемыми. Примат мультистейкхолдерского подхода как единственного верного формата принятия глобальных решений в отношении Сети прочно утвердился после Женевского и Тунисского этапов ВВУИО в 2003 г. и, соответственно, 2005 г. и, казалось, уже вряд ли будет подвергаться сомнению. Напротив, решение Национальной администрации по телекоммуникациям и информатизации (*NTIA*) США от 2011 г. не пытаться оспорить решение Правления *ICANN* о создании доменной зоны *.xxx* вопреки воле Правительственной комиссии Корпорации (*GAC*) стало жестом, который показал самостоятельность мультистейкхолдерной площадки принятия решений Корпорации интернета.

Но уже в 2012 г. все начало меняться – изначально на фоне процесса подготовки крупного и весьма значимого мероприятия Международного союза электросвязи (МСЭ) – Всемирной конференции по международной электросвязи (ВКМЭ), которая состоялась в декабре 2012 г. в Дубае, ОАЭ. У этого мероприятия МСЭ был необычный повод – обновление и внесение изменений в один из ключевых документов организации – Регламент международной электросвязи (РМЭ). Этот документ является договором глобального уровня, объектами регулирования в рамках которого выступают такие вопросы, как:

- установление общих принципов, касающихся обеспечения и эксплуатации международной электросвязи;
- обеспечение глобальных присоединений и взаимодействия сетей электросвязи;
- поддержание гармоничного развития и эффективной эксплуатации технических средств;
- содействие повышению эффективности, полезности и доступности услуг международной электросвязи.

Важно отметить, что последний раз перед ВКМЭ-2012 Регламент обновлялся лишь в 1988 г., т.е. фактически до распространения в мире интернета в его современном виде. Именно бурное развитие глобальной сети послужило причиной очередного пересмотра РМЭ. Эта попытка обернулась бурными дебатами и в конечном счете формированием двух групп государств – участников конференции, которые

выступили с противоположными позициями по поводу предложенных поправок в Регламент.

Россия, Иран, Судан, Китай и ряд арабских государств Персидского залива сформировали и достаточно консолидированно продвигали в ходе конференции свод новаций, вводящих в Регламент понятие интернета, а также закреплявших за государствами «суверенитет в информационном пространстве» и право на суверенное участие в процессе глобального управления интернетом, включая управление системами *IP*-адресации и *DNS*[1]. Кроме того, общим моментом в инициативах спонтанно возникшей коалиции сторонников государственного суверенитета в Сети, направляемой прежде всего Россией, стало укрепление роли МСЭ в вопросах глобального управления интернетом, включая косвенно связанные с контентом вопросы, такие как борьба со спамом.

Эти инициативы спровоцировали жесткую критику как со стороны ключевых мультистейхолдерских площадок в сфере управления интернетом (*ISOC*, *IGF* и проч.), так и – в еще большей степени – со стороны США, Канады, Австралии и европейских государств. Эти страны, традиционно поддерживавшие концепцию мультистейкхолдеризма как единственно возможного механизма управления Сетью, обвинили Россию, Китай и их единомышленников в попытках выдавить частный сектор и само интернет-сообщество из процесса принятия глобальных решений по поводу управления интернетом. Концепция же государственного суверенитета «в национальном сегменте сети Интернет» была воспринята как способ легализации цензуры в Сети и ограничения свободы слова и доступа к информации. Также в качестве глубоко порочной была воспринята идея перенести процесс выработки политических решений в области управления интернетом на исторически нейтральную, *техническую* площадку МСЭ, который вообще имеет отношение к интернету лишь частично на уровне телекоммуникаций, но никак не на уровне программных приложений и тем более их контента.

Острота и масштаб противоречий между сторонниками этих двух расходящихся концепций достигли такого градуса, что в последний день ВКМЭ, 14 декабря 2012 г., был нарушен принцип принятия решений консенсусом на площадке МСЭ. Представители государств-участников были вынуждены в сжатые сроки прибегнуть к процедуре

[1] См. подробнее: Предложения, полученные от государств – членов МСЭ: Регламент международной электросвязи (РМЭ) // Официальный сайт Международного союза электросвязи. Декабрь 2012 г. (http://www.itu.int/md/dologin_md.asp?lang=en&id=S12-WCIT12-121203-TD-0001!!MSW-E (последнее посещение – 18 ноября 2013 г.)).

голосования по пакету предложений, выдвинутому Ираном и вобравшему ряд идей «реформаторов» РМЭ. Что интересно, к этому моменту наиболее радикальные предложения типа делегирования государствам суверенных прав в части управления системами *IP*-адресации и *DNS* уже были исключены из текста проекта обновленного Регламента. Наиболее серьезной новацией оставалась Статья 7, которая посвящена борьбе с «незапрашиваемыми электронными сообщениями» (т.е. спамом) и косвенно затрагивает вопросы контента интернет-коммуникаций вопреки обозначенному в тексте Регламента принципу[1].

В итоге 89 государств-участников проголосовали за обновленный Регламент международной электросвязи, еще 55 государств отказались проголосовать «за» и таким образом сохранили за собой право следовать прежней версии РМЭ от 1988 г. Некоторые страны, как, например, Индия, вообще воздержались от того, чтобы формулировать четкую позицию по этому вопросу. Индийцы не стали голосовать ни за, ни против проекта РМЭ. Вместо этого они взяли время подумать и до сих пор не сформулировали вообще никакой однозначной позиции, таким образом, проигнорировав всю эту историю и избежав необходимости записываться в одну из двух противоборствующих коалиций, сформировавшихся по итогам Конференции. Позицию Индии в этом смысле можно рассматривать как любопытный аналог «политики неприсоединения» в киберпространстве.

Однако таких «нейтральных стран» оказалось абсолютное меньшинство. Большая же часть международного сообщества оказалась поделена на два лагеря, которые журналисты и эксперты позиционировали как соответственно «сторонников свободы в интернете» и «адептов суверенитета и интернет-цензуры». Даже несмотря на тот факт, что внесенные в РМЭ поправки не имели принципиального характера, ряд западных экспертов охарактеризовал ВКМЭ-2012 как «цифровую холодную войну»[2] и «ялтинскую конференцию 2.0.»[3], подразумевая якобы стартовавший процесс передела контроля над интернетом в пользу России, Китая и других «авторитарных» государств развивающегося мира.

---

[1] Final Acts. World Conference on International Telecommunications (Dubai, 2012) // International Telecommunication Union Official Website. December 2012 (http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf (последнее посещение – 18 ноября 2013 г.)).

[2] A digital cold war? // The Economist. 14 December 2012 (http://www.economist.com/blogs/babbage/2012/12/internet-regulation (последнее посещение – 18 ноября 2013 г.)).

[3] *Klimburg A.* The Internet Yalta // Center for a New American Security. 3 February 2013 (http://www.cnas.org/files/documents/publications/CNAS_WCIT_commentary.pdf (последнее посещение – 18 ноября 2013 г.)).

Но, как показали дальнейшие дискуссии, включая Всемирный форум по политике в области электросвязи / ИКТ (ВФПЭ), прошедший 14–16 мая 2013 г. в Женеве, никакой долгосрочной и эффективной коалиции из государств, которые продвигали линию радикального реформирования РМЭ, так и не сложилось, хотя есть устойчивые «группы по интересам», такие как государства Персидского залива, Иран, Китай, ряд государств Африки, страны Центральной Азии и Россия.

Как следствие, не вышло и новой холодной войны, хотя концепция суверенитета государств в интернете по-прежнему прорабатывается этими и другими государствами как на национальном, так и на международном уровне. Неожиданный, но мощнейший импульс этой тенденции придали разоблачения Эдварда Сноудена, которые уже побудили многих технических экспертов и политических лидеров, включая президента Бразилии Дилму Роуссефф, призвать к пересмотру сложившейся системы глобального управления интернетом.

За короткий промежуток времени с июля 2013 г. американский перебежчик Эдвард Сноуден стал настоящей информационной бомбой, рассекретив колоссальные объемы информации о негласной деятельности США и некоторых других стран по осуществлению слежения и сбора данных в интернете и иных коммуникационных сетях. В их числе программа *Bullrun* – масштабный комплекс мер по обходу криптографической защиты в Сети, в рамках которого с 2000 г. АНБ и другие спецслужбы практикуют сотрудничество с разработчиками средств шифрования в США, в рамках которого разработчиков давлением или подкупом заставляют оставлять программные и аппаратных закладки (*backdoors*) в создаваемых ими продуктах для ИТ-сервисов, банков и других клиентов, в том числе иностранных[1]. Не менее громким разоблачением стало раскрытие практики слежения спецслужб США за платежами физических лиц по картам *VISA*, а также межбанковскими транзакциями через S*WIFT*: программа *Follow the money* и база данных «Тракфин». В 2011 г. в этой базе данных были накопле-

[1] См. подробнее: Revealed: how US and UK spy agencies defeat internet privacy and security / James Ball, Julian Borger, Glenn Greenwald // The Guardian. 6 September 2013 (http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (последнее посещение – 18 ноября 2013 г.)); Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security / Jeff Larson, Nicole Perlroth, Scott Shane. ProPublica. 5 September 2013 (http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption (последнее посещение – 18 ноября 2013 г.)); *Демидов О.* Десять разоблачений Сноудена, которые потрясли мир: как ответит Россия и ее партнеры // ПИР-Центр. 15 октября 2013 г. (http://pircenter.org/pages/83-russia-confidential-archive (последнее посещение – 18 ноября 2013 г.)).

ны записи по 180 млн операций, из них 84% – операции частных лиц по кредитным картам. АНБ как минимум с 2012 г. обеспечило себе доступ к сетям системы межбанковских транзакций *SWIFT*, через которую проходят 3 млрд операций в месяц[1].

Но, пожалуй, наиболее громкую общественную реакцию из всех разоблачений Сноудена вызвали масштабные программы электронного слежения АНБ США – *PRISM* и *XKeyscore*. *PRISM*, запущенная в 2007 г., позволяет скачать закрытую информацию с серверов интернет-гигантов США (включая *Microsoft, Yahoo!, Google, Facebook, AOL, Skype, YouTube, Apple* и *PalTal*)[2]. С помощью *PRISM* АНБ, ЦРУ и ФБР имеют доступ к данным частной *email*-переписки, видео- и голосовых чатов, видеозаписей, фото, хранимой на *HDD* информации, голосового трафика (*VoIP*), передаваемых через сеть файлов, онлайн-видеоконференций, введенных логинов и паролей, записей и действий в соцсетях и т.д. Также отслеживаются звонки абонентов крупнейших сотовых операторов США как внутри страны, так и по миру[3]. Аналогичным по широте функционалом располагала программа слежения *XKeyscore* – универсальное орудие поиска и анализа данных.

Отдельным пунктом разоблачений Сноудена стала слежка АНБ за коммерческими компаниями в Бразилии и других странах. АНБ систематически прослушивало телефонные звонки и просматривало электронную почту руководства бразильского нефтяного гиганта *Petróleo Brasileiro S.A. (PetroBras)*. В аналогичной ситуации оказался и американский гигант *Google*. Эпизод с *PetroBras* примечателен тем, что ломает основную *линию обороны* Белого Дома, – «мы вынуждены шпионить во имя святой цели – борьбы с международным терроризмом». Разъяренная Дилма Роуссефф справедливо и четко заметила, что

---

[1] "Follow the Money": NSA Spies on International Payments // Spiegel. September 15, 2013 (http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html (последнее посещение – 18 ноября 2013 г.)).

[2] «Следим строже, чем за русскими». Американская разведка призналась в сборе данных интернет-пользователей // Lenta.Ru. 10 июня 2013 г. (http://lenta.ru/articles/2013/06/10/bigbro/ (последнее посещение – 18 ноября 2013 г.)).

[3] О программах *PRISM* и X-Keyscore также см.:

U.S., company officials: Internet surveillance does not indiscriminately mine data / Robert O'Harrow Jr., Ellen Nakashima, Barton Gellman. The Washington Post. 8 June 2013 (http://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_story.html (последнее посещение – 18 ноября 2013 г.)).

NSA Prism program taps in to user data of Apple, Google and others / Glenn Greenwald, Ewen MacAskill. The Guardian. 6 June 2013 (http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (последнее посещение – 18 ноября 2013 г.)).

«*PetroBras* не является угрозой национальной безопасности какой-либо из стран»[1]. Зато в полной мере является стратегическим и крупнейшим частным активом бразильской экономики с капитализацией более 100 млрд долл., годовым валовым доходом в 144 млрд долл. и 80% всей национальной нефтедобычи[2]. И вот тут аргументы США заканчиваются, а американская позиция по вопросам поведения государств в интернете трещит по швам. Шпионаж за стратегическими экономическими объектами всегда подавался Вашингтоном как одно из главных *табу* и обвинений в адрес Пекина; во многом именно этой угрозой оправдывалось наращивание бюджета и штата Киберкомандования США и других подобных структур армии и спецслужб. С июля 2013 г. критика Пекина за кибершпионаж и кибератаки внезапно полностью прекратилась по вполне понятным причинам.

Однако для политических лидеров мира самым болезненным и неожиданным из числа разоблачений Сноудена стали вскрытые факты систематического слежения спецслужб США за ними самими. Например, достоянием общественности стала информация о многочисленных операциях АНБ и британской *GCHQ* по перехвату данных высокопоставленных иностранных чиновников и делегаций, в том числе перехват защищенной спутниковой связи с Москвой Д.А. Медведева из посольства РФ в Лондоне во время саммита *G20* в апреле 2009 г. Перехват осуществлялся со шпионской станции Менвит-Хилл, результаты неизвестны[3]. Тогда же производился признанный успешным взлом шифра смартфонов *BlackBerry* для прослушивания звонков участников *G20* и слежки за их перепиской. Для России в этом эпизоде нет ничего неожиданного, но ряд подобных операций осуществлялся в отношении многих делегаций, стран, посольств, включая те, что считают себя союзниками Вашингтона. Особенно неожиданной такая практика стала для стран Латинской Америки, включая Мексику и Бразилию,

[1] NSA spying on Petrobras, if proven, is industrial espionage: Rousseff. Anthony Boadle // Reuters. September 9, 2013 (последнее посещение – 18 ноября 2013 г.).

[2] См. подробнее:

PetroBras. Website Profile. An integrated energy company (http://www.petrobras.com.br/en/about-us/profile/ (последнее посещение – 18 ноября 2013 г.)).

Brazil oil auction forces Rousseff to reconsider Petrobras's role. Stephen Kurczy // The Christian Science Monitor. 23 October 2013 (http://www.csmonitor.com/World/Americas/2013/1023/Brazil-oil-auction-forces-Rousseff-to-reconsider-Petrobras-s-role (последнее посещение – 18 ноября 2013 г.)).

[3] G20 summit: NSA targeted Russian president Medvedev in London / Ewen MacAskill, Nick Davies, Nick Hopkins, Julian Borger, James Ball. The Guardian. June 17, 2013 (http://www.theguardian.com/world/2013/jun/16/nsa-dmitry-medvedev-g20-summit (последнее посещение – 18 ноября 2013 г.)).

президенты которых стали жертвами телефонного прослушивания и слежения за электронной почтой со стороны АНБ.

Постановка вопроса об отмене запланированной на октябрь 2013 г. встречи бразильского президента Дилмы Роуссефф с Бараком Обамой стала лишь началом активизации Бразилии в борьбе с нелегальным сбором данных в интернете и укреплением своей информационной безопасности. 24 сентября 2013 г. президент Бразилии выступила на открытии 68-й сессии ГА ООН, в которой пообещала, что Бразилия приложит все необходимые усилий для разработки национального законодательства и создания технологического потенциала, призванного защитить ее граждан и государственные структуры от иностранных программ перехвата персональных данных и шпионажа в интернете.

Стоит отметить, что к этому моменту в самой Бразилии прозвучали инициативы, созвучные предложениям членов российского Совета Федерации в июле 2013 г., а именно обязать транснациональные интернет-компании физически перенести серверы, на которых обрабатываются персональные данные граждан какого-либо государства, на территорию этого же государства[1]. Ставшая жертвой шпионских программ АНБ корпорация *PetroBras* пообещала вложить 10 млрд долл. в повышение уровня собственной информационной безопасности[2].

Кроме того, г-жа Роуссефф потребовала у ООН возглавить многосторонний процесс по выработке мер, направленных на предотвращение массового незаконного перехвата данных в Сети и «превращения киберпространства в поле битвы между государствами с использованием шпионажа, саботажа и атак на компьютерную инфраструктуру»[3]. Призвав ООН сыграть лидирующую роль в регулировании поведения государств в области ИКТ и использования интернета, г-жа Роуссефф по сути призвала к осуществлению реформы системы управления глобальной сетью в межгосударственном формате.

В начале ноября 2013 г. представители Бразилии и Германии направили ГА ООН совместный проект резолюции «Право на неприкосновенность частной жизни в цифровую эпоху», текст которого

[1] Brazil to insist on local Internet data storage after U.S. spying / Esteban Israel, Anthony Boadle. Yahoo! News. 29 October 2013 (http://news.yahoo.com/brazil-insist-local-internet-data-storage-u-spying-212255804--finance.html (последнее посещение – 18 ноября 2013 г.)).

[2] Brazil's Petrobras to invest heavily in data security / Joe Leahy. Financial Times. 18 September 2013 (http://www.ft.com/cms/s/0/f3195d0a-2081-11e3-9a9a-00144feab7de.html#axzz2mppMkbEv (последнее посещение – 18 ноября 2013 г.)).

[3] President Dilma Rousseff at the UN General Assembly / Bruce Sterling. The Wired. September 24, 2013 (http://www.wired.com/beyond_the_beyond/2013/09/pres-dilma-rousseff-at-the-un-general-assembly/ (последнее посещение – 18 ноября 2013 г.)).

приводится в настоящем сборнике[1]. Проект резолюции, в частности, призывает государства – члены ООН: (1) уважать и обеспечивать защиту прав на неприкосновенность частной жизни; (2) предпринять меры по предотвращению нарушений этих прав, в том числе посредством приведения национального законодательства в соответствие с международным правом в области прав человека; (3) пересмотреть процедуры, практики и законодательство в отношении программ отслеживания коммуникаций; (4) сформировать механизмы обеспечения прозрачности и подотчетности перед обществом государственных программ слежки за коммуникациями.

В результате всех этих событий Россия, с 1998 г. привыкшая штурмовать бастионы *несправедливого миропорядка* в сфере интернета, оказалась в непривычной, но приятной ситуации. Если прежде Китай и другие союзники молчаливо прятались за спиной Москвы, выглядевшей одиноким воином в этом поле, то сегодня сама Россия может перевести дух и пропустить вперед разгневанную Бразилию. На этом фоне можно также ожидать ратификации двустороннего российско-бразильского соглашения о сотрудничестве в сфере МИБ, зависшего на стадии подписания в 2010 г. Читатели данного сборника также имеют возможность ознакомиться с текстом этого соглашения.

Но еще одной важной глобальной тенденцией, которая резко ускорилась после связанных со Сноуденом событий, является стратегический разворот в политике *ICANN* и все более явный курс на выход Корпорации интернета из-под влияния США и ориентация на стейкхолдеров развивающегося мира.

Первые значительные изменения статуса *ICANN* имели место в 2009 г. в связи с заключением между Министерством торговли США и *ICANN* Соглашения о подтверждении обязательств, которое зафиксировало статус Корпорации интернета как структуры, формально подотчетной Министерству, но полностью независимой в части принятия решений по всем вопросам в рамках своей компетенции.

Однако именно сегодня обозначились серьезные предпосылки к тому, чтобы свести к минимуму особую роль США в реализации функций *ICANN*. Подтверждением этому служит ряд заявлений президента Корпорации Фади Шехаде, сделанных в октябре 2013 г. в преддверии и в ходе 8-го Всемирного форума по управлению интернетом и касаю-

[1] См.: A/. Brazil and Germany: draft resolution. United Nations General Assembly. The right to privacy in the digital age. November 2013 // Auswaertiges Amt Website (http://www.auswaertiges-amt.de/cae/servlet/contentblob/660692/publicationFile/186838/131127_Right-2Privacy_EN.pdf (последнее посещение – 18 ноября 2013 г.)).

щихся необходимости ухода от особой роли США в сфере глобального управления интернетом, в том числе в связи с раскрытыми Сноуденом программами массированного слежения за интернет-пользователями[1].

Усиление сотрудничества с развивающимся миром, странами Азии, Африки и Латинской Америки отражают и институциональные нововведения *ICANN* за последние годы, такие как открытие новых региональных офисов Корпорации в Монтевидео и в Пекине. В совокупности с обсуждаемыми планами по перемещению офиса Президента *ICANN* из Лос-Анджелеса в Стамбул (где находится новая региональная штаб-квартира *ICANN*), последние заявления руководства Корпорации иллюстрируют тенденцию к повышению ее глобального статуса и позиционирования ее как полностью самостоятельного игрока, не привязанного в своей политике ни к США, ни к какому-либо иному государственному актору и ориентированного в том числе на развивающийся мир.

Еще до *IGF* большое внимание привлекло к себе так называемое *заявление Монтевидео* – коллективное заявление Руководителей организаций, отвечающих за глобальную координацию технической инфраструктуры интернета, подписанное в столице Уругвая 7 октября 2013 г.[2]. Помимо президента *ICANN* документ подписали главы таких структур, как Совет по архитектуре Интернета (*IAB*), Общество Интернета (*ISOC*), Сетевой координационный центр европейских *IP*-сетей (*RIPE NCC*) и Консорциум Всемирной паутины (*W3C*), а также других технических организаций. Один из ключевых тезисов этого документа – призыв к «ускорению глобализации функций *ICANN* и *IANA*» для обеспечения равноправного участия всех сторон, включая правительства, в процессе управления интернетом.

Кроме того, возвращаясь к Бразилии и ее политике по обеспечению доверия и безопасности в интернете, надо сказать, что после упомянутых выше заявлений президента Роуссефф в диалог с ней вступила *ICANN*, содействовав выдвижению еще одной важной бразильской инициативы.

---

[1] См., например: Fadi Chehadé's Opening Speech, IGF 2013 // ICANN Website. 21 October 2013 (http://www.icann.org/en/news/presentations/chehade-speech-igf-bali-21oct13-en.pdf (последнее посещение – 18 ноября 2013 г.)); Fadi Chehadé Speaks at the 2013 IGF // ICANN Website. 5 November 2013 (http://www.icann.org/en/about/learning/podcasts/podcast-chehade-igf-bali-05nov13-en.htm (последнее посещение – 18 ноября 2013 г.)).

[2] Заявление Монтевидео о будущем сотрудничества в сфере интернета от 7 октября 2013 г. // Сайт Корпорации интернета по распределенипю имен и адресов (http://www.icann.org/ru/news/announcements/announcement-07oct13-ru.htm (последнее посещение – 18 ноября 2013 г.)).

После встречи с президентом *ICANN* Фади Шехаде в октябре 2013 г. г-жа Роуссефф заявила о том, что уже в следующем году Бразилия выступит организатором новой глобальной дискуссии по вопросам совершенствования управления интернетом с участием всех заинтересованных сторон (стейкхолдеров)[1]. Дискуссия планируется в формате глобальной конференции стейкхолдеров в Бразилии в апреле 2014 г., о чем была достигнута договоренность с президентом *ICANN*. По словам министра, конечная цель саммита – синтезировать некое единое, всеобъемлющее видение проблем и путей их решения стейкхолдерами.

В совокупности эти и другие недавние инициативы и заявления руководства *ICANN* позволяют сформулировать весьма неординарный вопрос: идет ли *ICANN* по пути трансформации из относительно небольшой технической организации, ограниченной в своих компетенциях вопросами регулирования системы доменных имен и *IP*-адресов, в самостоятельного глобального игрока, замыкающего на себе политические вопросы управления интернетом? А если ответ положительный, то как эта тенденция соотносится с интересами глобального интернет-сообщества и с российскими национальными интересами?

Однозначный ответ на эти совсем недавно возникшие перед международным сообществом и интернет-сектором вопросы пока не может быть дан – потребуется отдельное исследование куда большего объема, чем эта статья. Но размышлять над поставленными вопросами читатель может и должен уже сейчас, особенно если его профессиональная деятельность так или иначе связана с политико-правовым регулированием ИКТ и интернета.

В этой связи читателям будет полезно ознакомиться с приводимыми в сборнике документами *ICANN*, для того чтобы лучше представлять и учитывать роль и статус Корпорации интернета при анализе будущих событий в сфере глобального управления Сетью.

[1] President Dilma Rousseff at the UN General Assembly / Bruce Sterling. The Wired. September 24, 2013 (http://www.wired.com/beyond_the_beyond/2013/09/pres-dilma-rousseff-at-the-un-general-assembly/ (последнее посещение – 18 ноября 2013 г.)).

РАЗДЕЛ II
ДОКУМЕНТЫ И МАТЕРИАЛЫ

1. Техническое сообщество, частный сектор

1.1. Корпорация интернета по распределению имен и адресов (*The Internet Corporation for Assigned Names and Numbers, ICANN*)[1]

ПОДТВЕРЖДЕНИЕ ОБЯЗАТЕЛЬСТВ СО СТОРОНЫ МИНИСТЕРСТВА ТОРГОВЛИ США И КОРПОРАЦИИ ИНТЕРНЕТА ПО РАСПРЕДЕЛЕНИЮ ИМЕН И АДРЕСОВ[2]

1. Данный документ представляет собой подтверждение обязательств (далее – Подтверждение) со стороны Министерства торговли США (далее – Министерство Торговли США) и некоммерческой организации «Корпорация интернета по распределению имен и адресов» (далее – *ICANN*). Отмечая завершение Соглашения о совместной реализации проекта и с целью регламентировать и документально зафиксировать осуществление технической координации системы доменных имен и адресов интернета (далее – система *DNS*)[3] в глобальном масштабе организацией, представляющей частный сектор, Стороны договорились о следующем.

2. Интернет представляет собой технологию, способную к трансформации, которая дает дополнительные возможности людям по всему

---

[1] *ICANN* – международная некоммерческая организация, создана в 1998 г. (Калифорния, США) для регулирования вопросов, связанных с доменными именами и *IP*-адресами.

[2] *Affirmation of Commitment by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers*. – URL:http://www.icann.org (неофициальный перевод М.Б. Касеновой).

[3] В целях настоящего документа система доменных имен и адресов интернета (*DNS*) определяется как: доменные имена; адреса интернет-протокола и адреса автономных систем; порты протокола и номера параметров. *ICANN* осуществляет координацию этих идентификаторов на общем уровне в соответствии со своей задачей.

миру, стимулировать новаторство, способствовать торговле и предпринимательству, обеспечивать свободное и беспрепятственное распространение информации. Одним из залогов успеха интернета является высокая степень децентрализации сети, позволяющая принимать решения на локальном уровне и способствующая этому. Несмотря на децентрализацию, для обеспечения оперативной совместимости требуется глобальная техническая координация фундаментальной инфраструктуры интернета, а именно системы *DNS*.

3. В данном документе подтверждаются ключевые обязательства Министерства Торговли США и *ICANN*, включающие: (*a*) обеспечение принятия решений в отношении глобальной технической координации *DNS* в интересах общественности, а также ответственность за принятие решений и прозрачность этих решений; (*b*) сохранение безопасности, стабильности и гибкости *DNS*; (*c*) стимулирование конкуренции, доверия потребителей и возможностей выбора на рынке услуг, связанных с *DNS*; а также (*d*) содействие международному участию в технической координации *DNS*.

4. Министерство Торговли США подтверждает свою приверженность модели технической координации *DNS*, объединяющей усилия различных заинтересованных сторон, при общем руководстве частного сектора, формирование политики, начинающейся на самом низовом уровне, в интересах пользователей интернета по всему миру. Гибкий механизм координации на частном уровне, результаты которого отражают интересы общественности, лучше всего способен соответствовать меняющимся требованиям интернета и его пользователей. *ICANN* и Министерство Торговли США отмечают существование групп участников, в большей мере задействованных в механизмах *ICANN*, нежели остальные пользователи интернета в целом. В обеспечение отражения интересов общественности, а не только интересов узкого круга заинтересованных лиц, при принятии решений *ICANN* обязуется проводить и публиковать результаты анализа положительного и отрицательного влияния, в том числе и финансового, своих решений на широкую общественность, а также возможного положительного или отрицательного воздействия на системную безопасность, стабильность и гибкость *DNS*.

5. Министерство Торговли США признает важность предоставления пользователям интернета по всему миру возможности работать с ним на родном языке с использованием соответствующего набора символов и одобряет оперативное внедрение национальных доменов верхнего уровня с интернационализированными доменными имена-

ми (*ccTLDs*) при условии предварительного решения связанных с этим вопросов безопасности, стабильности и гибкости *DNS*.

Содержание данного документа не представляет собой поддержку со стороны Министерства Торговли США какого-либо конкретного плана или предложения по внедрению новых Общих доменов верхнего уровня («*gTLDs*») и не является выражением мнения Министерства Торговли США о том, что потенциальные выгоды новых «*gTLDs*» перевешивают возможные издержки.

6. Министерство Торговли США также подтверждает обязательство Правительства США продолжать постоянное участие в Правительст-венном консультативном комитете *ICANN* (далее – *GAC*). Министер-ство Торговли США отмечает важность роли *GAC* в рамках процессов принятия решений и выполнения задач *ICANN*, равно как и эффективность рассмотрения предложений *GAC* со стороны *ICANN* в отношении аспектов общественной политики технической координации *DNS*.

7. *ICANN* заявляет о своей приверженности прозрачным и подотчетным механизмам формирования бюджета, разработке политики на основании фактов, дискуссиям между различными сообществами и динамичным консультационным процедурам, в рамках которых предоставляются подробные описания оснований для принятия решений, включая влияние комментариев на процесс разработки политики. *ICANN* также обязуется ежегодно публиковать отчет, в котором отражается прогресс корпорации в свете ее Устава, ответственности, стратегических и операционных планов. Кроме того, *ICANN* обязуется предоставлять подробные и взвешенные объяснения принимаемым решениям, их обоснования, а также указывать источники данных и информации, на которые опиралась *ICANN* при принятии решений.

8. *ICANN* подтверждает свою приверженность: (*a*) поддержанию возможности и способности координировать *DNS* Интернета на общем уровне и работать над поддержанием единой, оперативно совместимой сети; (*b*) существованию в форме некоммерческой корпорации со штаб-квартирой в Соединенных Штатах Америки и представительствами по всему миру, отвечающей нуждам мирового сообщества; и (*c*) продолжению деятельности в качестве организации, объединяющей различные заинтересованные стороны, с преобладанием частного сектора и приветствующей участие общественности, на благо которой *ICANN* призвана действовать при любых обстоятельствах. *ICANN* является частной организацией, и ни одно из положений данного

Подтверждения не должно рассматриваться как признание контроля со стороны какой-либо организации.

9. Отмечая, что *ICANN* будет развиваться и адаптироваться для выполнения своей ограниченной, но важной технической задачи по координации *DNS*, Корпорация также обязуется предпринимать следующие конкретные шаги вкупе с описанным ниже регулярным пересмотром обязательств.

9.1. *Обеспечение подотчетности, прозрачности и удовлетворения интересов пользователей интернета по всему миру*: *ICANN* обязуется использовать следующие методы для поддержания и улучшения надежных механизмов учета мнения общественности, подотчетности и прозрачности в обеспечении отражения общественных интересов в ходе принятия решений и подотчетности всем заинтересованным сторонам: (*a*) постоянная переоценка и улучшение методов деятельности Правления *ICANN*, включая текущую оценку деятельности Правления, процесса выборов Правления, степени, в которой состав Правления отвечает текущим и будущим нуждам *ICANN*, а также рассмотрение механизма подачи апелляций на решения Правления; (*b*) анализ роли и эффективности *GAC* и его взаимодействий с Правлением и предоставление рекомендаций по улучшению, обеспечивающих эффективное рассмотрение со стороны *ICANN* вклада *GAC* в аспекты общественной политики технической координации *DNS*; (*c*) постоянная переоценка и совершенствование процессов, при помощи которых *ICANN* принимает отзывы общественности (включая адекватное разъяснение принимаемых решений и их обоснование); (*d*) постоянный анализ степени, в которой решения *ICANN* воспринимаются, поддерживаются и принимаются общественностью и интернет-сообществом; и (*e*) переоценка механизма разработки политики с целью обеспечения более насыщенных обсуждений различными сообществами, разработки эффективной и своевременной политики.

ICANN будет организовывать пересмотр успешности выполнения вышеуказанных обязательств с регулярностью не менее одного раза в три года, первый пересмотр подобного рода должен быть завершен не позднее 31 декабря 2010 г. Пересмотр будет осуществляться на добровольной основе участниками сообщества, а состав соответствующей рабочей группы будет опубликован для общественного обсуждения; в него войдут следующие лица (или их представители): председатель *GAC*, председатель Правления *ICANN*, помощник секретаря по коммуникации и информации Министерства Торговли США, представители соответствующих консультативных комитетов и организаций

поддержки, а также независимые эксперты. Состав рабочей группы по пересмотру будет совместно согласовываться председателем *GAC* на основе консультаций с членами *GAC* и председателем Правления *ICANN*. Рекомендации, выработанные по результатам пересмотров, будут предоставляться Правлению и публиковаться для общественного обсуждения. Правление обязуется принимать меры в течение шести месяцев от получения рекомендаций. В ходе каждого из вышеупомянутых пересмотров будет рассматриваться степень успешности оценок и мер, принимаемых *ICANN*, по обеспечению прозрачности деятельности, подотчетности процесса принятия решений и соблюдения общественных интересов со стороны корпорации. Неотъемлемой частью пересмотров станут оценки успешности реализации Правлением и сотрудниками рекомендаций, вытекающих из прочих обязательств, перечисленных ниже.

9.2. *Поддержание безопасности, стабильности и гибкости*: *ICANN* разработала план по повышению рабочей стабильности, надежности, гибкости, безопасности и глобальной оперативной совместимости *DNS*, который будет регулярно обновляться в свете новых угроз, возникающих для этой системы. *ICANN* будет организовывать пересмотр успешности выполнения вышеуказанных обязательств с регулярностью не менее одного раза в три года. Первый пересмотр начнется через год с даты вступления в силу данного подтверждения. Особое внимание будет уделено: (*a*) вопросам физической и сетевой безопасности, стабильности и гибкости, связанным с безопасной и стабильной координацией *DNS* Интернета; (*b*) обеспечению адекватного планирования на случай возникновения непредвиденных обстоятельств; и (*c*) поддержанию прозрачности механизмов. В ходе всех пересмотров, осуществляемых в рамках данного раздела, будет оцениваться степень успешности работы *ICANN* по реализации плана безопасности, эффективности плана при решении реальных и потенциальных задач и угроз, степени надежности плана безопасности при решении реальных и потенциальных задач и угроз безопасности, стабильности и гибкости *DNS* Интернета в рамках ограниченной технической задачи *ICANN*. Пересмотр будет осуществляться на добровольной основе участниками сообщества, а состав соответствующей рабочей группы будет опубликован для общественного обсуждения; в него войдут следующие лица (или их представители): председатель *GAC*, Исполнительный директор *ICANN*, представители соответствующих консультативных комитетов и организаций поддержки, а также независимые эксперты. Состав рабочей группы по пересмотру бу-

дет совместно согласовываться председателем *GAC* на основе консультаций с членами *GAC* и Исполнительным директором *ICANN*. Рекомендации, выработанные по результатам пересмотров, будут предоставляться Правлению и публиковаться для общественного обсуждения. Правление обязуется принимать меры в течение шести месяцев от получения рекомендаций.

9.3. *Содействие конкуренции, доверию потребителей и возможностей выбора на рынке*: При рассмотрении возможности расширения пространства доменов верхнего уровня еще до ее реализации *ICANN* обеспечит адекватное рассмотрение различных связанных с этим вопросов (включая конкуренцию, защиту потребителей, безопасность, стабильность и гибкость, проблемы предумышленного злоупотребления, суверенитета и защиты прав). После одного года эксплуатации новых *gTLDs* (будь то с использованием *ASCII* или наборов символов для других языков) *ICANN* организует пересмотр, в ходе которого будет проанализирована степень, в которой ввод или расширение *gTLDs* способствовали росту конкуренции, доверия потребителей и возможностей выбора на рынке, а также эффективности (*a*) процесса подачи и оценки заявок, и (*b*) механизмов, призванных смягчать последствия проблем, связанных с вводом и расширением. Через два года после первого пересмотра *ICANN* организует повторный пересмотр успешности выполнения вышеуказанных обязательств, а затем будет проводить аналогичные пересмотры не менее одного раза в четыре года. Пересмотр будет осуществляться на добровольной основе участниками сообщества, а состав соответствующей рабочей группы будет опубликован для общественного обсуждения; в него войдут следующие лица (или их представители): председатель *GAC*, Исполнительный директор *ICANN*, представители соответствующих консультативных комитетов и организаций поддержки, а также независимые эксперты. Состав рабочей группы по пересмотру будет совместно согласовываться председателем *GAC* на основе консультаций с членами *GAC* и Исполнительным директором *ICANN*. Рекомендации, сделанные на основе пересмотров, будут предоставляться Правлению и публиковаться для общественного обсуждения. Правление обязуется принимать меры в течение шести месяцев от получения рекомендаций.

9.3.1. Кроме того, *ICANN* обязуется воплощать в жизнь свою существующую политику в отношении сервиса *WHOIS* с соблюдением соответствующего законодательства. Существующая политика требует от *ICANN* реализации мер по поддержанию своевременного, неограни-

ченного и открытого доступа к точным и полным сведениям в системе *WHOIS*, включая сведения о владельцах регистраций, техническую, финансовую и административную информацию. Через один год с даты вступления в силу настоящего документа, а затем с регулярностью не менее одного раза в три года *ICANN* организует пересмотр политики *WHOIS* и ее реализации для оценки эффективности, соответствия законным нуждам правоохранительных органов и содействия укреплению доверия пользователей. Пересмотр будет осуществляться на добровольной основе участниками сообщества, а состав соответствующей рабочей группы будет опубликован для общественного обсуждения; в него войдут следующие лица (или их представители): председатель *GAC*, Исполнительный директор *ICANN*, представители соответствующих консультативных комитетов и организаций поддержки, эксперты, представители мирового правоохранительного сообщества и глобальные эксперты в области конфиденциальности. Состав рабочей группы по пересмотру будет совместно согласовываться председателем *GAC*, на основе консультаций с членами *GAC* и Исполнительным директором *ICANN*. Рекомендации, вытекающие из пересмотров, будут предоставляться Правлению и публиковаться для общественного обсуждения. Правление обязуется принимать меры в течение шести месяцев с момента получения рекомендаций.

10. В целях содействия прозрачности и открытости процессов обсуждения и деятельности *ICANN* сроки и результаты анализа будут публиковаться для общественного обсуждения. Рабочие группы будут принимать во внимание комментарии общественности и вносить изменения в результаты на свое усмотрение перед предоставлением итогового отчета Правлению.

11. Министерство Торговли США принимает данное Подтверждение обязательств на основании своих полномочий в соответствии со статьями 15 U.S.C 1512 и 47 U.S.C 902 Свода законов США. 902. *ICANN* принимает данное Подтверждение в соответствии со своим Учредительным договором и Уставом.

Данное соглашение вступает в силу с **1 октября 2009** г. Соглашение рассчитано **на долгосрочную перспективу**, но может быть изменено в любое время со взаимного согласия Сторон. Любая из Сторон может расторгнуть данное Подтверждение обязательств с предоставлением письменного уведомления другой Стороне за 120 дней. Подтверждение не подразумевает перевода денежных средств (расчетов) между Сторонами. В случае расторжения подтверждения обязательств каждая из Сторон самостоятельно несет ответственность за возможные

понесенные ею расходы. Все обязательства Министерства Торговли США по данному Подтверждению обязательств зависят от наличия средств.

ЗА НАЦИОНАЛЬНОЕ УПРАВЛЕНИЕ
ПО ТЕЛЕКОММУНИКАЦИЯМ
И ИНФОРМАЦИИ
Лоуренс И. Стриклинг (*Lawrence E. Strickling*)
Помощник Секретаря по
коммуникациям и информации
30 сентября 2009 г.

ЗА КОРПОРАЦИЮ ИНТЕРНЕТА
ПО РАСПРЕДЕЛЕНИЮ ИМЕН И АДРЕСОВ:
Род Бэкстрем (*Rod Beckstrom*)
Президент и Исполнительный иректор
30 сентября 2009 г.

СТРАТЕГИЧЕСКИЙ ПЛАН *ICANN*. ИЮЛЬ 2012 – ИЮНЬ 2015 г.[1]

(*Извлечение*)

Единый мир. Единый Интернет

ICANN – всемирная организация, отвечающая за координацию систем уникальных идентификаторов в Интернете на благо пользователей во всем мире, обеспечивая работу единого глобального межплатформенного Интернета. Модель *ICANN*, учитывающая мнения большого числа заинтересованных сторон, и политики, разрабатываемые всем сообществом, позволяют использовать системы уникальных идентификаторов Интернета миллиардам компьютеров, телефонов и других устройств, применяемых для подключения людей к единому Интернету.

Кредо **ICANN**: Единый мир. Единый Интернет.

[1] Документ опубликован на русском языке: URL: http://www.icann.org/ru/about/planning/strategic/strategic-plan-2012-2015-18may12-ru.pdf

Миссия **ICANN**:

• координация на высшем уровне глобальных систем уникальных идентификаторов Интернета и

• обеспечение стабильности и безопасности работы систем уникальной идентификации Интернета.

Системы уникальной идентификации Интернета состоят из следующих компонентов: служба доменных имен (*DNS*), протокол Интернета (*IP*), номера автономных систем (АС) и номера портов и параметров протоколов. *ICANN* подтверждает свое обязательство работать над сохранением единого глобального межплатформенного Интернета.

Кредо и миссия *ICANN* охватывают четыре стратегических области, реализуемые в этом плане.

Кредо и миссия *ICANN* охватывают четыре стратегических области, реализуемые в этом плане.

<...>

Ключевые темы этого стратегического плана: реализация образцовой модели управления с участием многих заинтересованных сторон; глобальная координация безопасности, стабильности и отказоустойчивости (БСО); интернационализация корпорации *ICANN* и ее взаимоотношений; многообразие заинтересованных сторон и расширение масштабов; формулирование политик и выполнимых соглашений; обслуживание DNS через оказание безупречных услуг *IANA*; а также запуск ввода новых программ рДВУ и ИДИ.

<...>

Влияние и контроль

Миссия *ICANN* описывает широкие цели: обеспечивать стабильность и безопасность систем уникальных идентификаторов Интернета, поощряя конкуренцию и возможность выбора для потребителей, поддерживая независимый, широкий и демократический процесс разработки политики. Постановка соответствующих, реальных стратегических целей, отвечающих миссии, требует от организации понимания того, на что она может и должна влиять, а что она может и должна контролировать. Например, *ICANN* не может гарантировать абсолютно безотказное функционирование *DNS*, однако через форумы, путем разъяснительной работы и интеллектуального лидерства *ICANN* может влиять на действия ключевых участников для обеспечения безопасности, стабильности и отказоустойчивости в их зонах контроля Интернета. Стратегический план *ICANN* обусловлен (и ограничен) ее Уставом, Учредительным договором и документом «Подтверждение обязательств».

Таким образом, стратегический план *ICANN* включает задачи, в которых организация может и должна оказывать влияние на достижение целей, не входящих в область непосредственного контроля – действуя на благо широкого сообщества пользователей Интернета. План также содержит задачи по выполнению компонентов заявления о миссии в пределах непосредственного управления *ICANN*. Во многих областях *ICANN* располагает некоторыми средствами контроля и может оказывать влияние на достижение определенных целей. Важно, чтобы цели были зафиксированы письменно для должного отражения такой среды.

Хотя одностраничная версия стратегического плана не отражает различий между областями влияния и контроля, однако цели поставлены с учетом этих моментов. Упомянутая выше одностраничная версия плана дополняется нижеследующим рисунком, отражающим широкий спектр влияния *ICANN* в четырех сферах деятельности стратегического плана для контроля над выработкой реальных задач, нацеленных на реализацию заявления о миссии и на благо сообщества.

<...>

Каждая из сфер деятельности плана предусматривает различное соотношение влияния и контроля. Например, *ICANN* располагает большими возможностями контроля над задачами, лежащими в пределах рабочих полномочий (включая *IANA*), некоторым контролем, но значительным влиянием в отношении успешного ведения процесса выработки политики *ICANN*, и более широким влиянием по сравнению со средствами контроля в сфере проблем *DNS* – зачастую относящихся к аспектам безопасности, разработки и внедрения протоколов.

В прошлом году *ICANN* опубликовала первоначальный список стратегических показателей, связанных с каждой из сфер деятельности. Сообществу было предложено принять участие в разработке способов измерения этих показателей и отчетности по ним, поскольку соотношение возможностей влияния и контроля со стороны *ICANN* меняется в зависимости от показателя. Сообщество поставило перед *ICANN* задачу отчитываться по ежегодным показателям работы в процессе подготовки целей на следующий год. *ICANN* с нетерпением ждет совместной работы с сообществом над улучшением отчетности по стратегическим показателям.

Стабильность и безопасность *DNS*

Определение сферы деятельности. *ICANN* уполномочена решать следующие задачи: (*i*) обеспечение стабильной и безопасной работы

систем уникальной идентификации Интернета, (*ii*) усиление международного сотрудничества в технической координации *DNS* и (*iii*) координация эксплуатации и развитие системы корневых серверов имен *DNS*. Эта область касается операций, связанных с внешней безопасностью и стабильностью (в отличие от раздела «*IANA* и основная деятельность», в котором рассматриваются внутренние операции). Роль *ICANN* в стабильности и безопасности *DNS* в некоторых случаях осуществляется посредством прямого управления или ограничивается в других случаях использованием своего положения для влияния на другие заинтересованные стороны. Примеры таких обстоятельств – это корневые серверы имен (где у *ICANN* имеются прямые связи), серверы имен рДВУ (прямой контроль, предусмотренный контрактом), серверы имен нДВУ (прямые связи), серверы доменных имен второго и нижнего уровня (их миллионы, влияние через стандарты *IETF*, передовой опыт ККБС и обучение).

Текущее состояние дел. Стабильность, безопасность и отказоустойчивость (БСО) глобальных систем уникальной идентификации Интернета (*DNS*, *IP*-адреса и номера, параметры и порты АС) являются важными приоритетами для *ICANN*, отрасли и пользователей Интернета по всему миру. БСО составляют основные элементы миссии *ICANN*. Неправомерное использование и атаки на DNS и другие инфраструктуры Интернета ставят под угрозу общую безопасность уникальной идентификации. Количество и изощренность кибер-атак с целью нарушения безопасности отдельных лиц, корпораций и государств продолжают расти. Участие правоохранительных органов в борьбе с ними все более возрастает. Планирование непрерывности бизнеса (ПНБ) получает тем больший импульс, чем больше организаций планирует и проводит тестирование моделей прерывания бизнеса. Кроме того, новые ДВУ (включая ИДИ) и общий рост числа доменных имен будут и далее порождать новые возможности и сложные проблемы по мере развития сотрудничества ICANN с операторами новых ДВУ в сфере обеспечения стабильности, безопасности и отказоустойчивости. ИДИ и их варианты могут также увеличить уязвимость Интернета за счет расширения фишинга, и таким образом поставить под угрозу стабильность. Последние блоки адресного пространства IPv4 были распределены под руководством *ICANN* и РРИ, в то время как сообщество сетевых операторов осваивает сети IPv6. Для обеспечения безопасности, стабильности и отказоустойчивости, являющихся критически важными элементами систем уникальной идентификации, корпорация *ICANN* должна сотрудничать со всеми, кто занимается решением этих проблем.

Стратегические цели. В сфере деятельности «Безопасность, стабильность и отказоустойчивость» ICANN определила четыре стратегические цели. С каждой целью связаны проекты, персонал и задачи для сообщества, которые будут обеспечивать достижение стратегических целей в период реализации этого плана. Стратегические цели таковы:

Сохранение и обеспечение работоспособности DNS. С момента своего основания корпорация *ICANN* работает с сообществом, чтобы обеспечить безопасность, стабильность и отказоустойчивость *DNS*. Безусловно, это область, где *ICANN* ставит перед собой серьезную стратегическую цель (поддержание стопроцентно непрерывной работы *DNS*), не имея средств для ее достижения. Определенные аспекты *ICANN* контролирует, на определенные аспекты *ICANN* может существенно влиять. Но есть и такие области, где *ICANN* может более непосредственно воздействовать на коммуникации для достижения взаимопонимания в рамках сообщества. Например, *ICANN* может контролировать и гарантировать стабильную и непрерывную работу корневого сервера *L*. *ICANN* также имеет договорные и другие прочные отношения с ДВУ и регистраторами, позволяющие управлять этой областью. Стратегические проекты, призванные обеспечить непрерывную работу *DNS*, включают планирование непрерывности бизнеса для реестров и регистраторов и помощь во внедрении *IPv*6. *ICANN* будет работать в интересах РРИ над продвижением (через свои представительские группы) *IPv*6 в среду поставщиков услуг Интернета, потребителей и деловых кругов. Работа персонала и сообщества будет направлена на наращивание потенциала DNS и улучшение интеграции глобальных усилий.

Содействие широкому признанию DNSSEC. Внедрение расширений безопасности системы доменных имен (*DNSSEC*) будет и далее оставаться стратегической целью *ICANN*. *DNSSE*C обеспечивает механизм аутентификации ответов на запросы *DNS* и уменьшает риск определенных видов вредоносного поведения. *ICANN* продолжит сотрудничество с сообществом в сфере контроля и повышения устойчивости *DNS* к атакам. В 2011 г. *ICANN* стала свидетелем достижения в развивающихся странах целевого количества новых ДВУ, подписанных с помощью *DNSSEC*. В течение 2012 г. *ICANN* по-прежнему будет содействовать признанию *DNSSEC* доменами верхнего уровня. К концу этого периода планирования система *DNSSEC* будет широко внедрена. Кроме того, ICANN будет координировать разработку системы сертификации номерных ресурсов Интернета как средства повышения безопасности интернет-протокола (*IP*).

Расширение международного сотрудничества в области DNS. Атаки на систему уникальной идентификации могут возникать из любой точки земного шара. Надежные системы и методы обеспечения международной безопасности формируют передовую линию защиты от злонамеренного поведения. Работа персонала и сообщества будет сосредоточена на расширении глобальной безопасности и сотрудничестве с операторами региональных реестров Интернета (РРИ) в целях повышения общей безопасности и поддержки региональных и локальных организаций как лидеров в обеспечении стабильности, безопасности и отказоустойчивости. *ICANN* будет поддерживать рабочие группы сообщества в разработке таких решений, как координация группы чрезвычайной поддержки (*DNS CERT*), решений проблем с вариантами ИДИ и других необходимых решений для устранения проблем безопасности Интернета. *ICANN* вместе с сообществом будет работать над поиском экономически эффективных подходов к решениям по БСО. Кроме того, сообществу необходимо работать над развитием базы данных *Whois* для включения в нее интернационализированных регистрационных данных и соответствующих политик конфиденциальности. *ICANN* также стремится к непрерывному взаимодействию с интернет-сообществом и правоохранительными органами для противодействия злонамеренному поведению. Персонал *ICANN* будет работать над совместным наращиванием возможностей обеспечения БСО уникальных идентификаторов в развивающихся странах.

Улучшение управления рисками и отказоустойчивости трех типов уникальных идентификаторов. Это сфера, в которой усилия *ICANN* окажут прямое влияние на улучшение безопасности и стабильности всей *DNS* и других уникальных идентификаторов (*IP*-адреса, номера АС, портов и параметров) через международное участие в учениях по обеспечению непрерывности бизнеса, обучении и моделировании чрезвычайных ситуаций. *ICANN* будет координировать улучшение управления рисками для глобальной системы *DNS* через планирование непрерывности функционирования реестров и регистраторов и отработку учебных моделей прерывания бизнеса. *ICANN* будет сотрудничать со всеми заинтересованными сторонами в деле защиты целостности глобальной системы *DNS* через такие инициативы, как обучение операторов ДВУ. *ICANN* также усилит сотрудничество с сообществом, заинтересованным в глобальной компьютерной безопасности, и группами реагирования на чрезвычайные ситуации в целях улучшения и поощрения работы в сооб-

ществе по развитию и тестированию ПОНБ для защиты от рисков и угроз. *ICANN* будет стремиться к сотрудничеству с другими заинтересованными сторонами для разработки эффективных моделей управления рисками.

Улучшение мер реагирования на происшествия в сфере безопасности DNS. Угрозы безопасности Интернета продолжают расти, и этот рост приводит к необходимости улучшения процессов и систем, используемых организациями для реагирования на происшествия в сфере безопасности. *ICANN* продолжит реализацию программы ежегодной оценки риска *DNS* и систематического планирования действий в непредвиденных обстоятельствах, а также работу вместе с сообществом над созданием эффективных и экономичных способов реагирования на происшествия в сфере безопасности *DNS*. *ICANN* будет поддерживать усилия по формированию и планированию новой рабочей группы по вопросам управления рисками *DNS*. *ICANN* также будет содействовать инициативе по изучению управления рисками DNS вместе с сообществом и сторонними экспертами.

Стратегические показатели. Вкратце, стратегическими показателями в области стабильности и безопасности *DNS* являются:

- абсолютно безотказное функционирование корневого сервера *L*;
- инициирование разработки сообществом важнейших индикаторов эффективности для измерения «абсолютно безотказного функционирования *DNS*»;
- обеспечение выполнения договорных обязательств соглашений об уровне обслуживания в отношении бесперебойного функционирования ДВУ;
- количество глобальных учений по обеспечению непрерывности бизнеса;
- степень прогресса в сертификации соответствия глобальному стандарту обеспечения непрерывности бизнеса;
- количество подписанных *DNSSEC* ДВУ и широкое внедрение этой системы к концу периода планирования;
- количество мероприятий по повышению осведомленности о протоколе *IPv*6 с участием *ICANN*;
- инициирование усилий в области безопасности по сертификации номерных ресурсов Интернета и сотрудничество с сообществом при их реализации в течение периода планирования;
- Определение показателей для обеспечения выделения надлежащей части бюджета *ICANN* на проблемы стабильности, безопасности и отказоустойчивости *DNS*.

Конкуренция, доверие потребителей и возможности выбора на рынке

Определение сферы деятельности. *ICANN* уполномочена решать следующие задачи: (*i*) использование для операций открытых и прозрачных процессов, которые предполагают конкуренцию и свободный доступ на связанные с Интернетом рынки, (*ii*) разработка политик для определения обстоятельств, при которых могут добавляться новые ДВУ, (*iii*) поощрение конкуренции при регистрации доменных имен на благо и для реальной выгоды сообщества и (*iv*) укрепление доверия и расширение выбора для потребителей на рынке *DNS*. Роль *ICANN* в этой области заключается в координации функционирования многосторонней модели путем сотрудничества с сообществом в деле выявления, развития, принятия и внедрения политик, способствующих путем влияния или контроля расширению доверия, возможностей выбора, конкуренции, инновациям и предупреждению злоупотреблений. *ICANN* ведет портфель проектов, направленных на продвижение этих новых политик в сообществе.

Текущее состояние дел. По состоянию на 30 июня 2011 г. в мире существует более 215 000 000 доменных имен. 20 июня 2011 г. Правление *ICANN* проголосовало за утверждение и запуск программы ввода новых рДВУ с открытием окна приема заявок 12 января 2012 г. Добавление в Интернет новых интернационализированных доменов верхнего уровня (ИДИ) будет продолжаться. Количество сторон, связанных с *ICANN* договорными отношениями, существенно увеличится, по мере того как успешные кандидаты на регистрацию новых рДВУ будут становиться реестрами, заключившими договора с *ICANN*. Программа ввода новых рДВУ также привлечет большее внимание к *ICANN* и, соответственно, приведет к более критическому анализу эффективности работы корпорации. Благодаря появлению новых заинтересованных сторон будет наблюдаться непрерывное расширение их состава и смещение приоритетов.

Рынки реестров и регистраторов Интернета продолжают эволюционировать и включают в свой состав множество разных и развивающихся бизнес-моделей. Многие кандидаты в новые операторы ДВУ (включая ИДИ) будут использовать современные бизнес-модели, дающие им перспективу и высокие ожидания. Как и на любом другом развивающемся рынке, вырастет конкуренция, некоторые бизнес-модели выживут и будут восприняты сообществом, в то время как другие потерпят крах и исчезнут. Очень важен тот факт, что *ICANN* уделяет

значительное внимание непрерывности деятельности, а также защите владельцев регистраций и правообладателей в период внедрения новых процессов. Комментарии сообщества демонстрируют растущую важность безопасности *DNS*, совершенствования механизмов обеспечения соответствия требованиям, а также завоевания доверия потребителей. Доверие потребителей, помимо прочего, включает концепцию постоянной работы уникальных идентификаторов и обеспечения согласованных результатов при их использовании. Возможности выбора на рынке подразумевают, помимо прочего, возможность доступа пользователей к уникальным идентификаторам на родных языках с использованием национальной письменности. К концу реализации этого плана может существовать более 100 000 000 новых имен во многих инновационных областях и на различных языках мира.

Стратегические цели. В этой сфере деятельности *ICANN* определила пять стратегических целей.

Сохранение единственной достоверной корневой зоны. ICANN обязана использовать для своей деятельности открытые и прозрачные процессы, которые предполагают конкуренцию и доменных имен и внесение поправок в соглашение об аккредитации регистраторов. Персонал и сообщество продолжат сотрудничество с *WIPO* другими авторитетными органами с целью разработки и внедрения положений политики в отношении защиты прав для защиты и реализации прав на интеллектуальную собственность в Интернете.

Повышение конкуренции в отрасли. Интернет — это место применения и источник значительных деловых и технологических новшеств. Конкуренция является важнейшей характеристикой отрасли, способной стимулировать инновации. Одна из целей *ICANN* состоит в том, чтобы вовремя разглядеть такие новшества и подкрепить ими устойчивое развитие системы уникальных идентификаторов путем продвижения справедливых возможностей для содействия и поддержки открытого доступа на связанные с Интернетом рынки по всему земному шару. Проекты *ICANN*, связанные с этой целью, по-прежнему призваны поддерживать развитие и реализацию открытых и прозрачных политик и процессов, которые предполагают конкуренцию. *ICANN* будет продвигать реализацию и внедрение протокола *IDNA* (ИДИ в приложениях), чтобы гарантировать правильную работу ИДИ. *ICANN* продолжит сотрудничество с сообществом, предоставляя необходимую помощь малобюджетным организациям. Работа персонала *ICANN* и сообщества будет направлена на сбор, оценку и учет опыта реализации таких открытых программ, как внедрение ИДИ и новых рДВУ.

Стратегические показатели. Вкратце, стратегическими показателями в области конкуренции, доверия потребителей и возможностей выбора на рынке являются:

- запуск программы ввода новых рДВУ и своевременная обработка заявок;
- количество ежегодно делегируемых нДВУ с ИДИ;
- ввод новых рДВУ и процедура ускоренного ввода ИДИ: внедрение показателей успеха, совпадающих с основными ценностями *ICANN* и исходными целями программы;
- измерение эффективности механизмов защиты прав, предусмотренных в программе ввода новых рДВУ;
- формулирование приоритетов региональных образовательных программ и отчеты о ходе их реализации;
- разработка, опубликование и соблюдение режима исполнения договорных обязательств для решения вопросов в новом расширенном пространстве ДВУ;
- ввод и своевременное развитие улучшений программы *Whois*, в особенности, в плане интернационализированных данных;
- документальное оформление и опубликование руководства по ИДИ в 2012 году;
- решение проблемы доменных имен, не совместимых с протоколом IDNA 2008.

Основные операции, включая деятельность *IANA*

Определение сферы деятельности. *ICANN* уполномочена решать следующие задачи: (*i*) координация назначения технических параметров Интернета для обеспечения универсальных возможностей подключения, (*ii*) реализация и контроль функций по координации пространства *IP*-адресов и эксплуатации полномочной системы корневых серверов *DNS* Интернета и (*iii*) координация распределения и назначения трех наборов уникальных идентификаторов (*DNS*, *IP*-адреса, порты и параметры); а также принимать необходимые меры для: (*iv*) неукоснительного прозрачного и ответственного ведения бюджета и оперативных процессов и (*v*) публикации годового отчета о выполнении положений Устава, стратегических и текущих планов. Роль *ICANN* в этой области характеризуется прямым контролем над собственными функциональными операциями и отражает способ реализации *ICANN* этих процессов, ее отчетность, соответствие договорным обязательствам, прозрачность и подотчетность.

Эта сфера деятельности предусматривает непрерывное совершенствование и достижение высочайшего уровня в каждой из следующих областей:

1. Оценка текущей среды.
2. Создание плана конкретных улучшений.
3. Оценка значимости улучшений после их реализации.

Текущее состояние дел. Основная деятельность *ICANN* направлена на наращивание потенциала и возможностей предоставлять услуги и координировать следующие системы уникальных идентификаторов Интернета: *DNS*, *IP*-адреса, номера АС, порты и параметры. *ICANN* управляет корневым *L*-сервером и имеет значительный опыт и документацию, которыми может поделиться с международным сообществом. Достижение наивысшего качества операций необходимо для поддержки процедуры ускоренного ввода ИДИ и программ по новым рДВУ. По мере роста и развития Интернета технические достижения (например, сертификацию номерных ресурсов Интернета, новые стандарты) следует рассматривать с точки зрения их влияния на эволюцию услуг и операций *ICANN*. В ходе осуществления этого плана возникает множество факторов, которые затрудняют выполнение операций. В их числе: ввод новых доменов верхнего уровня, рост масштабов подключения мирового сообщества к Интернету и быстро растущее число мобильных и других устройств. Корпорация *ICANN* начала выполнять операции *IANA* в 1998 г., заключив соглашение с правительством США. Срок действия текущего многолетнего договора истекает в 2012 г. *ICANN* имеет хорошие шансы выиграть тендер и продолжить выполнение функций *IANA*. Корпорация *ICANN*, включая ее агентство *IANA*, также эффективно сотрудничает с другими глобальными организациями по обслуживанию единого межплатформенного Интернета. Кроме того, в рамках своей основной деятельности *ICANN* координирует проведение в разных странах мира трех ежегодных конференций, которые позволяют собираться вместе группе многочисленных заинтересованных сторон для решения стоящих перед *ICANN* задач.

Стратегические цели. Ниже приведены стратегические цели для *IANA* и основной деятельности.

Безупречная работа IANA и непрерывная долгосрочная ответственность за выполнение функций IANA. ICANN считает своим долгом способствовать непрерывному высококачественному функционированию Агентства по распределению номеров Интернета (*IANA*) и других основных служб. Продолжение предоставления услуг *IANA* с сохранением нейтральной позиции будет зафиксировано в ожидаемом долгосрочном

договоре на выполнение функций *IANA*. *ICANN* продолжает инвестировать в инфраструктуру *IANA* и совершенствование процессов через модель Европейского фонда управления качеством (*EFQM*) для выполнения или превышения условий соглашений об уровне обслуживания *IANA*. В период действия этого плана *ICANN* разработает улучшения безопасности (такие как сертификация номерных ресурсов Интернета) и продолжит модернизацию своих процессов за счет автоматизации (в частности, внедрение системы управления корневой зоной). Агентство *IANA* будет и далее сосредотачивать усилия на своевременной обработке запросов на уникальные идентификаторы, включая управление *DNSSEC*. Мы будем реагировать на мониторинг работы *IANA* со стороны сообщества, но будем также реализовывать и наши собственные механизмы оценки и обратной связи.

Отказоустойчивое функционирование корневого сервера L. Эксплуатация корневого сервера *L* позволяет *ICANN* подавать личный пример и предоставляет международному интернет-сообществу прозрачную и открытую для сотрудничества модель функционирования корневых серверов. *ICANN* будет изыскивать возможности для распространения своих знаний в этой области через все доступные международные каналы. *ICANN* будет выступать в качестве управляющего корневой зоны верхнего уровня.

Непрерывное усовершенствование (достижение наивысшего качества работы). Корпорация *ICANN* продолжает реализацию начатой в 2010 году культурно-ориентированной программы повышения эффективности управления процессами и совершенствования систем и документации во всех областях основной деятельности. *ICANN* считает своим долгом улучшать текущую эффективность разработки политик и внедрения процессов и модели участия всех заинтересованных сторон глобального сообщества. Корпорация будет поддерживать текущую инициативу ОПРИ по улучшению процесса разработки политики (ПРП), а также поощрять и поддерживать другие инициативы. Содействие эффективному участию Правительственного консультативного комитета (ПКК) в процессе разработки политики, начиная с ранних этапов этого процесса. *ICANN* будет и далее повышать безопасность, стабильность и непрерывность своих собственных операций через Инициативу по повышению эффективности деятельности, чтобы гарантировать непрерывное совершенствование работы, привлечение и долговременное удержание персонала. Работа сотрудников в этих областях (удержание персонала, внутренние операционные системы, поддержка Правления) необходима для поддержки

главных целей, связанных со стабильностью и координацией DNS. Поэтому указанные цели тоже являются стратегическими по своему характеру. *ICANN будет продолжать улучшение корпоративной системы и средств управления для*: увеличения потенциала и масштабируемости оперативной рабочей нагрузки, повышения эффективности работы, сопровождаемого относительным сокращением текущих расходов, повышения целостности и доступности данных, ускорения создания и публикации отчетов, повышения доступности финансовой информации, улучшения службы поддержки клиентов (как внутренней, так и внешней), более устойчивого развития базовых технологий. ICANN реализует преимущества новой финансовой системы, которая улучшит взаимосвязь между стратегическими и оперативными планами, а также поможет определять рабочие бюджеты, выделяемые на поддержку каждой из четырех стратегических сфер деятельности, и обосновывать масштабы затрат.

Интернационализация. ICANN будет работать с сообществом над определением принципов, которые помогут направлять процесс интернационализации *ICANN*. Цель *ICANN* состоит в укреплении международной деятельности и присутствия путем обеспечения адекватных уровней обслуживания заинтересованных сторон во всем мире за счет работы на нескольких языках и в нескольких часовых поясах. Интернет представляет собой глобальную, виртуальную технологию, однако люди, заставляющие работать системы уникальных идентификаторов Интернета, находятся во всех географических регионах мира. Ввод новых ИДИ и ДВУ в период осуществления данного плана требует, чтобы *ICANN* продолжала наращивать свой потенциал и присутствие. Другой важный аспект укрепления деятельности — это сохранение или улучшение стандартов обслуживания и всех ключевых оперативных показателей в период реализации плана, включая управление последствиями ввода новых рДВУ и нДВУ с ИДИ. *ICANN* также будет эффективно сотрудничать с техническим сообществом, в частности, с *IETF*, управляющими корневых серверов, другими группами операторов сетей и сообществами РРИ.

Развитие конференций ICANN. ICANN ежегодно координирует проведение трех международных конференций, являющихся важными собраниями сообщества, в которое входит множество заинтересованных сторон. *ICANN* по-прежнему будет ставить перед собой и сообществом задачу развития модели проведения конференций *ICANN* для более эффективного учета изменений в составе и приоритетах многосторонней модели *ICANN*.

Стратегические показатели. Вкратце, стратегическими показателями для работы в области основной деятельности, включая *IANA*, являются:

- выполнение или превышение показателей, предусмотренных в соглашении об уровне обслуживания *IANA*;
- продление или замена договора на выполнение функций *IANA* в 2011 году;
- оценка EFQM, демонстрирующая улучшение с течением времени;
- развертывание инфраструктуры открытых ключей ресурсов (ИОКР) за период действия плана;
- абсолютно безотказное функционирование корневого сервера *L*;
- критерии, показатели и результаты программы обеспечения организационной эффективности;
- определение показателей уровней обслуживания международных заинтересованных сторон;
- внедрение в 2011 году новой финансовой информационной системы *ICANN*;
- разработка и публикация дополнительных показателей и отчетов по эффективности обеспечения соблюдения договорных обязательств.

Здоровая экосистема управления Интернетом

Определение сферы деятельности. *ICANN* работает в следующих направлениях (*i*) создание глобальных выгод для сообщества Интернета в целом, (*ii*) координация дискуссий внутри сообщества и разработка политик, согласующихся с миссией *ICANN*, (*iii*) сотрудничество, при необходимости, с соответствующими международными организациями, (*iv*) обеспечение того, чтобы решения по технической координации *DNS* принимались на благо сообщества, были подотчетными и прозрачными, и (*v*) работа в качестве организации, действующей в соответствии с законами свободного рынка, открытой и заинтересованной в любых отзывах сообщества, интересы которого *ICANN* ставит превыше всего. Роль *ICANN* в этой области заключается во вкладе в разработку, развертывание и функционирование надежных механизмов надлежащего управления системами уникальной идентификации Интернета. Для этого *ICANN* должна участвовать в работе и влиять на работу форумов управления Интернетом и использовать другие возможности для диалога с сообществом на эту тему, а также периодически оценивать прогресс в этой области. Многосторонняя модель предусматривает и предоставляет право голоса для различных групп, таких как: географические, правительственные, деловые, технические, нетехнические, поликультурные и расширенные. Кроме того, разработанные *ICANN* политики должны отвечать интересам общественности.

Текущее состояние дел. *ICANN* считает своим долгом работать на благо интернет-сообщества в целом. Общество в целом — это совокупность разнообразных и несовместимых сообществ, связанных Интернетом и работающих как сложная экосистема. Поскольку Интернет остается серьезным фактором роста валового национального продукта, ежедневной деятельности государств и действий в сфере глобальной безопасности, важность качественного управления Интернетом также возрастает. В сентябре 2009 г. Министерство торговли США и *ICANN* подписали документ «Подтверждение обязательств» (Подтверждение), в котором подтвердили передачу функций технической координации *DNS* Интернета организации, действующей по принципам частного сектора – *ICANN*. За последние несколько лет Организация Объединенных Наций и другие международные организации также расширили свое участие в управлении Интернетом. Сообщество и *ICANN* провели проверку выполнения обязательств в отношении подотчетности и прозрачности (ГППП) и, по указанию Правления *ICANN*, выполняют рекомендации ГППП. Другие проверки, предусмотренные в Подтверждении, выполняются в настоящее время. Модель управления с участием множества заинтересованных сторон завоевывает признание во всем мире и будет по-прежнему использоваться при неуклонном повышении требований и проведении проверок.

Стратегические цели. В сфере деятельности «Здоровая экосистема управления Интернетом» *ICANN* определила четыре стратегические цели. С каждой целью связаны проекты, работа персонала и сообщества для поддержки достижения стратегических целей в период осуществления этого плана. Стратегические цели таковы:

Стремиться стать образцовой международной организацией с многосторонним участием. ICANN стремится к сохранению своего статуса образцовой модели глобального управления, учитывающей интересы множества разных сторон. Для создания здоровой экосистемы управления Интернетом проверки и обсуждения должны носить открытый, международный и тщательный характер. *ICANN* будет активно участвовать в широком диапазоне конструктивных дебатов, связанных с управлением Интернетом, в партнерстве с другими организациями.

Увеличение многообразия заинтересованных сторон и укрепление сотрудничества между ними. В течение последнего года сообщество все в большей степени использовало совместные рабочие группы ОП и КК. *ICANN* обязуется использовать следующие методы поддержания и улучшения надежных механизмов учета мнения общественности, подотчетности и прозрачности для отражения общественных интересов

в ходе принятия решений и подотчетности всем заинтересованным сторонам. Стратегические проекты включают постоянное уточнение всеобъемлющей модели, которая предусматривает учет мнений многих заинтересованных сторон, поощрение и управление активным сбором мнений мирового сообщества. *ICANN* продолжит свои усилия по расширению участия сообщества, используя технологии более удаленного участия. Очень важен тот факт, что *ICANN* продолжит работу по удержанию и поддержке существующих членов сообщества, опираясь на результаты недавних усилий по формализации модели пересекающихся заинтересованных сторон (то есть, с одновременным привлечением ПКК, поддерживающих организаций и других консультативных комитетов). Модель, предусматривающая учет мнений многих заинтересованных сторон, допускает влияние правительств, корпораций, некоммерческих организаций и учитывает то, как они вписываются в систему именования и адресации. Многостороннее сообщество продолжает развиваться с одновременным смещением приоритетов. *ICANN* будет работать над расширением взаимодействия между заинтересованными сторонами для достижения большего согласия в сообществе и ускорения процесса разработки политики.

Подотчетность и прозрачность мирового класса. Непреложное правило *ICANN* — разрабатывать политики и принимать решения только на основе фактов. Сообщество и *ICANN* завершили проверку ГППП, в результате которой было сформулировано 27 рекомендаций. *ICANN* продолжит совместную работу с сообществом по выполнению рекомендаций ГППП. *ICANN* продолжит развитие политик Правления для отражения передовых практических методов в модели управления с участием множества заинтересованных сторон. Устав *ICANN* требует постоянной оценки соответствующих организаций поддержки и консультативных комитетов, чтобы гарантировать непрерывное улучшение структуры организации и повышение ответственности заинтересованных сторон. Работа персонала *ICANN* будет направлена на обеспечение подробного и аргументированного объяснения принятых решений, их мотивировки и источников данных.

Действия в интересах мировой общественности. ICANN инициировала программу глобального партнерства в 2006 году для создания сети международных контактных лиц с целью повышения степени участия на местном уровне. Она продолжит развитие этой программы, возможно, с привлечением местных контактных лиц ИДИ в конкретных регионах, чтобы удовлетворить потребности определенных сообществ и максимально повысить эффективность программы ввода

ИДИ. Кроме того, целью *ICANN* является сохранение стабильности системы уникальной идентификации. Поэтому корпорация признает права и участие различных заинтересованных сторон с разными полномочиями, такими как правоприменительная деятельность и обеспечение свободного доступа к информации. Для достижения своих целей *ICANN* будет участвовать в конструктивных заседаниях Форума управления Интернетом, сотрудничать с международными организациями, такими как ЕС и ОЭСР, в сфере разработки стандартов и передовых практик, принимать участие в обсуждениях, разработке документации и взаимодействовать с участниками отрасли в других областях. При осуществлении всей перечисленной деятельности *ICANN* руководствуется интересами мировой общественности.

Повышение доверия к руководящей роли ICANN. Одной из целей *ICANN* является внесение вклада в здоровую экосистему управления Интернетом. Правление *ICANN* создало Комитет по международным отношениям Правления, чтобы поддержать глобальные усилия *ICANN* по наращиванию потенциала. *ICANN* борется за обеспечение независимости Правления и за то, чтобы состав Правления отражал все многообразие участников многосторонней модели. Работа персонала обеспечит вклад интеллектуального капитала в международные форумы и обсуждения вопросов управления Интернетом, включая организованный под эгидой ООН Форум управления Интернетом и другие межправительственные форумы. Кроме того, программа грантов *ICANN* в партнерстве с другими организациями обеспечивает обучение для поддержки потребностей в сфере *DNS* в развивающихся странах.

Удобство международного участия. По мере развертывания все большего числа ИДИ, новые регионы мира смогут высказаться относительно своих приоритетов при управлении Интернетом. Это подразумевает ведение разъяснительной работы и реализацию программ, обеспечивающих больший вклад на периферии модели с участием множества заинтересованных сторон. *ICANN* обязуется использовать комплексный подход к ведению разъяснительной деятельности и улучшению стратегии работы на многих языках для повышения удобства участия в многосторонней модели *ICANN*. Задача обеспечения удобства участия влияет на системы, процессы, документацию, собрания, средства связи и многие другие аспекты деятельности *ICANN*. Цель *ICANN* состоит в постоянном поиске методов, технологий, языков и средств, которые повысят удобство участия всех людей в многосторонней экосистеме управления Интернетом.

Стратегические показатели. Вкратце, стратегическими показателями в области здоровой экосистемы Интернета являются:

• своевременное завершение проверок, предусмотренных документом «Подтверждение обязательств»;

• своевременные решения и действия Правления по реализации рекомендаций, относящихся к проверкам, предусмотренным документом «Подтверждение обязательств»;

• сохранение единственной достоверной корневой зоны;

• формализованное участие различных заинтересованных сторон в многосторонней модели;

• улучшение методов обратной связи с Правлением *ICANN*;

• количество международных событий по управлению Интернетом с конструктивным участием *ICANN*;

• количество стипендиатов программы грантов *ICANN* и тенденция ее развития, а также соответствующее расширение участия в процессах *ICANN*;

• соответствие международного состава и разнообразия навыков Правления *ICANN* требованиям Устава.

1.2. Форум по управлению интернетом (*Internet Governance Forum, IGF*). Динамичная коалиция по правам и принципам интернета (*Dynamic Coalition on Internet Rights and Principles*) Форума по управлению интернетом[1]

ПРЕДВАРИТЕЛЬНАЯ ХАРТИЯ ПО ПРАВАМ ЧЕЛОВЕКА И ПРИНЦИПАМ ИНТЕРНЕТА[2] *(2010 г.)*

Управление интернетом должно основываться на правах человека исходя из следующих ключевых принципов:

1. *Универсальность и равенство* (*Universality and Equality*). Все люди рождаются свободными и равными в достоинствах и правах, которые должны уважаться, защищаться и осуществляться в онлайн-среде.

[1] Форум по управлению интернетом действует под эгидой ООН, на основании мандата ООН (2006 г.). Динамичная коалиция по правам и принципам интернета Форума по управлению интернетом создана после Хайдарабадской встречи *IGF* в 2008 г. и включает более 320 зарегистрированных участников – представителей всех заинтересованных сторон.

[2] *Beta Version of the Charter of Human Rights and Principles of the Internet*. – URL: http://internetrightsandprinciples.org/site/ (неофициальный перевод М.Б. Касеновой).

2. *Права и социальная справедливость* (*Rights and Social Justice*). Интернет является пространством содействия, защиты и реализации прав человека и развития социальной справедливости. Каждый человек обязан уважать права человека и все другие права в онлайн-среде.

3. *Доступность* (*Accessibility*). Каждый имеет равное право на доступ и использование безопасного и открытого интернета.

4. *Самовыражение и общение* (*Expression and Association*). Каждый человек имеет право свободно искать, получать и распространять информацию в интернете без цензуры или иных препятствий. Каждый имеет также право свободно общаться посредством интернета и в интернете в общественных, политических, культурных и в иных целях.

5. *Частная жизнь и защита персональных данных* (*Privacy and Data Protection*). Каждый имеет право на неприкосновенность частной жизни в интернете. Это право включает в себя свободу от наблюдения, право на использование шифрования и право на анонимность в онлайн-среде. Каждый имеет также право на защиту персональных данных, включая контроль за сбором, хранением, обработкой, передачей и раскрытием информации о персональных данных.

6. *Жизнь, свобода и безопасность* (*Life, Liberty and Security*). Право на жизнь, свободу и личную неприкосновенность должно уважаться, охраняться и осуществляться в онлайн-среде. Эти права не должны ущемляться или использоваться в нарушение иных прав в онлайн-среде.

7. *Разнообразие* (*Diversity*). Культурное и языковое разнообразие в интернете должно поощряться, а технологическая и инновационная политика должны способствовать поощрению выражения культурного и языкового разнообразия.

8. *Равенство в сети* (*Network Equality*). Каждый должен иметь универсальный и открытый доступ к интернет-контенту, свободному от дискриминационных преимуществ, фильтрации или контроля трафика, осуществляемых по коммерческим, политическим или иным основаниям.

9. *Правила и нормы* (*Standards and Regulation*). Архитектура интернета, системы связи, а также форматы документов и форматы данных должны базироваться на открытых стандартах, обеспечивающих полную совместимость, возможность подключения и равные возможности для всех.

10. *Управление* (*Governance*). Права человека и социальная справедливость должны формировать нормативно-правовую основу, на базе которой функционирует интернет и осуществляется его управление. Нормативно-правовую основу следует формировать в режиме транспарентности и на многостороннем уровне, исходя из принципов открытости, широкого участия (инклюзивности) и отчетности.

1.3. Ассоциация прогрессивных коммуникаций (*Association for Progressive Communications, APC*)[1]

КОДЕКС ЛУЧШЕЙ ПРАКТИКИ ПО ИНФОРМАЦИИ, УЧАСТИЮ И ИНФОРМАЦИОННОЙ ОТКРЫТОСТИ (ПРОЗРАЧНОСТИ) УПРАВЛЕНИЯ ИНТЕРНЕТОМ. ВЕРСИЯ 1.1, ИЮНЬ 2010 г.[2]

Введение

Интернет приобретает все более важное значение во всех аспектах человеческого общества. Он постоянно развивается – в технологиях, в доступе к интернету и доли участия. Его влияние на социальную, экономическую, культурную и политическую жизнь стремительно растет. Практически каждый в настоящее время находится под влиянием интернета, услуг интернета, использования интернета, и соответственно управления интернетом, независимо от того насколько много или мало он использует интернет.

Развитие и управление интернетом в значительной степени базировалось на принципах прозрачности (транспарентности) и обмена информацией, участия всех заинтересованных на открытом обсуждении и процессов принятия решений. Эти принципы в значительной степени способствовали динамизму и всеобъемлемости интернета.

Настоящий Кодекс основывается на опыте многих организаций, связанных с управлением интернетом в целях укрепления открытости, информированности и участия общественности. **Настоящий Кодекс предназначен в качестве концептуальной основы принципов и рекомендаций**, которые помогут этим организациям поддерживать и обеспечивать прозрачность, открытость и подотчетность в условиях продолжающегося широкого распространения интернета, многообразия и значения интернета.

Способы, в которых данные принципы и рекомендации могут реализовываться, будут варьироваться в зависимости от роли и обстоятельств различных организаций, которые участвуют в этом процессе.

---

[1] См. подробнее об организации: URL: http://www.apc.org/en/about

[2] *Code of Good Practice on Information, Participation and Transparency in Internet Governance. Version 1.1, June 2010.* Кодекс является совместной инициативой Ассоциации прогрессивных коммуникаций, Совета Европы и Европейской экономической комиссии ООН (ЕЭК ООН). – URL: http://www.apc.org/en/system/files/COGP_IG_Version_1.1_June2010_EN.pdf; см. также: URL: www.intgovcode.org (неофициальный перевод М.Б. Касеновой).

Определения

В настоящем Кодексе термин **«управление интернетом»** понимается как разработка и применение правительствами, частным сектором и гражданским обществом при выполнении ими своей соответствующей роли общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение интернета, т.е. в соответствии с определением, выработанным в ходе Тунисского этапа, согласованным на Всемирной встрече на высшем уровне по вопросам информационного общества в 2005 году.

В настоящем Кодексе термин **«принятие решения»** охватывает все процессы, включенные в обсуждение и принятие решений по вопросам политики, стандартов, координации и администрирования относительно интернета и для интернета, а также относительно тех интернет-отношений, которые связаны с иными сферами государственной политики. Эти процессы включают в себя все процессы, начиная с включения их в повестку дня до их применения в контексте «управления интернетом», содержательно понимаемом так, как было обозначено выше.

Принципы управления интернетом

Существует много различных организаций, имеющих отношение к управлению интернетом. Несмотря на то, что эти организации различаются по их роли и характеру, они разделяют приверженность к прозрачности и обмену информацией, мультистейкхолдеризму, открытому обсуждению и принятию решений, тому подходу, который возник в ходе развития интернета.

Такая приверженность вытекает из Принципов Всемирной встречи на высшем уровне по вопросам информационного общества, итоговых документов Тунисского этапа Всемирной встречи на высшем уровне по вопросам информационного общества, закрепивших следующее: «Международное управление интернетом должно быть многосторонним, открытым и демократичным, с широким участием правительств, частного сектора, гражданского общества и международных организаций. Такая приверженность должна гарантировать справедливое распределение ресурсов, облегчать доступ в интернет для всех и обеспечивать стабильное и безопасное функционирование интернета с учетом многоязычия».

Следующие принципы формируют основу для обеспечения всеобъемлемости и открытости управления интернетом:

1. Развитие интернета сбалансировало участие и требования различных заинтересованных групп, в частности правительств, бизнеса, гражданского общества и технического интернет-сообщества. Участие

всех заинтересованных сообществ сформировалось и должно оставаться общепринятой нормой управления интернетом.

2. Развитие интернета крайне важно для всех обществ. В этой связи существенное значение имеет то, чтобы заинтересованные стороны всех сообществ, с их различным социальным, экономическим и культурным опытом принимали участие в развитии интернета.

3. Развитие интернета требует вовлечения всех типов интернет-участников и должно отражать их разнообразные ценности, интересы и потребности. Интернет-участниками должны быть не только специалисты интернета и конечные пользователи, но и будущие пользователи интернета и те, кто не может пользоваться или не использует интернет самостоятельно.

4. Развитие интернета требует, чтобы обсужденные вопросы, разработанные политики и решения исполнялись в разных географических широтах, на глобальном и региональном, национальном и локальном уровнях, тем самым обеспечивая разнообразие участия различных заинтересованных сторон на всех этих уровнях.

5. Интернет все активнее взаимодействует со многими другими областями управления. Это важно и для интернета, и для общества в целом, для тех, кто в первую очередь связан с политикой в иных областях, таких как телекоммуникации и средства массовой информации, в области социального и экономического развития, в области окружающей среды и прав человека, – все они могут внести свой вклад в разработку политики и принятия решений, минуя пределы границ своих традиционных сфер.

6. В целях облегчения вышеуказанных взаимодействий заинтересованных групп, следует разрабатывать и поддерживать инклюзивные институциональные интерфейсы.

Хорошо информированные физические лица и организации обеспечивают основу открытого и всеобъемлющего глобального интернета. Доступ к информации и возможность участия в принятии решений, касающихся интернета, и связь интернета с другими аспектами жизни общества являются существенными, если эти принципы взаимодействия достигнуты.

Правила, касающиеся информации

Определения

В настоящем Кодексе термин **«информация»** включает в себя две составляющие:

справочную информацию, используемую в процессах принятия решений и материалы, которые будут поняты участниками и потенциальными

участниками в процессе принятия решений, другими заинтересованными сторонами и широкой общественностью;

материалы (программы, пояснительную документацию, информацию, используемую в процессах принятия решений, протоколы и т.д.), которые сами являются формой процесса принятия решений.

1. Решения по управлению интернетом и управленческие решения, связанные с управлением интернетом, должны быть (и будут) открытыми, прозрачными и всеобъемлющими.

2. Вся информация, которая связана с управлением интернетом и принятием решений или которая связана с деятельностью организаций по управлению интернетом, должна быть в общественном доступе и быть легко доступна для всех потенциальных участников в том формате и способе, который удобен для этих пользователей. Изъятия из настоящих Правил должны стать предметом открытой дискуссии и публичных разъяснений причин таких изъятий.

3. Организациям, связанным с вопросами управления интернетом, следует активно содействовать доступу к информации и содействовать повышению уровня знаний в интернет-сообществе относительно их работы в целом, в вопросах, которыми они занимаются, о тех решениях, которые они принимают, и о механизмах, с помощью которых могут быть достигнуты принимаемые ими решения.

Для этого организации, связанные с вопросами управления интернетом, должны подготовить и распространить для интернет-сообщества, средств массовой информации и широкой общественности информационные ресурсы, в которых обобщается их работа, освещаются конкретные вопросы и процессы принятия решений.

5. Эти информационные ресурсы должны облегчить понимание и осознанный выбор пользователей. Они должны содержать материалы, которые написаны таким образом, чтобы быть легко понятыми теми, кто не имеет специальных знания или опыта.

6. Организации, связанные с вопросами управления интернетом, должны стремиться сделать свою информацию доступной на любых языках, форматах и стандартах, с тем чтобы содействовать интеграции всех потенциальных групп пользователей.

7. Организации, связанные с вопросами управления интернетом, должны обеспечить связь с контактными лицами, в том числе с координаторами, с которыми можно связаться в оффлайновом режиме для получения дальнейшей информации относительно их работы, конкретных вопросов, по которым приняты решения, и процессов, а также информации о механизмах, посредством которых реализуются принятые решения.

8. Организации, связанные с вопросами управления интернетом, должны стремиться распространить настоящую информацию относительно принципов и практик через взаимодействие и совместную работу с другими органами управления, включая органы, деятельность которых находится в основном за пределами интернета.

Правила относительно участия

Определения

В настоящем Кодексе термин **«участие»** означает возможности, которые предоставляются тем, кто желает внести свой вклад в процесс принятия решений, которые (по их мнению) влияют на них (или в отношении которых они считают, что их голос должен быть услышан), а также означает механизмы, которые позволяют им внести свой вклад.

1. Организации, связанные с вопросами управления интернетом, и процессы, связанные с вопросами управления интернетом, должны позволять и поощрять всех тех, кто желает участвовать в процессах принятия решений, касающихся управления интернетом, чтобы внести свой вклад, с расчетом на то, что их мнение будет учтено.

2. Организации, связанные с вопросами управления интернетом, должны активно содействовать участию в своей работе всех тех, кто затронут, или может быть затронут, или считают себя затронутыми решениями, которые они принимают, в том числе индивидов или организаций от всех групп заинтересованных сторон сообществ и регионов мира.

3. Организации, связанные с вопросами управления интернетом, должны стремиться включить в процесс своих обсуждений государства и народы, которые недостаточно представлены, в том числе тех, кто в настоящее время не является постоянным пользователем интернета, и эти организации должны учитывать потребности своих будущих пользователей.

4. Любой индивид или организация должны иметь возможность инициировать идеи для обсуждения политики интернета, разработки стандартов, координации или администрирования, а также по вопросам управления и структуры организаций, связанных с вопросами управления интернетом. Они также должны иметь возможность принимать участие в таких дискуссиях.

5. Возможности участвовать в работе организаций, связанных с управлением интернетом, должны получить широкое распространение с тем, чтобы все желающие принять участие были проинформированы. Организации, связанные с управлением интернетом, должны признать,

что качество доступа в интернет может повлиять на способность потенциальных участников сотрудничать с ними, а также содействовать участию тех, кто не смог принять участие из-за плохого качества связи.

6. Для содействия участию и взаимодействию организации, связанные с вопросами управления интернетом, должны готовить и распространять ясную информацию о способах участия в их политике, в стандартах, в координационных и административных процессах. Такие организации должны признать, что отсутствие знаний и опыта может стать барьером для участия, и они должны предложить возможные варианты для новых участников в форме персонального участия или участия в онлайн-встречах.

7. Организации, связанные с вопросами управления интернетом, должны стремиться обеспечить участие в процессе принятия решений независимо от физического местонахождения лиц, дать возможность прибыть на место проведения встреч независимо от финансовых ресурсов. Усилия в достижении названных мер должны включать оффлайновые и иные механизмы для удовлетворения потребностей конкретных сообществ, а также возможность удаленного онлайн-участия.

8. Организации, связанные с вопросами управления интернетом, должны стремиться расширять настоящие принципы с помощью диалога и совместных разработок политики с другими органами управления, в том числе органами, основная деятельность которых находится за пределами интернета.

Мониторинг и обзор

Организации, связанные с вопросами управления интернетом, должны регулярно пересматривать свою информацию, участие и механизмы управления в свете настоящего Кодекса в целях использования результатов таких проверок, повышения инклюзивности, качества, прозрачности, своевременности и подотчетности принятия решений, а также целостности развития интернета. Это должно включать возможности для участия всех заинтересованных сторон. Методы достижения этой цели могут включать в себя независимую экспертизу и иные совместные или оценочные методы. Организации, связанные с вопросами управления интернетом, должны обнародовать результаты проведенных проверок.

2. Государства

2.2. Российская Федерация

УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ «О СОЗДАНИИ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ»

от 15 января 2013 г. № 31с

(*Выписка*)

В целях обеспечения информационной безопасности Российской Федерации постановляю:

1. Возложить на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

2. Определить основными задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

3. Установить, что Федеральная служба безопасности Российской Федерации:

а) организует и проводит работы по созданию государственной системы, названной в пункте 1 настоящего Указа, осуществляет контроль за исполнением этих работ, а также обеспечивает во взаимодействии с государственными органами функционирование ее элементов;

б) разрабатывает методику обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети государственных органов и по согласованию с их владельцами – на иные информационные системы и информационно-телекоммуникационные сети;

в) определяет порядок обмена информацией между федеральными органами исполнительной власти о компьютерных инцидентах, связанных с функционированием информационных ресурсов Российской Федерации;

г) организует и проводит в соответствии с законодательством Российской Федерации мероприятия по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

д) разрабатывает методические рекомендации по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак;

е) определяет порядок обмена информацией между федеральными органами исполнительной власти и уполномоченными органами иностранных государств (международными организациями) о компьютерных инцидентах, связанных с функционированием информационных ресурсов, и организует обмен такой информацией.

4. Настоящий Указ вступает в силу со дня его подписания.

Президент
Российской Федерации
В. ПУТИН

Москва, Кремль
15 января 2013 года
№ 31с

КОНЦЕПЦИЯ ВНЕШНЕЙ ПОЛИТИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ[1]

(Утверждена Президентом Российской Федерации 12 февраля 2013 г.)

I. Общие положения

1. Концепция внешней политики Российской Федерации (далее – Концепция) представляет собой систему взглядов на базовые принципы, приоритетные направления, цели и задачи внешнеполитической деятельности Российской Федерации.

2. Нормативно-правовую основу Концепции составляют Конституция Российской Федерации, федеральные законы, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, Указ Президента Российской Федерации от 7 мая 2012 г. № 605 «О мерах по реализации внешнеполитического курса Российской Федерации», а также Стратегия национальной безопасности Российской Федерации до 2020 года, Военная доктрина Российской Федерации, нормативные правовые акты Российской Федерации, регулирующие деятельность федеральных органов государственной власти в сфере внешней политики, и другие аналогичные документы.

3. Стремительное ускорение глобальных процессов в первом десятилетии XXI века, усиление новых тенденций в мировом развитии требуют по-новому взглянуть на ключевые направления динамично меняющейся ситуации в мире, переосмыслить приоритеты внешней политики России с учетом ее возросшей ответственности за формирование международной повестки дня и основ международной системы.

4. В соответствии с высшим приоритетом национальной безопасности – обеспечением защищенности личности, общества и государства – главные внешнеполитические усилия должны быть сосредоточены на достижении следующих основных целей:

а) обеспечение безопасности страны, сохранение и укрепление ее суверенитета и территориальной целостности, прочных и авторитетных позиций в мировом сообществе, в наибольшей мере отвечающих интересам Российской Федерации как одного из влиятельных и конкурентоспособных центров современного мира;

б) создание благоприятных внешних условий для устойчивого и динамичного роста экономики России, ее технологической модер-

[1] СПС «КонсультантПлюс».

низации и перевода на инновационный путь развития, повышения уровня и качества жизни населения, укрепления правового государства и демократических институтов, реализации прав и свобод человека;

в) активное продвижение курса на всемерное укрепление международного мира, всеобщей безопасности и стабильности в целях утверждения справедливой и демократической международной системы, основанной на коллективных началах в решении международных проблем, на верховенстве международного права, прежде всего на положениях Устава ООН, а также на равноправных и партнерских отношениях между государствами при центральной координирующей роли ООН как основной организации, регулирующей международные отношения;

г) формирование отношений добрососедства с сопредельными государствами, содействие устранению имеющихся и предотвращению возникновения новых очагов напряженности и конфликтов в прилегающих к Российской Федерации регионах;

д) развитие двусторонних и многосторонних отношений взаимовыгодного и равноправного партнерства с иностранными государствами, межгосударственными объединениями, международными организациями и форумами на основе принципов уважения независимости и суверенитета, прагматизма, транспарентности, многовекторности, предсказуемости, неконфронтационного отстаивания национальных приоритетов. Развертывание широкого и недискриминационного международного сотрудничества, содействие становлению гибких внеблоковых сетевых альянсов, активное участие в них России;

е) укрепление торгово-экономических позиций России в системе мирохозяйственных связей, дипломатическое сопровождение интересов отечественных экономических операторов за рубежом, недопущение дискриминации российских товаров, услуг, инвестиций, использование возможностей международных и региональных экономических и финансовых организаций в этих целях;

ж) всесторонняя защита прав и законных интересов российских граждан и соотечественников, проживающих за рубежом, отстаивание в различных международных форматах российских подходов по теме защиты прав человека;

з) распространение и укрепление позиций русского языка в мире, популяризация культурных достижений народов России, консолидация русской диаспоры за рубежом;

и) содействие развитию конструктивного диалога и партнерства между цивилизациями в интересах укрепления согласия и взаимообогащения различных культур и религий.

II. Современный мир и внешняя политика Российской Федерации

5. Главной, знаковой чертой современного этапа международного развития являются глубинные сдвиги в геополитическом ландшафте, мощным катализатором которых стал глобальный финансово-экономический кризис. Международные отношения переживают переходный период, существо которого заключается в формировании полицентричной международной системы. Этот процесс проходит непросто, сопровождается повышением турбулентности экономического и политического развития на глобальном и региональном уровнях. Международные отношения продолжают усложняться, их развитие становится все более труднопредсказуемым.

6. Продолжают сокращаться возможности исторического Запада доминировать в мировой экономике и политике. Происходит рассредоточение мирового потенциала силы и развития, его смещение на Восток, в первую очередь в Азиатско-Тихоокеанский регион. Выход на авансцену мировой политики и экономики новых игроков на фоне стремления западных государств сохранить свои привычные позиции сопряжен с усилением глобальной конкуренции, что проявляется в нарастании нестабильности в международных отношениях.

7. На фоне снижения опасности развязывания крупномасштабной войны, в том числе ядерной, меняется военное соотношение сил между различными государствами и группами государств. Стремление к наращиванию и модернизации наступательных потенциалов, созданию и развертыванию новых видов вооружений размывает структуру глобальной безопасности, цементируемую системой договоров и соглашений в области контроля над вооружениями.

8. В условиях глобальной турбулентности и растущей взаимозависимости государств и народов уже не имеют перспектив попытки строить отдельные «оазисы спокойствия и безопасности», а единственно надежной страховкой от возможных потрясений является соблюдение универсальных принципов равной и неделимой безопасности применительно к евроатлантическому, евразийскому и азиатско-тихоокеанскому пространствам.

9. На современном этапе традиционные военно-политические союзы не могут обеспечить противодействие всему спектру современных вызовов и угроз, являющихся трансграничными по своему характеру. На смену блоковым подходам к решению международных проблем приходит сетевая дипломатия, опирающаяся на гибкие формы участия

в многосторонних структурах в целях эффективного поиска решений общих задач.

10. На передний план выдвигаются, наряду с военной мощью, такие важные факторы влияния государств на международную политику, как экономические, правовые, научно-технические, экологические, демографические и информационные. Все больший вес приобретают вопросы обеспечения устойчивого развития, духовного и интеллектуального развития населения, роста его благосостояния, повышения уровня инвестиций в человека. Экономическая взаимозависимость государств является одним из ключевых факторов поддержания международной стабильности.

11. Осязаемо заявляют о себе финансово-экономические вызовы на фоне накопления кризисных элементов в мировой экономике. Нерешенность структурных проблем и затяжная депрессия в ведущих странах Запада негативно влияют на глобальное развитие. Незавершенность восстановительных процессов в условиях долгового кризиса в Европе и продолжающегося сползания еврозоны в рецессию представляет серьезные риски для будущего. Особую актуальность приобретают международные усилия по созданию новых, более сбалансированных и отвечающих реалиям глобализации мировых торговой и валютно-финансовой систем.

12. Возрастает конкуренция вокруг распределения стратегических ресурсов, которая лихорадит сырьевые биржи и рынки. Качественные трансформации происходят в энергетической сфере, что связано в том числе с использованием инновационных технологий добычи трудноизвлекаемых запасов углеводородов. В то время, когда для обеспечения экономической безопасности государств все больше требуется диверсификация их присутствия на мировых рынках, наблюдается ужесточение необоснованных ограничений и других дискриминационных мер.

13. Глобальная конкуренция впервые в новейшей истории приобретает цивилизационное измерение и выражается в соперничестве различных ценностных ориентиров и моделей развития в рамках универсальных принципов демократии и рыночной экономики. Все более громко заявляет о себе культурно-цивилизационное многообразие современного мира.

14. Оборотной стороной процессов глобализации становится тенденция повышения значения фактора цивилизационной идентичности. Стремление вернуться к своим цивилизационным корням отчетливо прослеживается в событиях на Ближнем Востоке и в Северной Африке, где политическое и социально-экономическое обновление общества зачастую проходит под лозунгом утверждения исламских

ценностей. Схожие процессы наблюдаются и в других регионах, что выводит в разряд первоочередных приоритетов мировой политики задачу предотвращения межцивилизационных разломов, наращивания усилий в интересах формирования партнерства культур, религий и цивилизаций, призванного обеспечить гармоничное развитие человечества. В этих условиях попытки навязывания другим собственной шкалы ценностей чреваты усилением ксенофобии, нетерпимости и конфликтности в международных делах, а в конечном итоге – сползанием к хаосу и неуправляемости в международных отношениях. Негативно на перспективы укрепления глобальной стабильности влияет обозначающаяся тенденция реидеологизации международных отношений.

15. Опасность для международного мира и стабильности представляют попытки регулировать кризисы путем применения вне рамок Совета Безопасности ООН одностороннего санкционного давления и иных мер силового воздействия, включая вооруженную агрессию. В отдельных случаях открыто игнорируются основополагающие международно-правовые принципы неприменения силы, прерогативы Совета Безопасности ООН, допускается произвольное прочтение его резолюций, реализуются концепции, направленные на свержение законной власти в суверенных государствах с использованием лозунгов защиты гражданского населения. Применение принудительных мер и вооруженной силы в обход Устава ООН и Совета Безопасности ООН неспособно устранить глубокие социально-экономические, межэтнические и другие противоречия, лежащие в основе конфликтов. Оно лишь ведет к расширению конфликтного пространства, провоцирует напряженность и гонку вооружений, усугубляет межгосударственные противоречия, разжигает национальную и религиозную рознь.

16. На первый план в современной международной политике выходят имеющие трансграничную природу новые вызовы и угрозы, стремительно возрастают их уровни, диверсифицируются их характер и география. Прежде всего, это опасность распространения оружия массового уничтожения и средств его доставки, международный терроризм, неконтролируемый трафик оружия и боевиков, радикализация общественных настроений, провоцирующая религиозный экстремизм и этноконфессиональные антагонизмы, нелегальная миграция, морское пиратство, незаконный оборот наркотиков, коррупция, региональные и внутренние конфликты, дефицит жизненно важных ресурсов, демографические проблемы, глобальная бедность, экологические и санитарно-эпидемиологические вызовы, изменение климата, угрозы информационной и продовольственной безопасности.

17. Глубоко трансформируется транснациональная организованная преступность, приобретающая в условиях глобализации макроэкономическое измерение, что приводит к появлению новых криминальных «центров силы», аккумулирующих значительные ресурсы и последовательно расширяющих сферы своего влияния, в том числе путем проникновения во властные структуры различных государств, финансовые и экономические институты, установления связей с террористическими и экстремистскими организациями.

18. Глобальные вызовы и угрозы требуют адекватного ответа со стороны международного сообщества, его солидарных усилий при центральной координирующей роли ООН и с учетом объективной взаимосвязанности вопросов безопасности, обеспечения устойчивого развития и защиты прав человека.

19. В условиях децентрализации глобальной системы управления укрепляется ее региональный уровень как основа – наряду с ООН – полицентричной модели, воплощающей многообразие мира, его неоднородность и многоукладность. Новые центры экономического роста и политического влияния все чаще и увереннее берут на себя ответственность за дела в своих регионах. Региональная интеграция становится действенным инструментом повышения конкурентоспособности ее участников. Сетевые форматы и объединения, торговые пакты и иные экономические договоренности, усиление роли региональных резервных валют являются факторами укрепления безопасности и финансово-экономической стабильности.

20. Неотъемлемой составляющей современной международной политики становится «мягкая сила» – комплексный инструментарий решения внешнеполитических задач с опорой на возможности гражданского общества, информационно-коммуникационные, гуманитарные и другие альтернативные классической дипломатии методы и технологии. Вместе с тем усиление глобальной конкуренции и накопление кризисного потенциала ведут к рискам подчас деструктивного и противоправного использования «мягкой силы» и правозащитных концепций в целях оказания политического давления на суверенные государства, вмешательства в их внутренние дела, дестабилизации там обстановки, манипулирования общественным мнением и сознанием, в том числе в рамках финансирования гуманитарных проектов и проектов, связанных с защитой прав человека, за рубежом.

21. Подлинное объединение усилий международного сообщества требует формирования ценностной основы совместных действий, опоры на общий духовно-нравственный знаменатель, который всегда

существовал у основных мировых религий, включая такие принципы и понятия, как стремление к миру и справедливости, достоинство, свобода и ответственность, честность, милосердие и трудолюбие.

22. Внешняя политика является одним из важнейших инструментов поступательного развития страны, обеспечения ее конкурентоспособности в глобализирующемся мире.

23. Российская Федерация, являясь постоянным членом Совета Безопасности ООН, участницей целого ряда влиятельных международных организаций, региональных структур, механизмов межгосударственного диалога и сотрудничества, обладая значительными ресурсами во всех областях жизнедеятельности, интенсивно развивая отношения с ведущими государствами и объединениями в различных частях мира в рамках многовекторного внешнеполитического курса, последовательно интегрируясь в мировую экономику и политику в качестве ответственного и конструктивного члена международного сообщества, способствует формированию позитивной, сбалансированной и объединительной международной повестки дня, решению глобальных и региональных проблем.

24. Фундаментальный характер и стремительный темп перемен создают для Российской Федерации, наряду с серьезными рисками, одновременно и новые возможности. Россия проводит самостоятельный и независимый внешнеполитический курс, продиктованный ее национальными интересами и опирающийся на безусловное уважение международного права.

25. Внешняя политика России является открытой, предсказуемой и прагматичной. Она характеризуется последовательностью, преемственностью и отражает уникальную, сформировавшуюся за века роль нашей страны как уравновешивающего фактора в международных делах и в развитии мировой цивилизации.

26. Россия всецело осознает свою особую ответственность за поддержание безопасности в мире как на глобальном, так и на региональном уровне и нацелена на совместные действия со всеми заинтересованными государствами в целях решения общих задач. Россия будет работать на опережение и упреждение событий, оставаясь готовой к любому варианту развития международной обстановки.

III. Приоритеты Российской Федерации в решении глобальных проблем

27. Многообразие и сложность международных проблем и кризисных ситуаций предполагают своевременную прогнозную оценку

приоритетности каждой из них во внешнеполитической деятельности Российской Федерации. Использование политико-дипломатических, правовых, военных, экономических, финансовых и иных инструментов при решении внешнеполитических задач должно быть соразмерно их реальному значению для обеспечения внешнеполитических интересов России и осуществляться при должной скоординированности действий всех ветвей власти и соответствующих ведомств.

Формирование нового мироустройства

28. Россия проводит политику, направленную на создание стабильной и устойчивой системы международных отношений, опирающейся на международное право и основанной на принципах равноправия, взаимного уважения, невмешательства во внутренние дела государств. Такая система призвана обеспечить надежную и равную безопасность каждого члена мирового сообщества в политической, военной, экономической, информационной, гуманитарной и иных областях.

29. Центром регулирования международных отношений и координации мировой политики в XXI веке должна оставаться ООН, которая доказала свою безальтернативность и наделена уникальной легитимностью. Россия поддерживает усилия по укреплению ее центральной и координирующей роли. Это предполагает:

а) обеспечение незыблемости ключевых положений и принципов Устава ООН, всемерное укрепление ее потенциала в целях рационального адаптирования ООН к новым мировым реалиям при сохранении ее межгосударственной природы;

б) дальнейшее повышение эффективности деятельности Совета Безопасности ООН, несущего главную ответственность за поддержание международного мира и безопасности, придание этому органу в процессе рационального реформирования ООН большей представительности при обеспечении должной оперативности в его работе. Любые решения по созданию дополнительных мест в Совете Безопасности ООН должны приниматься на основе самого широкого согласия государств – членов ООН. Статус пяти постоянных членов Совета Безопасности ООН должен быть сохранен.

30. Россия придает большое значение обеспечению устойчивой управляемости мирового развития, что требует коллективного лидерства ведущих государств мира, которое должно быть представительным в географическом и цивилизационном отношениях и осуществляться при полном уважении центральной и координирующей роли ООН.

В этих целях Россия будет наращивать взаимодействие в таких форматах, как «Группа двадцати», БРИКС (Бразилия, Россия, Индия, Китай, ЮАР), «Группа восьми», ШОС (Шанхайская организация сотрудничества), РИК (Россия, Индия и Китай), а также с использованием других структур и диалоговых площадок.

Верховенство права в международных отношениях

31. Россия последовательно выступает за укрепление правовых основ в международных отношениях, добросовестно соблюдает международно-правовые обязательства. Поддержание и укрепление международной законности – одно из приоритетных направлений ее деятельности на международной арене. Верховенство права призвано обеспечить мирное и плодотворное сотрудничество государств при соблюдении баланса их зачастую не совпадающих интересов, а также гарантировать стабильность мирового сообщества в целом. Россия намерена:

а) поддерживать коллективные усилия по укреплению правовых основ в межгосударственных отношениях;

б) противодействовать попыткам отдельных государств или групп государств подвергать ревизии общепризнанные нормы международного права, отраженные в универсальных документах – Уставе ООН, Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом ООН 1970 года, а также в Заключительном акте Совещания по безопасности и сотрудничеству в Европе (г. Хельсинки, 1 августа 1975 г.). Для международного мира и правопорядка особенно опасно осуществляемое в угоду политической конъюнктуре и интересам отдельных государств произвольное толкование важнейших международно-правовых норм и принципов, таких как: неприменение силы или угрозы силой, мирное разрешение международных споров, уважение суверенитета государств и их территориальной целостности, право народов на самоопределение. Опасны также попытки выдать нарушения международного права за его «творческое» применение. Недопустимо, чтобы под предлогом реализации концепции «ответственности по защите» осуществлялись военные интервенции и прочие формы стороннего вмешательства, подрывающие устои международного права, основанные на принципе суверенного равенства государств;

в) содействовать кодификации и прогрессивному развитию международного права, прежде всего осуществляемым под эгидой ООН,

достижению универсального участия в международных договорах ООН, их единообразному толкованию и применению;

г) продолжать усилия по совершенствованию санкционного инструментария ООН, вести дело к тому, чтобы решения о введении санкций принимались только Советом Безопасности ООН на коллегиальной основе после всесторонней проработки, прежде всего с учетом их эффективности для решения задач поддержания международного мира и безопасности и ненанесения ущерба гуманитарной ситуации;

д) вести дело к завершению международно-правового оформления государственной границы Российской Федерации, а также границ морского пространства, в отношении которого она осуществляет суверенные права и юрисдикцию, при безусловном обеспечении национальных интересов России, прежде всего в сфере безопасности и экономики, исходя из задачи укрепления доверия и сотрудничества с сопредельными государствами.

Укрепление международной безопасности

32. Россия последовательно выступает за снижение роли фактора силы в международных отношениях при одновременном укреплении стратегической и региональной стабильности. В этих целях Российская Федерация:

а) неукоснительно соблюдает свои международные обязательства по международным договорам в сфере контроля над вооружениями, а также принимает меры по укреплению доверия в военной сфере, добиваясь того же от своих партнеров; участвует в разработке и заключении новых договоренностей в этих областях, отвечающих ее национальным интересам и учитывающих все без исключения факторы, влияющие на стратегическую стабильность, на основе принципов равноправия и неделимости безопасности;

б) придает приоритетное значение выполнению Договора между Российской Федерацией и Соединенными Штатами Америки о мерах по дальнейшему сокращению и ограничению стратегических наступательных вооружений;

в) подтверждает неизменность курса на создание многосторонних политических и правовых основ универсального и прочного режима нераспространения ядерного оружия, других видов оружия массового уничтожения и средств их доставки; выступает за соблюдение Договора о нераспространении ядерного оружия, Конвенции о запрещении разработки, производства и накопления запасов бактериологического

(биологического) и токсинного оружия и об их уничтожении, а также Конвенции о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении; активно участвует в деятельности многосторонних режимов экспортного контроля, а также в международных усилиях в сфере контроля за оборотом материалов и технологий двойного назначения, содействует скорейшему вступлению в силу Договора о всеобъемлющем запрещении ядерных испытаний; выступает за создание глобального режима ракетного нераспространения на основе юридически обязывающей договоренности и за придание глобального характера обязательствам по Договору между СССР и США о ликвидации их ракет средней дальности и меньшей дальности;

г) поддерживает процесс создания зон, свободных от ядерного оружия и других видов оружия массового уничтожения;

д) выступает за укрепление технической и физической ядерной безопасности в глобальном масштабе, в частности за совершенствование международно-правовых механизмов обеспечения ядерной безопасности и предотвращения актов ядерного терроризма;

е) выступает за предотвращение размещения оружия в космосе, включая заключение соответствующего международного договора, развитие мер транспарентности и доверия в космической деятельности, создание системы коллективного реагирования на равноправной основе на возможные ракетные вызовы и против односторонних ничем не ограниченных действий по наращиванию противоракетной обороны одним государством или группой государств, наносящих ущерб стратегической стабильности и международной безопасности;

ж) в интересах решения проблем стратегической стабильности выступает за развитие двустороннего и многостороннего взаимодействия государств, прежде всего обладающих ядерным оружием, в целях обеспечения общей безопасности в духе стратегической открытости, в том числе в сфере доступности для всех заинтересованных стран благ «мирного атома»;

з) будет принимать необходимые меры в интересах обеспечения национальной и международной информационной безопасности, предотвращения угроз политической, экономической и общественной безопасности государства, возникающих в информационном пространстве, для борьбы с терроризмом и иными криминальными угрозами в сфере применения информационно-коммуникационных технологий, противодействовать их использованию в военно-политических целях, противоречащих международному праву, включая

действия, направленные на вмешательство во внутренние дела, а также представляющие угрозу международному миру, безопасности и стабильности;

и) будет добиваться выработки под эгидой ООН правил поведения в области обеспечения международной информационной безопасности;

к) поддерживает международные усилия по противодействию незаконному обороту легкого и стрелкового оружия;

л) в контексте усилий по укреплению региональной стабильности в Европе будет добиваться приведения европейского режима контроля над обычными вооружениями в соответствие с современными реалиями, а также безусловного соблюдения всеми сторонами согласованных мер укрепления доверия и безопасности;

м) считая международное миротворчество действенным инструментом урегулирования вооруженных конфликтов и решения задач государственного строительства на посткризисной стадии, намерена участвовать в международной миротворческой деятельности под эгидой ООН и в рамках взаимодействия с региональными и международными организациями; будет вносить активный вклад в совершенствование превентивного антикризисного потенциала ООН;

н) при подготовке решений Совета Безопасности ООН в области обеспечения международной безопасности, включая учреждение новых миротворческих операций или продление действующих, твердо выступает за разработку четких, не допускающих произвольных интерпретаций миротворческих мандатов, особенно связанных с применением силы, и обеспечение строгого контроля за их реализацией;

о) рассматривает статью 51 Устава ООН как адекватную и не подлежащую ревизии правовую основу для применения силы в порядке самообороны, в том числе в условиях существования таких угроз миру и безопасности, как международный терроризм и распространение оружия массового уничтожения;

п) рассматривает в качестве важнейшей национальной и внешнеполитической задачи борьбу с международным терроризмом, выступает за системное и комплексное использование политико-правовых, информационно-пропагандистских, социально-экономических и специальных мер с упором на превентивную составляющую такого противодействия на основе глобальных и региональных антитеррористических конвенций;

р) в соответствии с международным правом и своим законодательством применяет все необходимые меры по отражению и предотвращению террористических нападений на Россию и ее граждан,

по их защите от террористических актов, по недопущению на своей территории деятельности, имеющей целью организацию подобных актов против граждан и интересов других стран, по непредоставлению убежища и трибуны террористам и подстрекателям к террору, по предотвращению и пресечению финансирования терроризма;

с) добивается политико-дипломатического урегулирования региональных конфликтов на основе коллективных действий международного сообщества, исходя из того, что современные конфликты не имеют силовых решений и их урегулирование следует искать через вовлечение всех сторон в диалог и переговоры, а не через изоляцию какой-либо из них;

т) целенаправленно противодействует незаконному обороту наркотиков и организованной преступности, сотрудничая с другими государствами в многостороннем формате, прежде всего в рамках специализированных международных органов, и на двусторонней основе, в том числе в целях сохранения и укрепления международной системы контроля над наркотиками;

у) поддерживает создание под эгидой ООН и других международных и региональных организаций эффективных структур взаимодействия по реагированию на стихийные бедствия и крупные техногенные катастрофы, другие чрезвычайные ситуации, включая наращивание возможностей по преодолению их последствий и укрепление систем раннего предупреждения и прогнозирования; обладая уникальным опытом, техническими и кадровыми ресурсами, является важной и эффективной частью глобальной и трансъевропейской систем борьбы с чрезвычайными ситуациями;

ф) участвует в международном сотрудничестве по регулированию процессов миграции, обеспечению прав трудящихся-мигрантов;

х) как многонациональное и многоконфессиональное государство, имеющее многовековой опыт гармоничного сосуществования представителей различных народов, этнических групп и вероисповеданий, способствует диалогу и партнерству между культурами, религиями и цивилизациями, в том числе в рамках ООН, других международных и региональных организаций; поддерживает соответствующие инициативы гражданского общества, активно взаимодействует с Русской православной церковью и другими основными религиозными объединениями страны, противодействует экстремизму, радикализации общественных настроений, нетерпимости, дискриминации и разделению по этническому, конфессиональному, лингвистическому, культурному и другим признакам.

Международное экономическое и экологическое сотрудничество

33. Своими высокими темпами экономического роста, основанного на стабильном экспортном и расширяющемся внутреннем спросе, уникальными природными и накопленными финансовыми ресурсами, ответственной социально-экономической политикой Россия вносит значительный вклад в обеспечение стабильности глобальной экономики и финансов, участвует в международных усилиях по предотвращению и преодолению кризисных явлений. Россия намерена активно содействовать формированию справедливой и демократической глобальной торгово-экономической и валютно-финансовой архитектуры, определению ориентиров международного развития, исходя из того, что общность модернизационных вызовов открывает дополнительные перспективы углубления международного экономического сотрудничества.

34. Основные задачи России в сфере международных экономических отношений с учетом приоритетов инновационного развития страны заключаются в обеспечении ее равноправных позиций в современной системе мирохозяйственных связей, сведении к минимуму рисков, возникающих при интеграции в мировую экономику, в том числе в контексте вступления во Всемирную торговую организацию (ВТО) и присоединения к Организации экономического сотрудничества и развития (ОЭСР). Для решения этих задач Российская Федерация:

а) принимает меры торговой политики для защиты собственных интересов в соответствии с международными правилами и противодействует торгово-политическим мерам иностранных государств, ущемляющим права Российской Федерации и российских предприятий;

б) добивается адекватного учета российских интересов и подходов при выработке в рамках крупнейших международных форумов коллективной позиции по наиболее актуальным аспектам международного развития и функционирования мировой экономики, включая определение глобальной повестки дня в области укрепления энергетической и продовольственной безопасности, совершенствования режима торгового и транспортного сотрудничества;

в) создает благоприятные политические условия для диверсификации российского присутствия на мировых рынках за счет расширения номенклатуры экспорта и географии внешнеэкономических и инвестиционных связей России;

г) оказывает государственное содействие российским предприятиям и компаниям в освоении новых и развитии традиционных рынков,

противодействует дискриминации отечественных инвесторов и экспортеров;

д) содействует модернизации и диверсификации российской экономики, а также повышению доли наукоемких, инновационных и других приоритетных отраслей в общеэкономической структуре за счет привлечения передовых зарубежных научно-технических знаний и технологий, методов хозяйствования и ведения деловых операций, а также иностранных инвестиций;

е) укрепляет стратегическое партнерство с ведущими производителями энергетических ресурсов, активно развивает диалог со странами-потребителями и странами транзита, исходя из того, что меры, гарантирующие надежность поставок энергоресурсов, должны последовательно подкрепляться встречными мероприятиями по обеспечению стабильности спроса и надежности транзита;

ж) принимает меры для закрепления за Российской Федерацией статуса ключевого транзитного направления по обеспечению торгово-экономических связей между Европой и Азиатско-Тихоокеанским регионом, в том числе посредством расширения участия в формируемых трансконтинентальных маршрутах грузоперевозок;

з) активно использует возможности региональных экономических и финансовых организаций для отстаивания интересов Российской Федерации в соответствующих регионах, уделяя особое внимание деятельности организаций и структур, способствующих укреплению интеграционных процессов на пространстве Содружества Независимых Государств.

35. Российская Федерация выступает за расширение международного сотрудничества в целях обеспечения экологической безопасности и противодействия изменению климата на планете, в том числе с привлечением новейших энерго- и ресурсосберегающих технологий, в интересах всего мирового сообщества. Среди приоритетов в данной сфере – дальнейшая разработка научно обоснованных подходов к сохранению благоприятной природной среды и наращивание взаимодействия со всеми государствами по вопросам охраны окружающей природной среды для обеспечения устойчивого развития нынешнего и будущих поколений.

36. Россия рассматривает устойчивое социально-экономическое развитие всех стран как необходимый элемент современной системы коллективной безопасности и исходит из того, что содействие международному развитию должно быть нацелено на поиск эффективных путей поддержки усилий по ликвидации дисбалансов в развитии

различных регионов. В этих целях Россия, используя свой донорский потенциал, проводит активную и целенаправленную политику в сфере содействия международному развитию как на многостороннем, так и на двустороннем уровне.

37. Россия поддерживает международное сотрудничество в области охраны здоровья при ведущей роли Всемирной организации здравоохранения в качестве одного из приоритетов глобальной повестки дня, неотъемлемого компонента обеспечения устойчивого развития.

38. В условиях возрастающего как с экономической точки зрения, так и в плане укрепления безопасности значения морских пространств актуальной задачей становится их эффективное использование. Российская Федерация будет добиваться обеспечения отвечающих национальным интересам режимов безопасного судоходства, включая борьбу с морским пиратством, ответственного рыболовства и научно-исследовательской деятельности в Мировом океане в сочетании с мерами по защите морской среды, борьбе с международным терроризмом. Россия намерена установить в соответствии с международным правом внешние границы своего континентального шельфа, расширяя тем самым возможности для разведки и разработки его минеральных ресурсов.

Международное гуманитарное сотрудничество и права человека

39. Россия, приверженная универсальным демократическим ценностям, включая обеспечение прав и свобод человека, видит свои задачи в том, чтобы:

а) добиваться уважения прав и свобод человека во всем мире путем конструктивного равноправного международного диалога с учетом национальных, культурных и исторических особенностей каждого государства, осуществлять мониторинг ситуации с соблюдением прав человека в мире, способствовать привлечению к решению задач в данной сфере российских институтов гражданского общества, таких как Общественная палата Российской Федерации, неправительственные организации внешнеполитической направленности, содействуя их широкому участию в деятельности мировых экспертно-политологических форумов, в международном гуманитарном сотрудничестве;

б) способствовать гуманизации социальных систем во всем мире в целях обеспечения прав и основных свобод человека в политической, экономической, социальной и культурной областях;

в) обеспечивать дальнейшее комплексное развитие в соответствии с современными требованиями системы дипломатической и консульской защиты российских граждан, пребывающих за рубежом, в пределах, допускаемых международным правом и международными договорами Российской Федерации, в целях повышения ее эффективности, включая меры по расширению сети заграничных консульских учреждений;

г) защищать права и законные интересы соотечественников, проживающих за рубежом, на основе международного права и международных договоров Российской Федерации, рассматривая многомиллионную русскую диаспору в качестве партнера, в том числе в деле расширения и укрепления пространства русского языка и культуры;

д) способствовать консолидации организаций соотечественников в целях более эффективного обеспечения ими своих прав в странах проживания, сохранению этнокультурной самобытности русской диаспоры и ее связей с исторической Родиной, последовательно создавать условия для содействия добровольному переселению в Российскую Федерацию тех соотечественников, кто сделает такой выбор;

е) способствовать изучению и распространению русского языка как неотъемлемой части мировой культуры и инструмента международного и межнационального общения;

ж) развивать межгосударственные культурные и гуманитарные связи славянских народов;

з) твердо противодействовать проявлениям экстремизма, неонацизма, любых форм расовой дискриминации, агрессивного национализма, антисемитизма и ксенофобии, попыткам переписать историю и использовать ее в целях нагнетания конфронтации и реваншизма в мировой политике, подвергнуть ревизии итоги Второй мировой войны, способствовать деполитизации исторических дискуссий, переводу их исключительно в академическое русло;

и) привлекать институты гражданского общества к решению международных проблем в целях повышения эффективности российской внешней политики;

к) развивать, в том числе используя потенциал институтов гражданского общества в сфере общественной дипломатии, международное культурное и гуманитарное сотрудничество как средство налаживания межцивилизационного диалога, достижения согласия и обеспечения взаимопонимания между народами, уделяя особое внимание межрелигиозному диалогу;

л) наращивать взаимодействие с международными и неправительственными правозащитными организациями в целях укрепления уни-

версальных, без двойных стандартов норм защиты прав человека, их сопряжения с ответственностью личности за свои действия, прежде всего в плане недопущения оскорбления чувств верующих и укоренения толерантности, укрепления в диалоге по правам человека нравственных начал;

м) расширять участие Российской Федерации в международных договорах в области прав человека;

н) расширять правовые рамки международного сотрудничества с целью повышения уровня защиты прав и законных интересов российских детей, проживающих за рубежом;

о) работать над созданием положительного образа России, соответствующего авторитету ее культуры, образования, науки, спорта, уровню развития гражданского общества, а также участия в программах помощи развивающимся странам, формировать инструменты воздействия на ее восприятие в мире, совершенствовать систему применения «мягкой силы», искать оптимальные формы деятельности на этом направлении, учитывающие как международный опыт, так и национальную специфику и опирающиеся на механизмы взаимодействия с гражданским обществом и экспертами, продолжить формирование нормативной базы в указанной сфере.

Информационное сопровождение внешнеполитической деятельности

40. Важным направлением внешнеполитической деятельности Российской Федерации является доведение до широких кругов мировой общественности полной и точной информации о ее позициях по основным международным проблемам, о внешнеполитических инициативах и действиях Российской Федерации, о процессах и планах ее внутреннего социально-экономического развития, о достижениях российской культуры и науки.

41. В рамках публичной дипломатии Россия будет добиваться объективного восприятия ее в мире, развивать собственные эффективные средства информационного влияния на общественное мнение за рубежом, обеспечивать усиление позиций российских средств массовой информации в мировом информационном пространстве, предоставляя им необходимую государственную поддержку, активно участвовать в международном сотрудничестве в информационной сфере, принимать необходимые меры по отражению информационных угроз ее суверенитету и безопасности. В этой деятельности будут широко

использоваться возможности новых информационно-коммуникационных технологий. Россия будет добиваться формирования комплекса правовых и этических норм безопасного использования таких технологий.

IV. Региональные приоритеты

42. Приоритетными направлениями российской внешней политики являются развитие двустороннего и многостороннего сотрудничества с государствами – участниками СНГ, дальнейшее укрепление СНГ – основы углубления регионального взаимодействия его участников, имеющих не только общее историческое наследие, но и обширный потенциал интеграции в различных сферах.

43. Россия выстраивает дружественные отношения с каждым из государств – участников СНГ на основе равноправия, взаимной выгоды, уважения и учета интересов друг друга, стремясь к интенсификации интеграционных процессов на пространстве Содружества. С государствами, которые проявляют готовность к этому, развиваются отношения стратегического партнерства и союзничества.

44. Россия считает приоритетной задачу формирования Евразийского экономического союза, призванного не только максимально задействовать взаимовыгодные хозяйственные связи на пространстве СНГ, но и стать определяющей будущее стран Содружества моделью объединения, открытого для других государств. Строящийся на универсальных интеграционных принципах новый союз призван стать эффективным связующим звеном между Европой и Азиатско-Тихоокеанским регионом.

45. Россия намерена активно способствовать развитию взаимодействия государств – участников СНГ в гуманитарной сфере на базе сохранения и приумножения общего культурно-цивилизационного наследия, которое в условиях глобализации является важным ресурсом СНГ в целом и каждого государства – участника Содружества в отдельности. Особое внимание будет уделяться поддержке соотечественников, проживающих в государствах – участниках СНГ, согласованию договоренностей о защите их образовательных, языковых, социальных, трудовых, гуманитарных и иных прав и свобод.

46. Россия будет наращивать сотрудничество с государствами – участниками СНГ в сфере обеспечения взаимной безопасности, включая совместное противодействие общим вызовам и угрозам, прежде всего международному терроризму, экстремизму, незаконному обороту

наркотиков, транснациональной преступности, незаконной миграции. Первостепенными задачами являются нейтрализация указанных угроз, исходящих с территории Афганистана, недопущение дестабилизации обстановки в Центральной Азии и Закавказье.

47. В качестве одного из важнейших элементов современной системы обеспечения безопасности на постсоветском пространстве Россия рассматривает Организацию Договора о коллективной безопасности (ОДКБ). Сохраняется актуальность дальнейшей трансформации ОДКБ в универсальную международную организацию, способную противостоять современным вызовам и угрозам в условиях усиливающегося воздействия разноплановых глобальных и региональных факторов в зоне ответственности ОДКБ и прилегающих к ней районах.

48. В этих целях Россия будет:

а) работать над дальнейшей реализацией потенциала СНГ, его укреплением в качестве влиятельной региональной организации, форума для многостороннего политического диалога и механизма многопланового сотрудничества в сферах экономики, гуманитарного взаимодействия, борьбы с традиционными и новыми вызовами и угрозами;

б) содействовать практической реализации Договора о зоне свободной торговли, призванного качественно модернизировать нормативно-правовую базу торгово-экономического сотрудничества государств – участников СНГ;

в) расширять взаимодействие с Белоруссией в рамках Союзного государства в целях углубления интеграционных процессов во всех сферах;

г) активно поддерживать процесс евразийской экономической интеграции, реализуя совместно с Белоруссией и Казахстаном задачу преобразования Евразийского экономического сообщества (ЕврАзЭС) и формирования Евразийского экономического союза, содействовать привлечению к этой работе других государств – членов ЕврАзЭС, предпринимать шаги по дальнейшему развитию и совершенствованию механизмов и нормативно-правовой базы Таможенного союза и Единого экономического пространства, способствовать укреплению Евразийской экономической комиссии как единого постоянно действующего регулирующего органа Таможенного союза и Единого экономического пространства;

д) выстраивать отношения с Украиной как приоритетным партнером в СНГ, содействовать ее подключению к углубленным интеграционным процессам;

е) способствовать развитию ОДКБ в качестве ключевого инструмента поддержания стабильности и обеспечения безопасности в зоне

ответственности Организации, делая акцент на укреплении механизмов оперативного реагирования, ее миротворческого потенциала, а также на совершенствовании внешнеполитической координации государств – членов ОДКБ.

49. Россия продолжит играть активную роль в политико-дипломатическом урегулировании конфликтов на пространстве СНГ, в частности будет участвовать в поиске путей решения приднестровской проблемы на основе уважения суверенитета, территориальной целостности и нейтрального статуса Республики Молдова при определении особого статуса Приднестровья, способствовать урегулированию нагорно-карабахского конфликта во взаимодействии с другими государствами – сопредседателями Минской группы ОБСЕ и на основе принципов, изложенных в совместных заявлениях президентов России, США и Франции, сделанных в 2009–2011 годах.

50. Уважая право партнеров по Содружеству на выстраивание отношений с другими международными субъектами, Россия выступает за всеобъемлющее выполнение государствами – участниками СНГ взятых на себя обязательств в рамках региональных интеграционных структур с российским участием, обеспечение дальнейшего развития интеграционных процессов и взаимовыгодного сотрудничества на пространстве СНГ.

51. В числе российских приоритетов остается содействие становлению Республики Абхазия и Республики Южная Осетия как современных демократических государств, укреплению их международных позиций, обеспечению надежной безопасности и социально-экономическому восстановлению.

52. Россия заинтересована в нормализации отношений с Грузией в тех сферах, в которых к этому готова грузинская сторона, при учете политических реалий, сложившихся в Закавказье.

53. Подходы России к всестороннему взаимодействию с партнерами в Черноморском и Каспийском регионах будут выстраиваться с учетом сохранения приверженности целям и принципам Устава Организации Черноморского экономического сотрудничества и укрепления механизма сотрудничества пяти Прикаспийских государств на основе коллективно принимаемых ими решений.

54. Приоритетный характер имеет развитие отношений с государствами Евро-Атлантического региона, с которыми Россию связывают, помимо географии, экономики и истории, глубокие общецивилизационные корни. С учетом растущей востребованности коллективных усилий государств перед лицом транснациональных вызовов и угроз

Россия выступает за достижение единства региона без разделительных линий, через обеспечение подлинно партнерского взаимодействия России, Европейского союза и США.

55. Российская внешняя политика на евро-атлантическом направлении ориентирована на формирование общего пространства мира, безопасности и стабильности, основанного на принципах неделимости безопасности, равноправного сотрудничества и взаимного доверия. Россия последовательно выступает за перевод в юридически обязательную форму политических деклараций о неделимости безопасности вне зависимости от членства государств в каких-либо военно-политических союзах.

56. Основной задачей в отношениях с Европейским союзом для России как неотъемлемой, органичной части европейской цивилизации является продвижение к созданию единого экономического и гуманитарного пространства от Атлантики до Тихого океана.

57. Россия заинтересована в углублении сотрудничества с Европейским союзом как основным торгово-экономическим и важным внешнеполитическим партнером, выступает за укрепление взаимодействия, подчеркивая актуальность задачи формирования четырех общих пространств: экономического; свободы, безопасности и правосудия; внешней безопасности; научных исследований и образования, включая культурные аспекты. Россия выступает за заключение с Европейским союзом нового базового соглашения о стратегическом партнерстве на принципах равноправия и взаимной выгоды, будет способствовать эффективной реализации совместной инициативы Россия – ЕС «Партнерство для модернизации», развитию взаимовыгодного энергетического сотрудничества в целях создания объединенного энергетического комплекса Европы на основе строгого соблюдения имеющихся двусторонних и многосторонних договорных обязательств. Перспективной задачей является построение единого рынка с Европейским союзом.

58. Особое место в отношениях России и Европейского союза занимает задача взаимной отмены виз для краткосрочных поездок граждан. Визовый режим остается одним из основных барьеров на пути развития человеческих и экономических контактов между Россией и Европейским союзом. Его отмена станет мощным импульсом для реальной интеграции России и Европейского союза.

59. Учитывая значимую роль Европейского союза в международных делах, Россия настроена на поддержание интенсивного и взаимовыгодного политического диалога с Европейским союзом по основным вопросам внешнеполитической повестки дня, дальнейшее развитие

практического взаимодействия во внешне- и военно-политической сферах, создание соответствующих механизмов сотрудничества в области внешней политики и безопасности, с тем чтобы придать работе характер совместного принятия решений с их последующей совместной реализацией.

60. Важным ресурсом продвижения национальных интересов России в европейских и мировых делах, содействия переводу российской экономики на инновационный путь развития является активизация взаимовыгодных двусторонних связей с Германией, Францией, Италией, Нидерландами и другими государствами Европы. Россия хотела бы, чтобы в этом же русле использовался потенциал взаимодействия с Великобританией.

61. Россия продолжит усилия по укреплению Совета Европы как самостоятельной универсальной европейской организации, обеспечивающей за счет своих уникальных конвенционных механизмов единство правового и гуманитарного пространств континента.

62. Россия рассматривает Организацию по безопасности и сотрудничеству в Европе (ОБСЕ) в качестве важного механизма строительства равной и неделимой системы общеевропейской безопасности и заинтересована в укреплении ее роли и авторитета. Предпосылкой повышения востребованности ОБСЕ является фокусирование приоритетов деятельности Организации на действительно острых проблемах современности, прежде всего связанных с противодействием транснациональным вызовам и угрозам безопасности, а также разработка ее устава и реформирование работы исполнительных структур ОБСЕ в целях обеспечения надлежащих прерогатив коллективных межправительственных органов.

63. Россия будет выстраивать отношения с НАТО с учетом степени готовности альянса к равноправному партнерству, неукоснительному соблюдению принципов и норм международного права, реальным шагам по продвижению к общему пространству мира, безопасности и стабильности в Евро-Атлантическом регионе на принципах взаимного доверия, транспарентности и предсказуемости, выполнению всеми его членами взятого на себя в рамках Совета Россия – НАТО обязательства по необеспечению своей безопасности за счет безопасности других, а также обязательств по военной сдержанности. Россия сохраняет отрицательное отношение к расширению НАТО и к приближению военной инфраструктуры НАТО к российским границам в целом, как к действиям, нарушающим принцип равной безопасности и ведущим к появлению новых разъединительных линий в Европе.

64. Россия исходит из стратегической общности целей со всеми государствами Евро-Атлантического региона, в том числе со странами – членами НАТО, по поддержанию мира и стабильности, противодействию общим угрозам безопасности – международному терроризму, распространению оружия массового уничтожения, морскому пиратству, незаконному обороту наркотиков, природным и техногенным катастрофам.

65. Россия развивает поступательное практическое взаимодействие со странами Северной Европы, включая реализацию в рамках многосторонних структур совместных проектов по сотрудничеству в Баренцевом/Евроарктическом регионе и Арктике в целом, учитывая при этом интересы коренных народов. Важную роль играет участие России во взаимодействии в рамках Совета государств Балтийского моря. Россия выступает за дальнейшее раскрытие проектного потенциала «Северного измерения» и его партнерств как платформы регионального взаимодействия на севере Европы.

66. Россия нацелена на развитие всестороннего прагматичного и равноправного сотрудничества с государствами Юго-Восточной Европы. Балканский регион имеет для России важное стратегическое значение, в том числе как крупнейший транспортный и инфраструктурный узел, через территорию которого осуществляется доставка нефти и газа в страны Европы.

67. Российская Федерация выстраивает отношения с США с учетом значительного потенциала развития взаимовыгодного торгово-инвестиционного, научно-технического и иного сотрудничества, а также особой ответственности обоих государств за глобальную стратегическую стабильность и состояние международной безопасности в целом.

68. Долгосрочный приоритет российской политики – подведение под диалог с США солидного экономического фундамента, уплотнение связей во всех сферах, качественное наращивание равноправного, недискриминационного торгово-экономического сотрудничества на постоянной основе, совместная выработка культуры управления разногласиями на основе прагматизма и соблюдения баланса интересов, что позволит придать отношениям между двумя странами большую стабильность и предсказуемость, укрепить двустороннее взаимодействие на основе принципов равноправия, невмешательства во внутренние дела и уважения взаимных интересов.

69. Россия будет вести активную работу в целях противодействия введению односторонних экстерриториальных санкций США против российских юридических и физических лиц, продвигать инициативы по дальнейшей либерализации визового режима между двумя странами.

70. Россия последовательно выступает за конструктивное сотрудничество с США в сфере контроля над вооружениями, в том числе с учетом неразрывной взаимосвязи между стратегическими наступательными и оборонительными средствами, императивности придания процессу ядерного разоружения многостороннего характера, исходит из того, что переговоры о дальнейших сокращениях стратегических наступательных вооружений возможны только с учетом всех без исключения факторов, влияющих на глобальную стратегическую стабильность. В связи с созданием глобальной системы противоракетной обороны США Россия будет последовательно добиваться предоставления правовых гарантий ее ненаправленности против российских сил ядерного сдерживания.

71. Россия ожидает, что американская сторона в своих действиях на мировой арене будет строго руководствоваться нормами международного права, прежде всего Устава ООН, включая принцип невмешательства во внутренние дела других государств.

72. Важным элементом сбалансированной политики Российской Федерации на североамериканском направлении являются поступательно развивающиеся отношения с Канадой. Россия стремится к углублению двустороннего сотрудничества по актуальным международным проблемам, наращиванию динамики торгово-инвестиционных и научно-технических связей.

73. Россия проводит инициативную и конструктивную линию, направленную на укрепление разноформатного международного сотрудничества в Арктике. Последовательно реализуя национальные интересы, Россия исходит из достаточности имеющейся международной договорно-правовой базы для успешного урегулирования всех возникающих в регионе вопросов путем переговоров, включая вопросы установления внешних границ континентального шельфа в Северном Ледовитом океане. Отдавая приоритет взаимодействию с арктическими государствами, в том числе в рамках центрального регионального форума – Арктического совета, а также прибрежной арктической «пятерки», Совета Баренцева/Евроарктического региона и других многосторонних форматов, Россия открыта к взаимовыгодному сотрудничеству с внерегиональными игроками при уважении ими независимости, суверенных прав и юрисдикции арктических государств в Арктике. Существенное значение для развития региона имеет использование Северного морского пути как национальной транспортной коммуникации России в Арктике, открытой для международного судоходства на взаимовыгодной основе.

74. Будет продолжена работа по сохранению и расширению присутствия Российской Федерации в Антарктике, в том числе на основе эффективного использования механизмов и процедур, предусмотренных системой Договора об Антарктике.

75. Возрастающее значение приобретает укрепление позиции России в Азиатско-Тихоокеанском регионе, что обусловлено принадлежностью нашей страны к этому самому динамично развивающемуся геополитическому пространству, куда последовательно смещается центр тяжести мировой экономики и политики. Россия заинтересована в активном участии в интеграционных процессах в Азиатско-Тихоокеанском регионе, использовании его возможностей при реализации программ экономического подъема Сибири и Дальнего Востока, в создании в Азиатско-Тихоокеанском регионе транспарентной и равноправной архитектуры безопасности и сотрудничества на коллективных началах.

76. Принципиальное значение для России имеет общее оздоровление военно-политической обстановки в Азии, где сохраняется значительный конфликтный потенциал, наращиваются военные арсеналы, увеличивается опасность распространения оружия массового уничтожения. Россия последовательно выступает за урегулирование вовлеченными сторонами всех имеющихся разногласий политико-дипломатическими средствами при строгом соблюдении основополагающих принципов международного права.

77. Россия считает важными формирование и продвижение в Азиатско-Тихоокеанском регионе партнерской сети региональных объединений. Особое значение в этом контексте придается укреплению роли ШОС в региональных и глобальных делах, конструктивное влияние которой на положение дел в регионе в целом заметно возросло.

78. Россия рассматривает механизм Восточноазиатских саммитов как основную площадку для стратегического диалога лидеров по ключевым аспектам безопасности и сотрудничества в Азиатско-Тихоокеанском регионе. Усилия на данном направлении будут подкрепляться активностью и в других форматах – форуме «Азиатско-Тихоокеанское экономическое сотрудничество», диалоге Россия – Ассоциация государств Юго-Восточной Азии (АСЕАН), Региональном форуме АСЕАН по безопасности, форуме «Азия – Европа», Совещании по взаимодействию и мерам доверия в Азии, Совещании министров обороны стран АСЕАН с диалоговыми партнерами, форуме «Диалог по сотрудничеству в Азии».

79. Важнейшее направление российской внешней политики – развитие дружественных отношений с Китаем и Индией.

80. Россия будет продолжать наращивать всеобъемлющее равноправное доверительное партнерство и стратегическое взаимодействие с Китаем, активно развивать сотрудничество во всех областях. Совпадение принципиальных подходов двух стран к ключевым вопросам мировой политики рассматривается Россией в качестве одной из базовых составляющих региональной и глобальной стабильности. На этой основе Россия будет развивать внешнеполитическое взаимодействие с Китаем на различных направлениях, включая поиск ответов на новые вызовы и угрозы, решение острых региональных и глобальных проблем, сотрудничество в Совете Безопасности ООН, «Группе двадцати», БРИКС, Восточноазиатском саммите, ШОС и других многосторонних объединениях.

81. Россия проводит принципиальную линию на углубление привилегированного стратегического партнерства с Индией, упрочение взаимодействия по актуальным международным проблемам и укрепление взаимовыгодных двусторонних связей во всех областях, прежде всего в торгово-экономической сфере, ориентируясь на реализацию утвержденных сторонами долгосрочных программ сотрудничества.

82. Россия считает важным дальнейшее развитие механизма эффективного и взаимовыгодного внешнеполитического и экономического сотрудничества в формате Россия – Индия – Китай.

83. Россия намерена активно участвовать в работе по формированию в Северо-Восточной Азии эффективных механизмов укрепления мира, безопасности, взаимного доверия и взаимовыгодного сотрудничества как регионального компонента новой архитектуры безопасности в Азиатско-Тихоокеанском регионе.

84. Россия нацелена на поддержание дружественных, основанных на принципах добрососедства и взаимовыгодного сотрудничества отношений с Корейской Народно-Демократической Республикой и Республикой Корея, более полное использование потенциала этих связей для ускорения регионального развития, оказания поддержки межкорейскому политическому диалогу и экономическому взаимодействию как важнейшему условию поддержания мира, стабильности и безопасности в регионе. Россия неизменно выступает за безъядерный статус Корейского полуострова и будет всемерно содействовать последовательному продвижению этого процесса на основе соответствующих резолюций Совета Безопасности ООН, в том числе в рамках шестистороннего переговорного формата.

85. Российская Федерация намерена проводить курс на динамичное развитие добрососедских многоплановых отношений с Японией.

На фоне продвижения всего комплекса двустороннего сотрудничества и взаимодействия на международной арене Россия будет продолжать и диалог о путях взаимоприемлемого решения неурегулированных вопросов.

86. Россия намерена укреплять традиционно дружественные связи с Монголией.

87. Россия стремится последовательно углублять стратегическое партнерство с Вьетнамом, расширять сотрудничество с другими странами АСЕАН, будет продолжать линию на интенсификацию отношений с Австралией и Новой Зеландией, поддержание регулярных контактов и налаживание связей с островными государствами южной части Тихого океана.

88. Россия будет вносить весомый вклад в стабилизацию обстановки в регионе Ближнего Востока и Северной Африки, проводить последовательную линию на содействие достижению гражданского мира и согласия во всех государствах Ближнего Востока и Северной Африки и в регионе в целом на основе уважения суверенитета и территориальной целостности государств и невмешательства в их внутренние дела. Используя свой статус постоянного члена Совета Безопасности ООН и участника «квартета» международных посредников, Россия продолжит мобилизацию коллективных усилий для достижения на международно признанной основе всеобъемлющего и долгосрочного урегулирования арабо-израильского конфликта во всех его аспектах, включая создание независимого палестинского государства, сосуществующего в мире и безопасности с Израилем. Такое урегулирование должно быть достигнуто путем переговоров при содействии международного сообщества, использовании потенциала Лиги арабских государств и других заинтересованных сторон. Россия будет содействовать созданию на Ближнем Востоке зоны, свободной от оружия массового уничтожения и средств его доставки.

89. Россия будет последовательно проводить сбалансированную линию на всеобъемлющее политико-дипломатическое урегулирование ситуации вокруг иранской ядерной программы путем налаживания диалога на основе поэтапности, взаимности и неукоснительного соблюдения требований режима нераспространения ядерного оружия.

90. В целях дальнейшего расширения взаимодействия с государствами исламского мира Россия будет использовать возможности участия в качестве наблюдателя в Организации исламского сотрудничества и контакты с Лигой арабских государств, Советом сотрудничества

арабских государств Персидского залива. Россия настроена и далее развивать двусторонние отношения с государствами Ближнего и Среднего Востока и Северной Африки.

91. Продолжающийся кризис в Афганистане и предстоящий вывод из этой страны международных военных контингентов несут серьезную угрозу безопасности России и других государств – участников СНГ. Российская Федерация во взаимодействии с Афганистаном, другими заинтересованными государствами, ООН, СНГ, ОДКБ, ШОС и иными многосторонними институтами, в том числе в рамках проектов по линии Россия – НАТО, будет прилагать последовательные усилия в целях достижения прочного и справедливого политического урегулирования проблем этой страны при уважении прав и интересов всех населяющих ее этнических групп, постконфликтного восстановления Афганистана в качестве суверенного, миролюбивого, нейтрального государства с устойчивой экономикой. Неотъемлемым компонентом этих усилий являются комплексные меры по снижению уровня террористической угрозы, исходящей с территории Афганистана, а также по ликвидации или существенному, поддающемуся оценке сокращению незаконного производства и оборота наркотиков. Россия выступает за дальнейшее наращивание международных усилий под эгидой ООН, направленных на оказание Афганистану и сопредельным с ним государствам помощи в противодействии этим вызовам.

92. Россия продолжит всемерное укрепление отношений со странами Латинской Америки и Карибского бассейна с учетом растущей роли региона в мировых делах. Развитие стратегического сотрудничества с Бразилией, в том числе в рамках БРИКС, а также партнерских отношений с Аргентиной, Венесуэлой, Кубой, Мексикой, Никарагуа и другими государствами Латинской Америки и Карибского бассейна будет ориентировано на расширение политического взаимодействия, на продвижение торгово-экономического, инвестиционного, инновационного, культурно-гуманитарного сотрудничества, на совместный поиск ответов на новые вызовы и угрозы, на закрепление российских компаний в динамично развивающихся секторах промышленности, энергетики, связи и транспорта стран региона.

93. Россия будет стремиться к консолидации связей с латиноамериканскими партнерами на международных и региональных форумах, к расширению сотрудничества с многосторонними объединениями Латинской Америки и Карибского бассейна, в частности с Сообществом латиноамериканских и карибских государств и со странами – членами Южноамериканского общего рынка.

94. Россия будет расширять разноплановое взаимодействие с африканскими государствами на двусторонней и многосторонней основе с упором на совершенствование политического диалога и продвижение взаимовыгодного торгово-экономического сотрудничества, содействовать урегулированию и предотвращению региональных конфликтов и кризисных ситуаций в Африке. Важная составная часть этой линии – развитие партнерских отношений с Африканским союзом и субрегиональными организациями.

V. Формирование и реализация внешней политики Российской Федерации

95. Президент Российской Федерации в соответствии со своими конституционными полномочиями осуществляет руководство внешней политикой страны и как глава государства представляет Российскую Федерацию в международных отношениях.

96. Совет Федерации Федерального Собрания Российской Федерации и Государственная Дума Федерального Собрания Российской Федерации в рамках своих конституционных полномочий ведут работу по законодательному обеспечению внешнеполитического курса страны и выполнению ее международных обязательств, а также способствуют повышению эффективности парламентской дипломатии.

97. Правительство Российской Федерации осуществляет меры по реализации внешней политики страны.

98. Совет Безопасности Российской Федерации ведет работу по формированию основных направлений государственной внешней и военной политики, оценке вызовов и угроз национальным интересам и безопасности России в международной сфере, осуществляет подготовку предложений Президенту Российской Федерации для принятия главой государства решений по вопросам внешней политики Российской Федерации в области обеспечения национальной безопасности, координации деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации в процессе реализации принятых ими решений в области обеспечения национальной безопасности, а также дает оценку эффективности этих решений.

99. Министерство иностранных дел Российской Федерации разрабатывает общую стратегию внешней политики Российской Федерации, представляет соответствующие предложения Президенту Российской Федерации и ведет работу по реализации внешнеполитического курса Российской Федерации в соответствии с Концепцией и Указом Президен-

та Российской Федерации от 7 мая 2012 г. № 605 «О мерах по реализации внешнеполитического курса Российской Федерации», а также осуществляет координацию внешнеполитической деятельности федеральных органов исполнительной власти в соответствии с Указом Президента Российской Федерации от 8 ноября 2011 г. № 1478 «О координирующей роли Министерства иностранных дел Российской Федерации в проведении единой внешнеполитической линии Российской Федерации».

100. Федеральное агентство по делам Содружества Независимых Государств, соотечественников, проживающих за рубежом, и по международному гуманитарному сотрудничеству участвует в выработке предложений и реализации внешней политики Российской Федерации в сфере содействия международному развитию, международного гуманитарного сотрудничества, поддержки российских соотечественников, проживающих за рубежом, укрепления позиций русского языка в мире, развития сети российских центров науки и культуры за рубежом.

101. Субъекты Российской Федерации развивают свои международные связи в соответствии с Конституцией Российской Федерации, Федеральным законом от 4 января 1999 г. № 4-ФЗ «О координации международных и внешнеэкономических связей субъектов Российской Федерации» и другими законодательными актами. Министерство иностранных дел Российской Федерации и другие федеральные органы исполнительной власти оказывают содействие субъектам Российской Федерации в осуществлении ими международного и внешнеэкономического сотрудничества при строгом соблюдении суверенитета и территориальной целостности России, используя в этих целях возможности действующего при Министерстве иностранных дел Российской Федерации Совета глав субъектов Российской Федерации. Развитие регионального и приграничного сотрудничества является важным резервом двусторонних связей с соответствующими странами и регионами в торгово-экономической, гуманитарной и иных областях.

102. При подготовке внешнеполитических решений федеральные органы исполнительной власти на постоянной основе взаимодействуют с палатами Федерального Собрания Российской Федерации, политическими партиями, неправительственными организациями, экспертно-академическим сообществом, культурно-гуманитарными объединениями, деловыми кругами и средствами массовой информации России, содействуя их участию в международном сотрудничестве. Широкое вовлечение представителей гражданского общества во внешнеполитический процесс соответствует общемировой практике и тенденциям внутреннего развития России, отвечает задаче укрепле-

ния консенсусного характера и повышения результативности внешней политики страны, способствует ее эффективной реализации.

103. При финансировании внешнеполитических мероприятий могут привлекаться внебюджетные средства в рамках государственно-частного партнерства на добровольной основе.

104. Последовательное осуществление государственной внешней политики России призвано создавать благоприятные условия для реализации исторического выбора народов Российской Федерации в пользу правового государства, демократического общества, социально ориентированной рыночной экономики.

ОСНОВЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПЕРИОД ДО 2020 ГОДА[1]

I. Общие положения

1. Настоящие Основы являются документом стратегического планирования Российской Федерации.

2. Настоящими Основами определяются основные угрозы в области международной информационной безопасности, цель, задачи и приоритетные направления государственной политики Российской Федерации в области международной информационной безопасности (далее – государственная политика Российской Федерации), а также механизмы их реализации.

3. Нормативную правовую базу настоящих Основ составляют Конституция Российской Федерации, международные договоры Российской Федерации в области международной информационной безопасности, федеральные законы, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, иные нормативные правовые акты Российской Федерации.

4. Настоящие Основы конкретизируют отдельные положения Стратегии национальной безопасности Российской Федерации до 2020 года, Доктрины информационной безопасности Российской Федерации, Концепции внешней политики Российской Федерации и других документов стратегического планирования Российской Федерации.

[1] Опубликовано на официальном сайте Совета Безопасности Российской Федерации (2013 г.): URL: http://www.scrf.gov.ru/documents/6/114.html

5. Настоящие Основы предназначены:

а) для продвижения на международной арене российских инициатив в области формирования системы международной информационной безопасности, включая совершенствование правового, организационного и иных видов ее обеспечения;

б) для формирования межгосударственных целевых программ в области международной информационной безопасности, в осуществлении которых участвует Российская Федерация, а также государственных и федеральных целевых программ в данной области;

в) для организации межведомственного взаимодействия при реализации государственной политики Российской Федерации в области международной информационной безопасности;

г) для достижения и поддержания технологического паритета с ведущими мировыми державами за счет более широкого использования информационных и коммуникационных технологий в реальном секторе экономики.

6. Под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

7. Под системой международной информационной безопасности понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства.

Система международной информационной безопасности призвана оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве.

Сотрудничество в области формирования системы международной информационной безопасности отвечает национальным интересам Российской Федерации и способствует укреплению ее национальной безопасности.

8. Основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискреди-

тацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

II. Цель и задачи государственной политики Российской Федерации

9. Цель государственной политики Российской Федерации заключается в содействии установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности.

10. Достижению цели государственной политики Российской Федерации будет способствовать участие Российской Федерации в решении следующих задач:

а) формирование системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях;

б) создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

в) формирование механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях;

г) создание условий для противодействия угрозам использования информационных и коммуникационных технологий в экстремист-

ских целях, в том числе в целях вмешательства во внутренние дела суверенных государств;

д) повышение эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий;

е) создание условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами.

III. Основные направления государственной политики Российской Федерации

11. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях, являются:

а) создание условий для продвижения на международной арене российской инициативы в необходимости разработки и принятия государствами – членами Организации Объединенных Наций Конвенции об обеспечении международной информационной безопасности;

б) содействие закреплению российских инициатив в области формирования системы международной информационной безопасности в итоговых документах, изданных по результатам работы Группы правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также содействие выработке под эгидой Организации Объединенных Наций правил поведения в области обеспечения международной информационной безопасности, отвечающих национальным интересам Российской Федерации;

в) проведение на регулярной основе двусторонних и многосторонних экспертных консультаций, согласование позиций и планов действий с государствами – членами Шанхайской организации сотрудничества, государствами – участниками Содружества Независимых Государств, государствами – членами Организации Договора о коллективной безопасности, государствами – участниками БРИКС, странами – членами Азиатско-тихоокеанского экономического сотрудничества, странами – членами «Группы восьми», «Группы двадцати», другими государствами и международными структурами в области международной информационной безопасности;

г) продвижение на международной арене российской инициативы в интернационализации управления информационно-телекоммуникационной сетью «Интернет» и увеличение в этом контексте роли Международного союза электросвязи;

д) организационно-штатное укрепление структурных подразделений федеральных органов исполнительной власти, участвующих в реализации государственной политики Российской Федерации, а также совершенствование координации деятельности федеральных органов исполнительной власти в данной области;

е) создание механизма участия российского экспертного сообщества в совершенствовании аналитического и научно-методического обеспечения продвижения российских инициатив в области формирования системы международной информационной безопасности;

ж) создание условий для заключения между Российской Федерацией и иностранными государствами международных договоров о сотрудничестве в области обеспечения международной информационной безопасности;

з) усиление взаимодействия в рамках Соглашения между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности и содействие расширению состава участников указанного Соглашения;

и) использование научного, исследовательского и экспертного потенциала Организации Объединенных Наций, других международных организаций для продвижения российских инициатив в области формирования системы международной информационной безопасности.

12. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий, способствующих снижению риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности, являются:

а) развитие диалога с заинтересованными государствами о национальных подходах к противодействию вызовам и угрозам, возникающим в связи с масштабным использованием информационных и коммуникационных технологий в военно-политических целях;

б) участие в выработке на двустороннем и многостороннем уровнях мер по укреплению доверия в области противодействия угрозам

использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии;

в) содействие развитию региональных систем и формированию глобальной системы международной информационной безопасности на основе общепризнанных принципов и норм международного права (уважение государственного суверенитета, невмешательство во внутренние дела других государств, неприменение силы и угрозы силой в международных отношениях, право на индивидуальную и коллективную самооборону, уважение прав и основных свобод человека);

г) содействие подготовке и принятию государствами – членами Организации Объединенных Наций международных правовых актов, регламентирующих применение принципов и норм международного гуманитарного права в сфере использования информационных и коммуникационных технологий;

д) создание условий для установления международного правового режима нераспространения информационного оружия.

13. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях, являются:

а) развитие сотрудничества с государствами – членами Шанхайской организации сотрудничества, государствами – участниками Содружества Независимых Государств, государствами – членами Организации Договора о коллективной безопасности, государствами – участниками БРИКС, способствующего предупреждению, выявлению, пресечению, раскрытию и расследованию актов деструктивного воздействия на элементы национальной критической информационной инфраструктуры, минимизации последствий реализации таких актов, а также противодействию использования информационно-телекоммуникационной сети «Интернет» и других информационно-телекоммуникационных сетей в целях пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

б) содействие подготовке и принятию государствами – членами Организации Объединенных Наций акта, определяющего порядок обмена информацией о передовых практиках в области обеспечения безопасности функционирования элементов критической информационной инфраструктуры.

14. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию усло-

вий для противодействия угрозам использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств, являются:

а) участие в разработке и реализации межгосударственной системы мер по противодействию указанным угрозам;

б) содействие созданию международного механизма постоянного контроля за недопущением использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств.

15. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по повышению эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий, являются:

а) продвижение на международной арене российской инициативы в необходимости разработки и принятия под эгидой Организации Объединенных Наций Конвенции о сотрудничестве в сфере противодействия информационной преступности, а также активизация работы с государствами – членами Шанхайской организации сотрудничества, государствами – участниками Содружества Независимых Государств, государствами – членами Организации Договора о коллективной безопасности, государствами – участниками БРИКС по поддержке данной инициативы;

б) развитие сотрудничества в сфере противодействия информационной преступности с государствами – членами Шанхайской организации сотрудничества, государствами – участниками Содружества Независимых Государств, государствами – членами Организации Договора о коллективной безопасности, государствами – участниками БРИКС, странами – членами Азиатско-тихоокеанского экономического сотрудничества, странами – членами «Группы восьми», «Группы двадцати», другими государствами и международными структурами;

в) повышение эффективности информационного обмена между правоохранительными органами государств в ходе расследования преступлений в сфере использования информационных и коммуникационных технологий;

г) совершенствование механизма обмена информацией о методиках расследования и судебной практике рассмотрения дел о преступлениях в сфере использования информационных и коммуникационных технологий.

16. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами, являются:

а) содействие разработке и реализации международных программ, способствующих преодолению информационного неравенства между развитыми и развивающимися странами;

б) содействие развитию национальных информационных инфраструктур и участию государств мирового сообщества в процессах создания и использования глобальных информационных сетей и систем.

IV. Механизмы реализации государственной политики Российской Федерации

17. Государственная политика Российской Федерации реализуется федеральными органами исполнительной власти и надзорными органами в соответствии с предметами их ведения при выполнении соответствующих межгосударственных целевых программ, в осуществлении которых участвует Российская Федерация, государственных и федеральных целевых программ, в том числе в рамках государственно-частного партнерства.

18. Подготовка предложений Президенту Российской Федерации по реализации основных направлений государственной политики Российской Федерации осуществляется рабочими органами Совета Безопасности Российской Федерации во взаимодействии с заинтересованными самостоятельными подразделениями Администрации Президента Российской Федерации, федеральными органами исполнительной власти и организациями.

19. Общая координация деятельности федеральных органов исполнительной власти, связанной с реализацией государственной политики Российской Федерации, а также с продвижением согласованной позиции Российской Федерации по этому вопросу на международной арене, осуществляется Министерством иностранных дел Российской Федерации.

* * *

20. Интенсивное развитие информационных и коммуникационных технологий, их широкое применение во всех сферах деятельности человека создали условия для формирования глобальной информационной инфраструктуры, которая предоставила качественно новые

возможности социализации людей, их общения и доступа к накопленным человечеством знаниям.

В современном обществе информационные и коммуникационные технологии являются основным фактором, определяющим уровень социально-экономического развития и состояние национальной безопасности.

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года призваны способствовать активизации внешней политики Российской Федерации на пути достижения согласия и учета взаимных интересов в процессе интернационализации глобального информационного пространства.

КОНВЕНЦИЯ ОБ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (КОНЦЕПЦИЯ)[1]

(2011 г.)

Преамбула

Государства – участники настоящей Конвенции,

отмечая значительный прогресс в развитии информационно-коммуникационных технологий и средств, формирующих информационное пространство,

выражая озабоченность угрозами, связанными с возможностями использования таких технологий и средств в целях, не совместимых с задачами обеспечения международной безопасности и стабильности, как в гражданской, так и в военной сферах,

придавая важное значение международной информационной безопасности как одному из ключевых элементов системы международной безопасности,

будучи убежденными в том, что дальнейшее углубление доверия и развитие взаимодействия государств-участников в вопросах обеспечения международной информационной безопасности являются настоятельной необходимостью и отвечают их интересам,

принимая во внимание важное значение информационной безопасности для реализации основных прав и свобод человека и гражданина,

[1] Документ опубликован на официальном сайте Совета Безопасности Российской Федерации: URL: http://www.scrf.gov.ru/documents/6/112.html

учитывая резолюцию Генеральной Ассамблеи Организации Объединенных Наций A/RES/65/41 от 8 декабря 2010 г. «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности»,

стремясь ограничить угрозы международной информационной безопасности, обеспечить информационную безопасность государств-участников и создать информационное пространство, для которого характерны мир, сотрудничество и гармония,

желая создать правовые и организационные основы сотрудничества государств-участников в области обеспечения международной информационной безопасности,

ссылаясь на резолюцию Генеральной Ассамблеи Организации Объединенных Наций A/RES/55/29 от 20 ноября 2000 г. «Роль науки и техники в контексте международной безопасности и разоружения», в которой, в частности, признается, что достижения науки и техники могут иметь как гражданское, так и военное применение, и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях,

признавая необходимость предотвращения возможности использования информационно-коммуникационных технологий в целях, которые не совместимы с задачами обеспечения международной стабильности и безопасности и способны оказать отрицательное воздействие на целостность государственных инфраструктур, нанося ущерб их безопасности,

подчеркивая необходимость усиления координации и укрепления сотрудничества между государствами в борьбе с преступным использованием информационных технологий и в этом контексте отмечая ту роль, которую могут сыграть Организация Объединенных Наций и другие международные и региональные организации,

подчеркивая важность безопасного, непрерывного и стабильного функционирования Интернета и необходимость защиты Интернета и других информационно-коммуникационных сетей от возможного неблагоприятного воздействия и подверженности угрозам,

подтверждая необходимость общего понимания вопросов безопасности Интернета и дальнейшего сотрудничества на национальном и международном уровнях,

вновь подтверждая, что политические полномочия по связанным с Интернетом вопросам государственной политики являются суверенным правом государств, и что государства имеют права и обязанности в отношении связанных с Интернетом вопросов государственной политики международного уровня,

признавая, что доверие и безопасность в использовании информационно-коммуникационных технологий относятся к фундаментальным основам информационного общества и что необходимо поощрять, формировать, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности, как отмечается в резолюции Генеральной Ассамблеи Организация Объединенных Наций A/RES/64/211 от 21 декабря 2009 г. «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур»,

отмечая необходимость активизации усилий по преодолению «цифрового разрыва» путем облегчения передачи информационно-коммуникационных технологий развивающимся странам и наращивая их потенциал в вопросах передовой практики и профессиональной подготовки в области кибербезопасности, как отмечается в резолюции Генеральной Ассамблеи Организация Объединенных Наций A/RES/64/211 от 21 декабря 2009 г. «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур»,

будучи убеждены в необходимости проведения в приоритетном порядке общей политики, нацеленной на защиту общества от правонарушений в информационном пространстве, в том числе путем принятия соответствующих законодательных актов и укрепления международного сотрудничества,

сознавая глубокие перемены, вызванные внедрением цифровых технологий, объединением и продолжающейся глобализацией компьютерных сетей,

будучи озабоченными угрозой того, что компьютерные сети могут также использоваться для совершения уголовных преступлений, и что доказательства совершения таких правонарушений могут храниться в этих сетях и передаваться по ним,

признавая необходимость сотрудничества между государствами и частным бизнесом в борьбе против правонарушений в информационном пространстве и необходимость защиты законных интересов в сфере использования и развития информационно-коммуникационных технологий,

полагая, что для эффективной борьбы против правонарушений в информационном пространстве требуется более широкое, оперативное и хорошо отлаженное международное сотрудничество в области противодействия правонарушениям,

будучи убежденными в том, что настоящая Конвенция необходима для противодействия нарушениям конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерной

информации, а также злоупотреблениям такими системами, сетями и информацией путем обеспечения наказуемости таких деяний, описываемых в настоящей Конвенции, и предоставления полномочий, достаточных для эффективной борьбы с такими правонарушениями, путем содействия выявлению и расследованию таких правонарушений и преследованию за их совершение как на внутригосударственном, так и на международном уровнях и путем разработки договоренностей относительно оперативного и надежного международного сотрудничества,

памятуя о необходимости обеспечения должного баланса между интересами поддержания правопорядка и уважением основополагающих прав человека, как это предусмотрено Международным пактом о гражданских и политических правах 1966 года, а также другими международными договорами о правах человека, в которых подтверждается право каждого беспрепятственно придерживаться своих мнений и право на свободное выражение своего мнения, включая свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ,

памятуя также о праве на уважение частной жизни и защиту персональных данных,

учитывая положения Конвенции о правах ребенка 1989 года и Конвенции о запрещении и немедленных мерах по искоренению наихудших форм детского труда, принятой Генеральной конференцией Международной организации труда в 1999 году,

приветствуя события последнего времени, способствующие дальнейшему росту международного взаимопонимания и сотрудничества в борьбе с правонарушениями в информационном пространстве, включая меры, принятые Организацией Объединенных Наций, Шанхайской организацией сотрудничества, Европейским Союзом, Организацией Азиатско-Тихоокеанского сотрудничества, Организацией американских государств, Ассоциацией стран Юго-Восточной Азии, Организацией экономического сотрудничества и развития, «Группой восьми» и другими международными организациями и форумами,

согласились о нижеследующем:

Глава 1. Общие положения

Статья 1. Предмет и цель Конвенции

Предметом регулирования настоящей Конвенции является деятельность государств по обеспечению международной информационной безопасности.

Целью настоящей Конвенции является противодействие использованию информационно-коммуникационных технологий для нарушения международного мира и безопасности, а также установление мер, способствующих тому, чтобы деятельность государств в информационном пространстве:

1) способствовала общему социальному и экономическому развитию;

2) осуществлялась таким образом, чтобы быть совместимой с задачами поддержания международного мира и безопасности;

3) соответствовала общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека;

4) была совместимой с правом каждого искать, получать и распространять информацию и идеи, как это зафиксировано в документах ООН, с учетом того, что такое право может быть ограничено законодательством для защиты интересов национальной и общественной безопасности каждого государства, а также для предотвращения неправомерного использования и несанкционированного вмешательства в информационные ресурсы;

5) гарантировала свободу технологического обмена и свободу обмена информацией с учетом уважения суверенитета государств и их существующих политических, исторических и культурных особенностей.

Статья 2. Термины и определения

Для целей настоящей Конвенции используются следующие термины и определения:

«доступ к информации» – возможность получения информации и ее использования;

«информационная безопасность» – состояние защищенности интересов личности, общества и государства от угроз деструктивных и иных негативных воздействий в информационном пространстве;

«информационная война» – противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны;

«информационная инфраструктура» – совокупность технических средств и систем формирования, преобразования, передачи, использования и хранения информации;

«информационная система» – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

«информационное оружие» – информационные технологии, средства и методы, предназначенные для ведения информационной войны;

«информационное пространство» – сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;

«информационно-коммуникационные технологии» – совокупность методов, производственных процессов и программно-технических средств, интегрированных с целью формирования, преобразования, передачи, использования и хранения информации;

«информационные ресурсы» – информационная инфраструктура, а также собственно информация и ее потоки;

«конфиденциальность информации» – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

«критически важный объект информационной инфраструктуры» – часть (элемент) информационной инфраструктуры, воздействие на которую может иметь последствия, непосредственно затрагивающие национальную безопасность, включая безопасность личности, общества и государства;

«международная информационная безопасность» – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве;

«неправомерное использование информационных ресурсов» – использование информационных ресурсов без соответствующих прав или с нарушением установленных правил, законодательства государств либо норм международного права;

«несанкционированное вмешательство в информационные ресурсы» – неправомерное воздействие на процессы формирования, обработки, преобразования, передачи, использования и хранения информации;

«оператор информационной системы» – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

«правонарушение в информационном пространстве» – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях;

«предоставление информации» – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

«распространение информации» – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

«терроризм в информационном пространстве» – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях;

«угроза в информационном пространстве (угроза информационной безопасности)» – факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве.

Статья 3. Исключения в применении Конвенции

Настоящая Конвенция не применяется в случаях, когда действия осуществлены в рамках информационной инфраструктуры одного государства, гражданином или юридическим лицом, находящимся под юрисдикцией этого государства, и последствия этих действий имели место только в отношении граждан и юридических лиц, находящихся под юрисдикцией этого же государства, и никакое другое государство не имеет оснований для осуществления своей юрисдикции.

Статья 4. Основные угрозы международному миру и безопасности в информационном пространстве

В качестве основных угроз в информационном пространстве, приводящих к нарушению международного мира и безопасности, рассматриваются следующие:

1) использование информационных технологий и средств для осуществления враждебных действий и актов агрессии;

2) целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры другого государства;

3) неправомерное использование информационных ресурсов другого государства без согласования с государством, в информационном пространстве которого располагаются эти ресурсы;

4) действия в информационном пространстве с целью подрыва политической, экономической и социальной систем другого госу-

дарства, психологическая обработка населения, дестабилизирующая общество;

5) использование международного информационного пространства государственными и негосударственными структурами, организациями, группами и отдельными лицами в террористических, экстремистских и иных преступных целях;

6) трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальным законодательствам государств;

7) использование информационной инфраструктуры для распространения информации, разжигающей межнациональную, межрасовую и межконфессиональную вражду, расистских и ксенофобских письменных материалов, изображений или любого другого представления идей или теорий, которые пропагандируют, способствуют или подстрекают к ненависти, дискриминации или насилию против любой личности или группы лиц, если в качестве предлога к этому используются факторы, основанные на расе, цвете кожи, национальном или этническом происхождении, а также религии;

8) манипулирование информационными потоками в информационном пространстве других государств, дезинформация и сокрытие информации с целью искажения психологической и духовной среды общества, эрозия традиционных культурных, нравственных, этических и эстетических ценностей;

9) использование информационно-коммуникационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационном пространстве;

10) противодействие доступу к новейшим информационно-коммуникационным технологиям, создание условий технологической зависимости в сфере информатизации в ущерб другим государствам;

11) информационная экспансия, приобретения контроля над национальными информационными ресурсами другого государства.

Дополнительными факторами, усиливающими опасность перечисленных угроз, являются:

1) неопределенность в идентификации источника враждебных действий, особенно с учетом возрастающей активности отдельных лиц, групп и организаций, включая преступные организации, которые выполняют посреднические функции в осуществлении деятельности от имени других;

2) потенциальная опасность включения в информационно-коммуникационные технологии недекларируемых деструктивных возможностей;

3) различия в степени оснащенности информационно-коммуникационными технологиями и их безопасности в разных государствах («цифровое неравенство»);

4) различия в национальных законодательствах и практике формирования безопасной и быстро восстанавливающейся информационной инфраструктуры.

Статья 5. Основные принципы обеспечения международной информационной безопасности

Информационное пространство является общечеловеческим достоянием. Его безопасность является основой обеспечения устойчивого развития мировой цивилизации.

В целях создания и поддержания атмосферы доверия в информационном пространстве необходимо соблюдение государствами-участниками следующих принципов:

1) деятельность каждого государства-участника в информационном пространстве должна способствовать социальному и экономическому развитию и осуществляться таким образом, чтобы быть совместимой с задачами поддержания международного мира и безопасности, соответствовать общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы в международных отношениях, невмешательства во внутренние дела других государств, уважения суверенитета государств, основных прав и свобод человека;

2) государства-участники в ходе формирования системы международной информационной безопасности будут руководствоваться принципом неделимости безопасности, означающим, что безопасность каждого из них неразрывно связана с безопасностью всех других государств и мирового сообщества в целом, а также не будут укреплять свою безопасность в ущерб безопасности других государств;

3) каждое государство-участник должно стремиться к преодолению различий в степени оснащенности национальных информационных систем современными информационно-коммуникационными технологиями, сокращению «цифрового разрыва» в целях снижения общего уровня угроз в информационном пространстве;

4) все государства-участники в информационном пространстве пользуются суверенным равенством, имеют одинаковые права и обязанности и являются равноправными субъектами информационного пространства независимо от различий экономического, социального, политического или иного характера;

5) каждое государство-участник вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством. Суверенитет и законы распространяются на информационную инфраструктуру, расположенную на территории государства-участника или иным образом находящуюся под его юрисдикцией. Государства-участники должны стремиться к гармонизации национальных законодательств, различия в них не должны создавать барьеры на пути формирования надежной и безопасной информационной среды;

6) каждое государство-участник должно придерживаться принципа ответственности за собственное информационное пространство, в том числе за его безопасность и за содержание размещаемой в нем информации;

7) каждое государство-участник имеет право свободно осуществлять без вмешательства извне развитие своего информационного пространства, и каждое другое государство обязано уважать это право в соответствии с принципом равноправия и самоопределения народов, закрепленного в Уставе Организации Объединенных Наций;

8) каждое государство-участник, учитывая законные интересы безопасности других государств, может свободно и самостоятельно определять свои интересы обеспечения информационной безопасности на основе суверенного равенства, а также свободно выбирать способы обеспечения собственной информационной безопасности в соответствии с международным правом;

9) государства-участники признают, что агрессивная «информационная война» составляет преступление против международного мира и безопасности;

10) информационное пространство государства-участника не должно быть объектом приобретения другим государством в результате угрозы силой или ее применения;

11) каждое государство-участник имеет неотъемлемое право на самооборону перед лицом агрессивных действий в информационном пространстве в отношении его при условии достоверного установления источника агрессии и адекватности ответных мер;

12) каждое государство-участник будет определять свой военный потенциал в информационном пространстве на основе национальных процедур с учетом законных интересов безопасности других государств, а также необходимости содействовать укреплению международного мира и безопасности. Ни одно из государств-участников не будет предпринимать попыток добиться господства в информационном пространстве над другими государствами;

13) государство-участник может размещать свои силы и средства обеспечения информационной безопасности на территории другого государства в соответствии с соглашением, выработанным ими на добровольной основе в ходе переговоров, а также в соответствии с международным правом;

14) каждое государство-участник принимает необходимые меры для обеспечения невмешательства в деятельность международных информационных систем управления транспортными, финансовыми потоками, средствами связи, средствами международного информационного, в том числе научного и образовательного обмена, исходя из понимания того, что подобное вмешательство может негативно повлиять на информационное пространство в целом;

15) государства-участники должны поддерживать и стимулировать научно-технические разработки в области освоения информационного пространства, а также образовательно-просветительскую деятельность, направленную на формирование глобальной культуры кибербезопасности;

16) каждое государство-участник в рамках имеющихся средств обеспечивает в своем информационном пространстве соблюдение основных прав и свобод человека и гражданина, соблюдение прав на интеллектуальную собственность, включая патенты, технологии, коммерческую тайну, торговые марки и авторские права;

17) каждое государство-участник гарантирует свободу слова, выражение мнений в информационном пространстве, защиту от незаконного вмешательства в частную жизнь граждан;

18) каждое государство-участник стремится к соблюдению баланса между основными свободами и эффективным противодействием террористическому использованию информационного пространства;

19) государства-участники не вправе ограничивать или нарушать доступ граждан к информационному пространству, кроме как в целях защиты национальной и общественной безопасности, а также предотвращения неправомерного использования и несанкционированного вмешательства в национальную информационную инфраструктуру;

20) государства-участники стимулируют партнерство бизнеса и гражданского общества в информационном пространстве;

21) государства-участники признают свои обязанности по обеспечению осведомленности своих граждан, общественных и государственных органов, других государств и мирового сообщества о новых угрозах в информационном пространстве и об известных путях повышения уровня их безопасности.

Глава 2. Основные меры предотвращения и разрешения военных конфликтов в информационном пространстве

Статья 6. Основные меры предотвращения военных конфликтов в информационном пространстве

Руководствуясь изложенными в Статье 5 принципами, государства-участники обязуются принимать меры к упреждающему выявлению потенциальных конфликтов в информационном пространстве, а также прилагать совместные усилия для их предотвращения, мирного урегулирования кризисов и споров.

С этой целью государства-участники:

1) обязуются сотрудничать друг с другом в сфере обеспечения международной информационной безопасности для поддержания международного мира и безопасности и содействия международной экономической стабильности и прогрессу, общему благосостоянию народов и международному сотрудничеству, свободному от дискриминации;

2) будут предпринимать все необходимые меры для предотвращения деструктивного информационного воздействия со своей территории или с использованием информационной инфраструктуры, находящейся под его юрисдикцией, а также обязуются взаимодействовать для определения источника компьютерных атак, проведенных с использованием их территории, противодействия этим атакам и ликвидации последствий;

3) будут воздерживаться от разработки и принятия планов, доктрин, способных спровоцировать возрастание угроз в информационном пространстве, а также вызвать напряженность в отношениях между государствами и возникновение «информационных войн»;

4) будут воздерживаться от любых действий, направленных на полное или частичное нарушение целостности информационного пространства другого государства;

5) обязуются не использовать информационно-коммуникационные технологии для вмешательства в дела, относящиеся ко внутренней компетенции другого государства;

6) будут воздерживаться в международных отношениях от угрозы силой или ее применения против информационного пространства любого другого государства для его нарушения или в качестве средства разрешения конфликтов;

7) обязуются воздерживаться от организации или поощрения организации каких-либо иррегулярных сил для осуществления неправомерных действий в информационном пространстве другого государства;

8) обязуются воздерживаться от клеветнических утверждений, а также от оскорбительной или враждебной пропаганды для осуществления интервенции или вмешательства во внутренние дела других государств;

9) имеют право и обязуются бороться против распространения недостоверных или искаженных сообщений, которые могут рассматриваться как вмешательство во внутренние дела других государств или как наносящие ущерб международному миру и безопасности;

10) будут принимать меры по ограничению распространения «информационного оружия» и технологий его создания.

Статья 7. Меры, направленные на разрешение военных конфликтов в информационном пространстве

1) Государства-участники разрешают конфликты в информационном пространстве, в первую очередь путем переговоров, обследования, посредничества, примирения, арбитража, судебного разбирательства, обращения к региональным органам или соглашениям или иными мирными средствами по своему выбору таким образом, чтобы не подвергать угрозе международный мир и безопасность.

2) В случае любого международного конфликта право государств-участников, находящихся в конфликте, выбирать методы или средства ведения «информационной войны» ограничено применимыми нормами международного гуманитарного права.

Глава 3. Основные меры противодействия использованию информационного пространства в террористических целях

Статья 8. Использование информационного пространства в террористических целях

Государства-участники осознают возможность использования информационного пространства для осуществления террористической деятельности.

Статья 9. Основные меры противодействия использованию информационного пространства в террористических целях

В целях противодействия использованию информационного пространства в террористических целях государства-участники:

1) принимают меры по противодействию использованию информационного пространства в террористических целях и признают для этого необходимость совместных решительных действий;

2) будут стремиться к выработке единых подходов к прекращению функционирования Интернет-ресурсов террористического характера;

3) осознают необходимость установления и расширения обмена информацией об угрозах совершения компьютерных атак, о признаках, фактах, методах и средствах использования сети Интернет в террористических целях, об устремлениях и деятельности террористических организаций в информационном пространстве, а также обмена опытом и лучшими практиками мониторинга информационных ресурсов сети Интернет, поиска и отслеживания содержимого сайтов террористической направленности, проведения криминалистических компьютерных экспертиз в этой сфере, правового регулирования и организации деятельности по противодействию использованию информационного пространства в террористических целях;

4) принимают такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить компетентным органам проводить следственные, розыскные и иные процессуальные мероприятия, направленные на предотвращение, пресечение и ликвидацию последствий проведения террористических действий в информационном пространстве, а также наказание виновных в них лиц и организаций;

5) принимают необходимые меры законодательного и иного характера, которые гарантируют доступ законным образом на территорию государства-участника к отдельным частям информационно-коммуникационной инфраструктуры, в отношении которых имеются законные основания полагать их использование для ведения в информационном пространстве или с их использованием террористической деятельности или деятельности, способствующей проведению террористических актов или деятельности террористических организаций, групп или отдельных террористов.

Глава 4. Основные меры противодействия правонарушениям в информационном пространстве

Статья 10. Основные меры противодействия правонарушениям в информационном пространстве

В целях противодействия правонарушениям в информационном пространстве государства-участники:

1) прилагают усилия по криминализации использования информационных ресурсов и (или) воздействия на них в информационном пространстве в противоправных целях, к которым в том числе относятся неправомерное распространение информации, нарушения конфиденциальности, целостности и доступности информации, а также прини-

мают законодательные и иные меры, необходимые для того, чтобы установить и применить ответственность к лицам за покушение, соучастие, подстрекательство к совершению и совершение криминализированных социально опасных деяний в информационном пространстве;

2) принимают законодательные и иные меры, необходимые для того, чтобы к лицам, совершившим правонарушения в информационном пространстве, применялись эффективные, соразмерные и убедительные меры наказания.

Статья 11. Меры по организации уголовного процесса

В целях организации уголовного процесса государства-участники:

1) принимают законодательные и иные меры, необходимые для установления полномочий и процедур в целях проведения конкретных уголовных расследований или судебного разбирательства по фактам совершения в информационном пространстве криминализированных социально опасных деяний;

2) обеспечивают установление, исполнение и применение полномочий и процедур в целях проведения конкретных уголовных расследований или судебного разбирательства по фактам совершения в информационном пространстве криминализированных социально опасных деяний в соответствии с условиями и гарантиями, предусмотренными его законодательством и обеспечивающими надлежащую защиту прав и свобод человека, и в соответствии с принципом соразмерности;

3) принимают законодательные и иные меры, необходимые для того, чтобы его компетентные органы имели возможность оперативно обеспечивать сохранность конкретных данных, включая данные о потоках информации, которые хранятся в информационно-коммуникационной инфраструктуре, когда имеются основания полагать, что эти данные особенно подвержены риску утраты или изменения;

4) принимают законодательные и иные меры, необходимые для того, чтобы гарантировать оперативное предоставление компетентным органам государства-участника или лицу, назначенному этими органами, достаточного количества данных о потоках информации, которые позволят идентифицировать поставщиков услуг и путь, которым передавалось конкретное сообщение в его информационном пространстве;

5) принимают законодательные и иные меры, которые могут потребоваться для предоставления его компетентным органам полномочий на обыск или иной аналогичный доступ к информационно-коммуникационным системам и их частям и хранящимся в них данным, носителям информации, на которых могут храниться искомые данные,

на его территории, а также к другим данным и информационно-коммуникационным системам своего информационного пространства, в отношении которых имеется достаточно оснований полагать, что в них находятся искомые данные;

6) принимают законодательные и иные меры, необходимые для предоставления его компетентным органам полномочий требовать от лица, находящегося на территории государства и обладающего знаниями о функционировании соответствующей информационно-коммуникационной системы, применяемых мерах защиты, хранящихся там данных, для предоставления необходимых сведений, которые позволят им в пределах установленных полномочий осуществлять процедуры в целях проведения конкретных уголовных расследований или судебного разбирательства по фактам совершения в информационном пространстве криминализированных социально опасных деяний;

7) принимают законодательные и иные меры, необходимые для предоставления его компетентным органам полномочий собирать или записывать информацию с применением технических средств на его территории, а также обязать поставщиков услуг осуществлять в реальном масштабе времени аналогичные действия в сотрудничестве с компетентными органами данного государства;

8) принимают законодательные и иные меры для установления юрисдикции в отношении любого криминализированного социального опасного деяния в информационном пространстве, совершаемого на его территории, на борту судна, плавающего под флагом этого государства, на борту самолета или иного летательного аппарата, зарегистрированного согласно законам этого государства.

Если на юрисдикцию в отношении предполагаемого правонарушения претендует более одного государства-участника, заинтересованные государства проводят консультации с целью определения наиболее подходящей юрисдикции для осуществления судебного преследования.

Глава 5. Международное сотрудничество в сфере международной информационной безопасности

Статья 12. Сотрудничество государств-участников

1) Государства-участники обязуются осуществлять сотрудничество друг с другом в соответствии с положениями настоящей Конвенции и через применение других международных договоренностей.

2) Государства-участники на основе добровольности и взаимности обмениваются лучшими практиками в работе по предотвращению, пра-

вовому разбирательству и ликвидации последствий преступных деяний, включая действия в террористических целях, с использованием информационного пространства. Обмен может производиться как на двусторонней, так и на многосторонней основе. Государство-участник, предоставляющее информацию, вправе устанавливать требования о ее конфиденциальности. Государство-участник, получившее такую информацию, вправе использовать ее как аргумент в отношениях с предоставившим государством-участником при обсуждении вопросов взаимной помощи.

Статья 13. Меры доверия в области военного использования информационного пространства

Каждое государство-участник должно стремиться к укреплению мер доверия в области военного использования информационного пространства, к которым относятся:

1) обмен национальными концепциями обеспечения безопасности в информационном пространстве;

2) оперативный обмен информацией о кризисных событиях и угрозах в информационном пространстве и принимаемых мерах в отношении их урегулирования и нейтрализации;

3) консультации по вопросам деятельности в информационном пространстве, которая может вызывать озабоченность государств-участников, и сотрудничество в отношении урегулирования конфликтных ситуаций военного характера.

Статья 14. Консультативная помощь

Государства-участники обязуются консультироваться и сотрудничать друг с другом в решении любых вопросов, которые могут возникнуть в отношении целей или в связи с выполнением положений настоящей Конвенции.

Заключительные положения

Статья 15. Подписание Конвенции

Настоящая Конвенция открыта для подписания ее всеми государствами.

Статья 16. Ратификация Конвенции

Настоящая Конвенция подлежит ратификации. Ратификационные грамоты сдаются на хранение Генеральному секретарю Организации Объединенных Наций.

Статья 17. Присоединение к Конвенции

Настоящая Конвенция открыта для присоединения к ней любого государства. Документы о присоединении сдаются на хранение Генеральному секретарю Организации Объединенных Наций.

Статья 18. Вступление в силу Конвенции

1. Настоящая Конвенция вступает в силу на тридцатый день после даты сдачи на хранение Генеральному секретарю Организации Объединенных Наций двадцатой ратификационной грамоты или документа о присоединении.

2. Для каждого государства, которое ратифицирует настоящую Конвенцию или присоединяется к ней после сдачи на хранение двадцатой ратификационной грамоты или документа о присоединении, настоящая Конвенция вступает в силу на тридцатый день после сдачи таким государством на хранение его ратификационной грамоты или документа о присоединении.

Статья 19. Внесение поправок в Конвенцию

1. Любое государство-участник может предложить поправку и представить ее Генеральному секретарю Организации Объединенных Наций. Генеральный секретарь затем препровождает предложенную поправку государствам-участникам с просьбой указать, высказываются ли они за созыв конференции государств-участников с целью рассмотрения этих предложений и проведения по ним голосования. Если в течение четырех месяцев, начиная с даты такого сообщения, по крайней мере одна треть государств-участников выскажется за такую конференцию, Генеральный секретарь созывает эту конференцию под эгидой Организации Объединенных Наций. Любая поправка, принятая большинством государств-участников, присутствующих и участвующих в голосовании на этой конференции, представляется Генеральной Ассамблее на утверждение.

2. Поправка, принятая в соответствии с пунктом 1 настоящей статьи, вступает в силу по утверждении ее Генеральной Ассамблеей Организации Объединенных Наций и принятия ее большинством в две трети государств-участников.

3. Когда поправка вступает в силу, она становится обязательной для тех государств-участников, которые ее приняли, а для других государств-участников остаются обязательными положения настоящей Конвенции и любые предшествующие поправки, которые ими приняты.

Статья 20. Оговорки к Конвенции

1. Генеральный секретарь Организации Объединенных Наций получает и рассылает всем государствам текст оговорок, сделанных государствами в момент ратификации или присоединения.

2. Оговорка, не совместимая с целями и задачами настоящей Конвенции, не допускается.

3. Оговорки могут быть сняты в любое время путем соответствующего уведомления, направленного Генеральному секретарю Организации Объединенных Наций, который затем сообщает об этом всем государствам. Такое уведомление вступает в силу со дня его получения Генеральным секретарем.

Статья 21. Денонсация Конвенции

Любое государство-участник может денонсировать настоящую Конвенцию путем письменного уведомления Генерального секретаря Организации Объединенных Наций. Денонсация вступает в силу по истечении одного года после получения уведомления Генеральным секретарем.

Статья 22. Депозитарий Конвенции

Генеральный секретарь Организации Объединенных Наций назначается депозитарием настоящей Конвенции.

Статья 23. Подлинник настоящей Конвенции, английский, арабский, испанский, китайский, русский и французский тексты которой являются равно аутентичными, сдается на хранение Генеральному секретарю Организации Объединенных Наций

В удостоверение чего нижеподписавшиеся полномочные представители, должным образом на то уполномоченные своими соответствующими правительствами, подписали настоящую Конвенцию.

КОНЦЕПТУАЛЬНЫЕ ВЗГЛЯДЫ НА ДЕЯТЕЛЬНОСТЬ ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

(2011 г.)

Источником внешней угрозы информационной безопасности Российской Федерации является разработка рядом государств концепций информационных войн, предусматривающих создание средств

опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

(Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г.)

Введение

Высокие темпы развития информационных систем различного назначения, компьютерных сетей типа Интернет и электронных СМИ привели на рубеже тысячелетий к формированию глобального информационного пространства. Наряду с сухопутным, морским, воздушным и космическим пространством, информационное пространство в армиях наиболее развитых стран стало активно использоваться для решения широкого круга военных задач.

Вследствие уязвимости информационно-коммуникационных систем к радиоэлектронным и программно-аппаратным воздействиям в мире возникло и стало быстро распространяться информационное оружие, обладающее трансграничными поражающими факторами, резко возросла роль информационной войны. Российская Федерация, стремительно продвигающаяся по пути информатизации всех сфер жизнедеятельности общества, оказалась перед лицом новой серьезной угрозы, исходящей из глобального информационного пространства.

Чрезвычайная важность противодействия актам агрессивной информационной войны впервые была отмечена в Доктрине информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 9 сентября 2000 г. В ней определено, что одним из приоритетных направлений противодействия данной угрозе является решение задач «совершенствования приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника. Кроме того, в последнее время вследствие широкого применения в системах управления войсками и оружием компьютерной техники, этот перечень дополнился задачей защиты информационной инфраструктуры Вооруженных Сил Российской Федерации от различного рода компьютерных атак.

Опыт вооруженных конфликтов последнего десятилетия, а также практика оперативной подготовки войск и штабов позволяют констатировать, что в настоящее время в Вооруженных Силах Российской Федерации сложилась цельная система деятельности, призванная обеспечить эффективное сдерживание, предотвращение и разрешение военных конфликтов в информационном пространстве.

Настоящие Концептуальные взгляды раскрывают основные принципы, правила и меры доверия, в соответствии с которыми Вооруженные Силы Российской Федерации используют глобальное информационное пространство для решения задач обороны и безопасности.

1. Основные термины и определения

Для целей настоящего документа используются следующие основные термины и определения:

Военный конфликт в информационном пространстве– форма разрешения межгосударственных или внутригосударственных противоречий с применением информационного оружия.

Деятельность вооруженных сил в информационном пространстве – использование вооруженными силами информационных ресурсов для решения задач обороны и безопасности.

Информационная безопасность вооруженных сил– состояние защищенности информационных ресурсов вооруженных сил от воздействия информационного оружия.

Информационная война– противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны. Информационная инфраструктура– совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации.

Информационное оружие– информационные технологии, средства и методы, применяемые в целях ведения информационной войны.

Информационное пространство– сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том

числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию.

Информационные ресурсы – информационная инфраструктура, а также собственно информация и ее потоки.

Кризисная ситуация – этап эскалации конфликта, характеризующийся применением военной силы для его разрешения.

Международная информационная безопасность – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.

Система обеспечения информационной безопасности Российской Федерации – часть системы обеспечения национальной безопасности страны, предназначенная для реализации государственной политики в сфере информационной безопасности.

2. Принципы

Деятельность Вооруженных Сил Российской Федерации в информационном пространстве строится исходя из совокупности принципов: законности, приоритетности, комплексности, взаимодействия, сотрудничества, инновационности.

2.1. Законность

Соблюдение принципа законности требует от Вооруженных Сил Российской Федерации в ходе своих действий в информационном пространстве неукоснительно руководствоваться нормами и принципами действующего российского законодательства, а также общепризнанными нормами и принципами международного права.

В частности, в соответствии со ст. 20 Военной доктрины Российской Федерации применение Вооруженных Сил Российской Федерации в мирное время осуществляется по решению Президента Российской Федерации в порядке, установленном федеральным законодательством. Так, решение на применение Вооруженных Сил Российской Федерации за пределами территории Российской Федерации принимается Президентом Российской Федерации на основании соответствующего постановления Совета Федерации Федерального Собрания Российской Федерации. Данное положение следует распространить также и на применение Вооруженных Сил Российской Федерации в информационном пространстве. Что касается международного права, то Воору-

женные Силы Российской Федерации применительно к особенностям военной деятельности в глобальном информационном пространстве руководствуются следующими его нормами и принципами:

уважение государственного суверенитета,

невмешательство во внутренние дела других государств,

неприменение силы и угрозы силой,

право на индивидуальную и коллективную самооборону.

Кроме того, Вооруженные Силы Российской Федерации руководствуются нормами международного гуманитарного права (ограничение неизбирательного применения информационного оружия; установление особой защиты для информационных объектов, являющихся потенциально опасными источниками техногенных катастроф; запрещение вероломных методов ведения информационной войны).

2.2. Приоритетность

Соблюдение принципа приоритетности требует от Вооруженных Сил Российской Федерации в ходе своей деятельности в информационном пространстве в первоочередном порядке стремиться к сбору актуальной и достоверной информации об угрозах, ее оперативной обработке, глубокому анализу и своевременной выработке мер защиты. Все это в совокупности создает благоприятные условия для эффективного управления войсками и оружием, поддержания необходимого морально-психологического состояния личного состава.

Принятие комплекса мер по защите информационных ресурсов, позволит в условиях информационной войны избежать дезориентации органов военного управления, дезорганизации системы управления войсками и оружием, катастрофического разрушения элементов тыловой и транспортной инфраструктуры, деморализации личного состава и населения в зоне военных действий. В современных условиях необходимость принятия данных мер в приоритетном порядке обуславливается, в том числе тем, что сейчас сотни миллионов человек (целые страны и континенты) вовлечены в единое глобальное информационное пространство, образованное Интернетом, электронными СМИ и системами мобильной связи.

2.3. Комплексность

Соблюдение принципа комплексности требует от Вооруженных Сил Российской Федерации в ходе своей деятельности в информа-

ционном пространстве использовать все имеющиеся силы и средства для эффективного решения стоящих перед ними задач.

В целом деятельность в информационном пространстве включает мероприятия штабов и действия войск по разведке, оперативной маскировке, радиоэлектронной борьбе, связи, скрытому и автоматизированному управлению, информационной работе штабов, а также защите своих информационных систем от радиоэлектронных, компьютерных и иных воздействий.

Деятельность в информационном пространстве представляет собой согласованную единую систему, в которой каждый компонент выполняет свои задачи присущими ему способами и приемами, а с другой стороны, интегрируясь в единую систему, повышает возможности всей системы по достижению целей, стоящих перед Вооруженными Силами Российской Федерации.

В организации деятельности в информационном пространстве в мирное, в военное время, при подготовке и в ходе операций (боевых действий) принимают непосредственное участие командование и штабы всех уровней.

Каждый из этих органов управления в соответствии со своими функциями и ответственностью разрабатывает и планирует мероприятия и действия подчиненных войск, объединенные единым замыслом действий в информационном пространстве.

2.4. Взаимодействие

Соблюдение принципа взаимодействия требует от Минобороны России согласовывать свои действия в информационном пространстве с другими федеральными органами исполнительной власти.

Взаимодействие осуществляется в рамках системы обеспечения информационной безопасности Российской Федерации, определенной Доктриной информационной безопасности Российской Федерации (2000 г.).

2.5. Сотрудничество

Соблюдение принципа сотрудничества требует согласования усилий с дружественными государствами и международными организациями.

Основной целью развития сотрудничества на глобальном уровне является установление международно-правового режима, регулирующего, в том числе, военную деятельность государств в мировом

информационном пространстве на основе принципов и норм международного права.

Развитие сотрудничества на региональном уровне преследует следующие цели: создание механизмов принятия эффективных коллективных действий, направленных на выявление, предупреждение и пресечение применения информационно-телекоммуникационных технологий для угрозы миру и безопасности, осуществления актов агрессии урегулирование и разрешение международных споров и конфликтных ситуаций, связанных с враждебным использованием информационно-телекоммуникационных технологий, укрепление доверия в области использования информационных систем трансграничного характера и обеспечение безопасности использования единого информационного пространства.

2.6. Инновационность

Соблюдение принципа инновационности требует от Вооруженных Сил Российской Федерации использовать для подготовки и осуществления деятельности в информационном пространстве наиболее передовые технологии, средства и методики, а также привлекать к решению задач по информационной безопасности высококвалифицированный личный состав.

Поэтому для разработки и производства таких средств и технологий может привлекаться научно-производственный потенциал наиболее передовых инновационных центров Российской Федерации, а сама разработка осуществляться в рамках государственных и ведомственных программ и НИОКР.

Подготовка специалистов в сфере организации и осуществления деятельности в информационном пространстве проводится в образовательных учреждениях высшего профессионального образования Министерства обороны Российской Федерации.

Кроме того, для решения задач информационной безопасности Вооруженных Сил Российской Федерации могут привлекаться, в установленном законодательством Российской Федерации порядке, специалисты, закончившие иные образовательные учреждения Российской Федерации.

3. Правила

В ходе своей деятельности Вооруженные Силы Российской Федерации руководствуются совокупностью правил сдерживания, предо-

твращения и разрешения военных конфликтов в информационном пространстве

Военная политика Российской Федерация
направлена на недопущение гонки вооружений,
сдерживание и предотвращение военных конфликтов...
(Военная доктрина Российской Федерации, утвержденная
Указом Президента Российской Федерации
от 5 февраля 2010 г., ст. 17)

3.1. Сдерживание и предотвращение конфликтов

Вооруженные Силы Российской Федерации в своей практической деятельности руководствуются следующими правилами сдерживания и предотвращения военных конфликтов в информационном пространстве:

1. Развивать систему обеспечения информационной безопасности Вооруженных Сил Российской Федерации, предназначенную для сдерживания и разрешения военных конфликтов в информационном пространстве.

2. Поддерживать силы и средства обеспечения информационной безопасности в постоянной готовности к отражению угроз военно-политического характера в информационном пространстве.

3. Налаживать сотрудничество на приоритетной основе со странами Организации Договора о коллективной безопасности, Содружества Независимых Государств и Шанхайской организации сотрудничества, расширять круг государств-партнеров и развивать сотрудничество с ними на основе общих интересов в сфере укрепления международной информационной безопасности в соответствии с положениями Устава ООН и другими нормами международного права.

4. Стремиться к заключению под эгидой ООН договора об обеспечении международной информационной безопасности, распространяющего действие общепризнанных норм и принципов международного права на информационное пространство.

5. Принимать все возможные меры по раннему выявлению потенциальных военных конфликтов в информационном пространстве, а также разоблачению организаторов конфликта, подстрекателей и пособников.

6. Определять факторы возникновения и эскалации конфликта и устанавливать контроль над ними с тем, чтобы избежать возникновения чрезвычайных ситуаций.

7. Принимать первоочередные меры по противодействию развитию (консервации или обострению) конфликта и его переходу в такое состояние, которое значительно увеличивает цену урегулирования.

8. Принимать меры недопущения распространения конфликта на смежные сферы межгосударственных отношений, на урегулирование последствий которого потребуются дополнительные затраты и усилия.

9. Принимать меры по нейтрализации факторов, породивших конфликт, с тем, чтобы направить взаимодействие конфликтующих сторон в русло конструктивного сотрудничества.

10. Публично, объективно и своевременно разъяснять мировой общественности причины и истоки конфликта. Формирование необходимого общественного мнения подразумевает соответствующую его ориентацию и мобилизацию, позволяет создать в глобальном информационном пространстве климат, способствующий ограничению возможности совершения организаторами конфликта дальнейших эскалационных шагов.

3.2. Разрешение конфликтов

Российская Федерация считает правомерным применение Вооруженных Сил и других войск для отражения агрессии против нее и (или) ее союзников, поддержания (восстановления) мира по решению Совета Безопасности ООН, других структур коллективной безопасности, а также для обеспечения защиты своих граждан, находящихся за пределами Российской Федерации, в соответствии с общепризнанными принципами и нормами международного права и международными договорами Российской Федерации.

(Военная доктрина Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 февраля 2010 г., ст. 20)

Вооруженные Силы Российской Федерации руководствуются следующими правилами разрешения военных конфликтов в информационном пространстве:

1. Разрешение конфликтов в информационном пространстве осуществлять, в первую очередь, путем переговоров, примирения, обращения к Совету Безопасности ООН или к региональным органам, или соглашениям, или иными мирными средствами.

2. В случае усиления напряженности стремиться к недопущению перехода конфликта в крайние, разрушительные формы противоборства, и особенно те, которые могут привести к дестабилизации международной обстановки и возникновению кризисной ситуации.

3. В условиях эскалации конфликта в информационном пространстве и перехода его в кризисную фазу воспользоваться правом на индивидуальную или коллективную самооборону с применением любых избранных способов и средств, не противоречащих общепризнанным нормам и принципам международного права.

4. В интересах решения задач индивидуальной и коллективной самообороны определять необходимый потенциал ответных действий на основе национальных демократических процедур с учетом законных интересов обеспечения безопасности других государств, а также необходимости обеспечения международной информационной безопасности и стабильности.

5. В интересах индивидуальной и коллективной самообороны размещать свои силы и средства обеспечения информационной безопасности на территории других государств в соответствии с соглашениями, выработанными ими на добровольной основе в ходе переговоров, а также в соответствии с международным правом.

6. В ходе конфликта постоянно информировать отечественные и зарубежные СМИ о складывающейся ситуации и, опираясь на общественное мнение, эффективнее влиять на ее деэскалационное развитие и закрепление достигнутых результатов разрешения конфликтных противоречий.

4. Меры доверия

Вооруженные Силы Российской Федерации будут стремиться к выработке мер укрепления доверия в области военного использования информационного пространства. В частности, к таким мерам относятся:

1. Обмен национальными концепциями обеспечения безопасности в информационном пространстве.

2. Оперативный обмен информацией о кризисных событиях и угрозах в информационном пространстве и принимаемых мерах в отношении их урегулирования и нейтрализации.

3. Консультации по вопросам деятельности в информационном пространстве, которая может вызывать озабоченность сторон, и сотрудничество в отношении урегулирования конфликтных ситуаций военного характера.

Заключение

В современных условиях обороноспособность Российской Федерации существенно зависит от эффективности деятельности Вооруженных Сил в информационном пространстве и во многом определяется их возможностями по сдерживанию, предотвращению и разрешению конфликтов, возникающих в информационном пространстве.

Вооруженные Силы Российской Федерации планируют решать стоящие перед ними задачи обеспечения обороны и безопасности, опираясь на основополагающие принципы и правила деятельности Вооруженных Сил Российской Федерации в информационном пространстве, а также меры доверия, изложенные в настоящих Концептуальных взглядах.

Реализуя настоящие Концептуальные взгляды, Вооруженные Силы Российской Федерации будет стремиться к максимальному использованию возможностей информационного пространства для укрепления обороноспособности государства, сдерживания и предотвращения военных конфликтов, развития военного сотрудничества, а также формирования системы международной информационной безопасности в интересах всего мирового сообщества.

2.3. Соединенные Штаты Америки

МЕЖДУНАРОДНАЯ СТРАТЕГИЯ В ОТНОШЕНИИ КИБЕРПРОСТРАНСТВА. ПРОЦВЕТАНИЕ, БЕЗОПАСНОСТЬ И ОТКРЫТОСТЬ СЕТЕВОГО МИРА

(Май 2011 г.)
(Извлечения)

[Полное содержание документа

I. Формирование политики в области киберпространства
Стратегический подход.
Опора на достижения.
Осознание вызовов.
Приверженность принципам.
II. Будущее киберпространства

Будущее, к которому мы стремимся.
Открытость и функциональная совместимость (интероперабельность): киберпространство, открывающее возможности.
Безопасность и надежность: киберпространство, которое выдерживает испытание временем.
Стабильность через создание норм.
II. Наша роль в будущем киберпространстве
Дипломатия: укрепление партнерства.
Система обороны: сдерживание и предупреждение.
Развитие: содействие процветанию и безопасности.
III. Политические приоритеты
Экономика: продвижение международных стандартов и инновационных, открытых рынков.
Защита наших сетей: повышение безопасности, надежности и устойчивости.
Правоприменение: расширение сотрудничества и верховенство закона.
Военные аспекты: подготовка к решению проблем безопасности XXI века.
Управление интернетом: продвижение эффективных и всесторонних структур.
Международное развитие: потенциал, безопасность и процветание.
Свобода интернета: поддержка основных свобод и частной жизни.
IV. Движение вперед]

I. Формирование политики в сфере киберпространства

Цифровая инфраструктура во все большей степени становится главной опорой процветающих экономик, энергичных научных сообществ, мощных держав, исповедующих принципы прозрачности правительств и свободных обществ. Как никогда прежде, информационные технологии благоприятствуют транснациональному диалогу и облегчают глобальные потоки товаров и услуг. Такие социальные и торговые свя-

зи становятся совершенно необходимыми для нашей повседневной жизни. Особо важные инфраструктурные системы, обеспечивающие нас электричеством и водой, контролирующие движение воздушных судов, поддерживающие нашу финансовую систему, – все они зависят от объединенных в сети информационных систем. В настоящее время страны стремятся рационализировать оказание основных услуг средствами так называемого электронного правительства. Социальные и политические движения строят свою работу на основе интернета как способа достижения новых, более широких организационных форм и акций. Охват сетевых технологий поистине впечатляющ и глобален. Для всех стран мира базовая цифровая инфраструктура является или станет в скором будущем национальным активом.

Для полномасштабной реализации тех преимуществ и выгод, которые сетевые технологии способны дать миру, такие системы должны работать надежно и безопасно. У людей должна быть уверенность в том, что информация будет доставляться адресату безошибочно и без срывов. Обеспечение свободных информационных потоков, безопасности и конфиденциальности информации, надежной работы связанных между собой сетей имеет жизненно важное значение для процветания экономики США и всего мира, безопасности и укрепления всеобщих прав.

Почти треть населения мира пользуется интернетом, и гораздо больше людей, так или иначе, затрагиваются Всемирной сетью в повседневной жизни. Сегодня в мире насчитывается свыше 4 млрд цифровых беспроводных устройств. Каких-то 50 лет назад это число равнялось нулю. Мы переживаем тот редкий исторический момент, когда имеется реальная возможность обеспечить на фундаменте успехов киберпространства его безопасное будущее для граждан США и мирового сообщества.

Для того чтобы эти технологии продолжали открывать новые возможности людям, улучшать общество, содействовать научным исследованиям, развитию и инновациям, столь важным для формирования современных экономик, интернет должен сохранить открытость и функциональную совместимость, которые до сих пор неизменно сопровождали его взрывное развитие. В основе этого лежат технические принципы и эффективные структуры управления, требующие нашей поддержки. В то же время наши сети должны быть надежными и безопасными; они должны сохранять доверие к себе со стороны граждан, бизнеса и правительств, демонстрируя устойчивость к случайным или злоумышленным нарушениям в работе.

Миру надлежит сообща осознать угрозы, связанные с вмешательством злоумышленников в киберпространство, и соответствующим об-

разом модернизировать и укрепить национальные и международные принципы в этой сфере. Действия в интернет-пространстве находят отражение для жизни в обычном, физическом мире, и мы должны работать над укреплением верховенства закона, над устранением того, чтобы риски перевешивали преимущества Сети. Будущее открытого, функционально совместимого, безопасного и надежного киберпространства зависит от того, насколько страны осознают и сумеют защитить то наиболее важное, что должно быть сохранено, и насколько эффективно они будут противодействовать тем, кто хотел бы дестабилизировать или подорвать наш мир, все более тесно объединяемый Сетью.

Стратегический подход

Подход Соединенных Штатов к принципам международного киберпространства основывается на убеждении, что сетевые технологии обладают огромным потенциалом для страны и мира. На протяжении последних трех десятилетий мы, Соединенные Штаты Америки, наблюдали за тем, как эти технологии революционизируют нашу экономику и преобразуют нашу повседневную жизнь. Мы наблюдали также за тем, как в киберпространство проникают проблемы извне, к примеру эксплуатация и агрессия. Адаптируясь к этим вызовам, мы будем подавать пример другим. Соединенные Штаты будут придерживаться таких принципов в отношении международного киберпространства, которые бы открывали возможности для инноваций, стимулирующих развитие экономики и обеспечивающих повышение качества жизни в нашей стране и за рубежом. В основу этой работы будут заложены принципы, имеющие жизненно важное значение не только для внешней политики США, но и для будущего и интернета как такового.

Опора на достижения

Соединенные Штаты Америки привержены сохранению и развитию преимуществ цифровых сетей для наших обществ и экономик.

Осознание вызовов

Соединенные Штаты признают, что развитие этих сетей несет новые вызовы для нашей национальной и экономической безопасности, равно как и для безопасности мирового сообщества.

Приверженность принципам

Соединенные Штаты будут противостоять этим вызовам исходя из защиты наших ключевых принципов.

Наша политика зиждется как на сохранении всего лучшего, что есть в киберпространстве, так и на приверженности нашим принципам. Наша политика в отношении международного киберпространства отражает нашу принципиальную приверженность *защите основных свобод*, *неприкосновенности частной жизни* и *свободе распространения информации*.

<...>

II. Будущее киберпространства

Будущее, к которому мы стремимся

Сфера киберпространства, к которой мы стремимся, поощряет инновации и поддерживает предпринимателей, соединяет индивидуумов и укрепляет общность; влияет на деятельность правительств и способствует «прозрачности» действий правительств; стоит на страже основных свобод и обеспечивает неприкосновенность личной жизни; она способствует пониманию, уточняет нормы поведения и повышает национальную и международную безопасность. **Для поддержания такой среды наилучшей практической формой является международное сотрудничество – это первый принцип.**

Наша цель

Соединенные Штаты Америки будут сотрудничать на международной арене с целью содействия развитию ***открытой, функционально совместимой (интероперабельной), безопасной и надежной*** *инфраструктуры информационных технологий и связи, поддерживающей международную торговлю, повышающей международную безопасность и благоприятствующей свободе слова и инновациям. Для достижения этой цели мы сформируем и будем поддерживать пространство, в котором нормы ответственного поведения регулируют действия государств, поддерживают партнерство, а также верховенство закона в киберпространстве.*

<...>

Стабильность через создание норм

<...>

К числу существующих принципов, которые следует соблюдать в киберпространстве, относятся следующие:

- **защита основных свобод**: государства должны уважать фундаментальные свободы слова и объединений – как в сети, так и вне ее;

• **охрана права собственности**: государства в своих обязательствах и средствами национального законодательства должны соблюдать права интеллектуальной собственности, включая патенты, коммерческие секреты, товарные знаки, авторские права;

• **ценность частной жизни**: граждане должны иметь защиту от произвольного или незаконного вмешательства государства в их частную жизнь, когда они пользуются интернетом;

• **защита от преступлений**: государства должны выявлять и наказывать киберпреступников, обеспечивать отсутствие в законах и правоприменительной практике лазеек для создания преступниками убежищ, своевременно сотрудничать при проведении международных уголовных расследованиях;

• **право на самооборону**: в соответствии с Уставом ООН, государства обладают неотъемлемым правом на самооборону, которая может потребоваться после определенных актов агрессии в киберпространстве.

Из перечисленных выше традиционных принципов межгосударственного поведения могут быть выведены обязательства, в большей степени соответствующие киберпространству. Они сфокусированы прежде всего на сохранение функциональности глобальной сети и повышение уровня безопасности киберпространства. Многие из этих обязательств уходят своими корнями в технические реалии интернета. Поскольку базовая функциональность сети зиждется на системах доверия (к примеру, протокол *BGP* – протокол пограничной маршрутизации), государства должны осознавать возможные международные последствия своих технических решений и действовать уважительно по отношению к сетям других стран и интернету в широком смысле. Аналогичным образом при разработке следующего поколения таких систем мы должны отстаивать общие интересы, поддерживая наиболее здравые технические стандарты и структуры управления, а не те, что нацелены лишь на повышение национального престижа или усиление политического контроля. Эти новейшие нормы, также являющиеся основополагающими для рассматриваемого пространства, включают следующее:

• **глобальная функциональная совместимость (интероперабельность):** государствам надлежит действовать в рамках своих полномочий для содействия обеспечению сквозной функциональной совместимости общедоступного интернета;

• **сетевая устойчивость**: государствам следует уважительно относиться к свободе распространения информации в национальных сетевых

конфигурациях, избегая произвольного вмешательства в международную взаимосвязанную инфраструктуру;

• **надежный доступ: г**осударствам не следует произвольно лишать граждан доступа в интернет или к иным сетевым технологиям либо нарушать такой доступ;

• **многостороннее управление**: усилия по управлению интернетом не должны сводиться к действиям правительств – они должны включать всех заинтересованных лиц;

• **предварительная оценка безопасности киберпространства**: государствам надлежит признать свою ответственность в части защиты информационных инфраструктур и обеспечения безопасности национальных систем от повреждения или злоупотреблений и действовать исходя из такой ответственности.

<...>

Дипломатия: укрепление партнерства

Дипломатическая цель

Соединенные Штаты будут создавать стимулы и вырабатывать консенсус по вопросам международного пространства, в котором государства, признающие ценность открытого, функционально совместимого, безопасного и надежного киберпространства, будут вместе работать и выступать в качестве ответственных участников.

<...>

Система обороны: сдерживание и предупреждение

Цель в области обороны

Соединенные Штаты вместе с другими странами будут поощрять ответственное поведение и противостоять тем, кто пытается нарушать работу сетей и систем, будут обуздывать и сдерживать злоумышленников, сохраняя за собой право защищать эти жизненно важные национальные ценности необходимыми и адекватными средствами.

<...>

Развитие: содействие процветанию и безопасности

Задачи развития

Соединенные Штаты будут содействовать наращиванию потенциала в сфере безопасности киберпространства за рубежом на двусторонней основе, в рамках многосторонних организаций, с тем чтобы каждая страна имела средства для защиты своей цифровой инфраструктуры, будут укреплять глобальные сети, устанавливать более тесное сотрудничество на принципах консенсуса для создания открытых, функционально совместимых, безопасных и надежных сетей.

<...>

III. Политические приоритеты

Экономика: продвижение международных стандартов и инновационных, открытых рынков

С тем чтобы киберпространство и дальше удовлетворяло потребности наших экономик и новаторов, мы будем:

• **поддерживать свободное рыночное окружение, поощряющее технологические инновации через доступные, глобально связанные сети**. Подобно тому, как свобода потоков информации исключительно важна для функционирования наших сетей, свободная торговля способствует поддержке инноваций и рыночному росту в эпоху информации. Глобальный охват интернета во многом отражается в распространении более дешевых и повсеместно доступных компьютеров и сетевых технологий. Конкуренция на этих рынках стимулирует инновации, а среда свободной торговли дает производителям возможность поддерживать конкурентные цены и высокие стандарты. Уважительное отношение к международным стандартам разработки технологий и торговли представляет собой существенную часть поддержания открытых рынков и позволяет компаниям, занимающимся высокими технологиями, быстро доводить до потребителя преимущества своих инновационных продуктов и услуг. В течение нескольких будущих десятилетий глобализация разработки технологий будет только нарастать, принося ощутимые выгоды для наших сетей и потребителей. Соединенные Штаты будут работать над поддержанием такой среды свободной торговли (прежде всего в секторе высоких технологий) для обеспечения будущих инноваций;

• **защищать интеллектуальную собственность, в том числе коммерческую тайну, от воровства**. Те же самые сети, которые питают

инновации, открывают также новые лазейки для промышленного шпионажа и кражи интеллектуальной собственности и коммерческой информации. Киберпространство может использоваться для воровства беспрецедентных объемов информации у компаний, университетов и государственных органов. Потери от кражи информации и технологий могут достигать миллиардов долларов. Отдельные инциденты зачастую остаются незамеченными или необнаруженными. Результат таких действий может варьироваться от недобросовестной конкуренции до банкротства целых компаний, а в национальном масштабе последствия могут быть на несколько порядков более серьезными. Постоянные кражи интеллектуальной собственности, будь то преступниками, иностранными фирмами или агентами тех или иных государств, могут подрывать конкурентность в мировой экономике и снижать инновационные возможности бизнеса. Соединенные Штаты будут принимать меры для обнаружения неправомерных действий и реагирования на такие действия с тем, чтобы укреплять международную среду, в которой подобные действия признаются противозаконными, недопустимыми и требующими привлечения таких нарушителей к ответственности;

• **обеспечивать верховенство совместимых и безопасных технических стандартов, вырабатываемых техническими экспертами**. Разработка международных добровольных, основанных на консенсусе стандартов, относящихся к киберпространству, и создание продуктов, процессов и услуг на основе таких стандартов являются фундаментом интероперабельной, безопасной и устойчивой глобальной инфраструктуры. Государственный и частный секторы должны работать рука об руку над разработкой, поддержанием и внедрением этих стандартов, равно как и поддерживать разработку международных стандартов и процедур оценки соответствия, которые бы устраняли барьеры для международной торговли и коммерции. Международная стандартизация киберпространства и добровольные, основанные на принципе консенсуса процедуры служат общим интересам. Они поощряют инновации, облегчают взаимную функциональную совместимость, повышают безопасность и устойчивость, доверие к транзакциям, осуществляемым через интернет, стимулируют конкуренцию на глобальных рынках. Соединенные Штаты будут укреплять сотрудничество между государственным и частным секторами в поддержку распространения требований к продукции и услугам, основанных на международных стандартах;

Защита наших сетей: повышение безопасности, надежности и устойчивости

Поскольку надежная кибербезопасность критически важна для понимаемой более широко экономической и национальной безопасности, мы:

• **будем стимулировать сотрудничество по вопросам киберпространства, в частности, в области норм поведения государств и кибербезопасности – в двухстороннем порядке и в рамках целого ряда многосторонних организаций и многонационального партнерства**. Все большее число международных организаций вовлекаются в решение вопросов кибербезопасности и киберпространства вообще, и Соединенные Штаты продолжат содействие этой важной работе так, чтобы формируемое киберпространство отвечало потребностям тех организаций, в которых мы участвуем. США приложили усилия для включения насущных вопросов киберпространства в повестку заседаний Организации американских государств (*OAS*), Регионального форума Ассоциации государств Юго-Восточной Азии (*ASEAN*), Организации Тихоокеанского экономического сотрудничества (*APEC*), Организации по безопасности и сотрудничеству в Европе (*OSCE*), Африканского союза (*AU*), Организации экономического сотрудничества и развития (*OECD*), «Большой восьмерки» (*G*-8), Европейского союза, ООН и Совета Европы и для обеспечения того, чтобы такая работа поддерживалась эффективными институциональными структурами. На указанных выше и других форумах Соединенные Штаты продолжат усилия по консолидации регионального и международного консенсуса по ключевым видам деятельности, связанной с киберпространством (в том числе по вопросу норм). Кроме того, мы с надеждой смотрим в сторону форумов, где реально осуществляется многостороннее сотрудничество и продвижение к консенсусу и где могут вырабатываться те принципы дальнейшего развития интернета, которые обсуждаются в этом документе. Мы приветствуем расширение такой работы на географические регионы, в настоящее время не достаточно представленные в диалоге (прежде всего это Африка и Ближний Восток), для продвижения нашего интереса к наращиванию соответствующего потенциала по всему миру;

• **будем бороться за уменьшение числа вторжений в сети США и срывов их работы.** Несанкционированный доступ в сети создает угрозы целостности экономик и подрывает национальную безопасность. Различные ведомства правительства США сотрудничают между собой и с частным сектором в сфере защиты инноваций от промышленного

шпионажа, защиты федеральных сетей, сетей штатов и местных государственных сетей, защиты военных операций в условиях нарушенной операционной среды, защиты критически важной инфраструктуры от вторжений и атак (прежде всего объектов энергетических, транспортных и финансовых систем) и защиты промышленной базы. Соединенные Штаты будут по-прежнему добиваться широкого международного согласия государств, признающих важность уважения к собственности и устойчивости сетей, и будут поддерживать такую точку зрения с учетом нашей готовности и готовности наших партнеров к защите сетей от действий, создающих для них угрозу;

• **обеспечим оперативное реагирование на инциденты, устойчивость и возможности восстановления информационной инфраструктуры.** Во взаимосвязанной глобальной среде низкий уровень безопасности систем одной страны создает риск для других. Ни одна из стран не сможет получить полного ознакомления с системами по всему миру. У нас имеется обязательство делиться информацией о наших собственных сетях и сотрудничать с другими странами в ситуациях, когда те или иные события могут угрожать нам всем. Так как мы продолжаем наращивать и укреплять наши возможности в плане реагирования, мы будем работать сообща с другими странами над расширением международных сетей, поддерживающих повышение уровня глобальной ситуационной осведомленности и реагирования на инциденты (включая сотрудничество между правительством и отраслью). Правительство США активно участвует в контроле, предупреждении инцидентов и реагировании на таковые посредством обмена информацией с надежными сетями международных партнеров. Мы будем и дальше наращивать эти возможности в рамках международного сотрудничества для повышения общего уровня устойчивости. Кроме того, Соединенные Штаты будут прилагать усилия по международному участию в учениях, посвященных безопасности в киберпространстве, по повышению качества и усилению существующих оперативных процедур вместе с нашими партнерами;

• **повысим надежность высокотехнологичной цепочки поставок, в консультациях с отраслью.** Работа критически важных сетей и информационных инфраструктур зависит от гарантированной эксплуатационной готовности надежного аппаратного и программного обеспечения. Уязвимости в логистических цепочках могут открыть возможности для атак на целостность, готовность или конфиденциальность сетей и содержащихся в них данных. Использование этих уязвимых мест снижает экономическую эффективность и ослабляет национальную

безопасность. Соединенные Штаты продолжат сотрудничество с отраслевыми и международными партнерами в том, что касается разработки передовых практических методов защиты целостности информационных систем и критически важной инфраструктуры. Таким образом мы значительно повысим безопасность глобализированных логистических цепочек, от которых зависит свободная открытая торговля.

Правоприменение: расширение сотрудничества и верховенство закона

Для повышения доверия к киберпространству и преследования тех, кто допускает злоупотребления в онлайн-системах, мы будем:

• **принимать полноценное участие в развитии международной политики по вопросам киберпреступности.** Соединенные Штаты обязуются активно участвовать в обсуждениях вопросов выработки международных норм и мер по киберпреступности в рамках двусторонних и многосторонних контактов, на форумах, доказавших свою компетентность и имеющих достижения в плане продвижения эффективных принципов борьбы с такой преступностью. Обсуждения подобного рода будут включать текущие усилия, например, по расширению области влияния таких институтов, как Будапештская конвенция. США будут базировать эти усилия на успешном партнерстве между национальными правоприменительными органами и на плодотворных политических диалогах, которые мы в настоящее время ведем, развивая чувство ответственности у государств, вовлекаемых в такую работу;

• **гармонизировать законы о киберпреступности на международном уровне, расширяя число стран, присоединившихся к Будапештской конвенции.** Соединенные Штаты и наши союзники зачастую оказываются поставленными в зависимость от сотрудничества с другими странами и их содействия при расследовании киберпреступлений и привлечении нарушителей к ответственности. Такое сотрудничество наиболее эффективно и содержательно, когда страны имеют схожие законы о преступлениях в киберпространстве, что облегчает совместное использование улик, экстрадицию и другие формы скоординированных действий. Будапештская конвенция по борьбе с преступлениями в киберпространстве дает странам модель для выработки проектов таких законов и внесения изменений в соответствующее законодательство, она доказала свою эффективность в качестве механизма углубления международного сотрудничества при расследовании киберпреступлений. Соединенные Штаты продолжат поощрение других стран к присоединению к Конвенции и оказание содействия пока

не присоединившимся в использовании Конвенции в качестве основы для разработки собственных законов. В краткосрочной перспективе это позволит облегчить двустороннее сотрудничество, а в долгосрочной – подготовит такие страны к присоединению к Конвенции;

• **делать акцент в законах о киберпреступности на борьбе с нелегальной деятельностью, а не на ограничении доступа в интернет.** Действия преступников в киберпространстве должны наталкиваться на эффективную правоприменительную практику. Здесь нельзя сводить все к политике ограничения законного доступа к интернету или находящемуся там контенту. Для достижения этой цели правительство Соединенных Штатов работает в рамках двусторонних и многосторонних контактов для обеспечения понимания другими странами того, что акцент в борьбе против онлайн-преступлений должен быть сделан на предупреждении таких деяний, поимке и наказании нарушителей, а не на неизбирательном ограничении доступа к интернету, поскольку широкое ограничение доступа затрагивает невинных пользователей. В условиях, когда Соединенные Штаты и наши партнеры вовлечены в диалог и содействуют упрочению потенциала в сфере правоприменения по всему миру, мы намерены интегрировать этот подход, объединив защиту неприкосновенности частной жизни, основных свобод и инноваций с сотрудничеством в сфере борьбы с преступлениями в киберпространстве;

• **стремиться лишить террористов и прочих преступников возможности использовать интернет для планирования операций, их финансирования или проведения атак.** Соединенные Штаты обладают разнообразными международными программами по наращиванию потенциала и обучению по вопросам киберпреступности. Он могут быть использованы правоприменительными органами и законодателями для разработки эффективных правовых норм и получения компетенций для расследования и преследования лиц, использующих интернет для террористических или иных преступных целей. Лишение террористов возможностей (тем более их расширения) для найма хакеров и использования организованных преступных инструментов представляет собой важный приоритет для международного сообщества, и решение этой проблемы потребует эффективных законов по киберпреступности. Соединенные Штаты исполнены решимости выявлять и пресекать работу сетей финансирования террористов и киберпреступников, используя для этого технический инструментарий и структуры международного сотрудничества (к примеру, Международную группу по борьбе с финансовыми злоупотреблениями (*FATF*)).

Военные аспекты: подготовка к решению проблем безопасности XXI века

В силу нашего обязательства по защите наших граждан, союзников и интересов в любой точке, где они окажутся под угрозой, мы:

• **будем учитывать растущие потребности военных в надежных и безопасных сетях и приспосабливаться к этим потребностям.** Мы осознаем, что наши вооруженные силы во все большей степени зависят от сетей, поддерживающих их работу, и намерены работать над обеспечением того, чтобы наши военные оставались в полной мере оснащенными для проведения операций даже в такой среде, где другие силы могут попытаться нарушить работу систем или иной инфраструктуры, жизненно важных для национальной обороны. Как и все страны, Соединенные Штаты имеют непреходящий интерес в сфере защиты наших жизненно важных активов, равно как и наших базовых принципов и ценностей, и мы обязуемся защищаться от тех, кто попытается ослабить наши возможности в этой области;

• **создадим и усовершенствуем существующие военные союзы для противостояния возможным угрозам в киберпространстве.** Безопасность в киберпространстве не может быть достигнута одной страной в отрыве от других, и потребуется серьезное международное сотрудничество для противодействия лицам, стремящимся нарушить работу наших сетей или использовать их в ненадлежащих целях. Работа в этом направлении начинается с признания того факта, что связанные между собой сетевые системы наших ближайших союзников (к примеру, системы НАТО и стран-членов НАТО) создают как возможности, так и новые риски. Продолжая движение вперед, Соединенные Штаты будут и дальше сотрудничать с военными и гражданскими коллегами наших союзников и партнеров для расширения ситуационной осведомленности и совместного использования систем предупреждения, укрепления наших возможностей для сотрудничества в мирное время и во время кризисов, разработки средств и методов коллективной самообороны в киберпространстве. Такие военные союзы и партнерства будут усиливать наши коллективные возможности в части сдерживания, равно как и наши возможности в плане защиты Соединенных Штатов от действий со стороны других государств или иных лиц;

• **расширим сотрудничество с союзниками и партнерами в киберпространстве с целью повышения общей безопасности.** Вызовы в сфере киберпространства создают также возможности для совместной работы в новых направлениях с военными союзниками и партнерами. Развивая общее понимание стандартных операционных процедур, наши воору-

женные силы способны повышать уровень безопасности посредством координации усилий и более широкого обмена информацией. Эти контакты снижают вероятность ошибочного восприятия оборонной деятельности и возможности для эскалационного поведения. Диалог и обмен передовыми практическими подходами как способ усиления партнерских возможностей (например, цифровые методы судебной экспертизы, развитие персонала, тестирование защиты от несанкционированного доступа в сеть и устойчивости сети) представляются важными в этом плане. Соединенные Штаты будут работать в тесном партнерстве с государствами-единомышленниками для максимально полезного использования всех возможностей, снижения коллективных рисков, содействия многосторонним инициативам с целью сдерживания злоупотреблений в киберпространстве.

Управление интернетом: продвижение эффективных и всесторонних структур

Для продвижения структур управления интернетом, эффективно удовлетворяющих нужды всех пользователей интернета, мы:

• **сделаем упор на открытость и инновации в интернете.** Возможности для эффективного распространения информации в интернете лежат в основе современной экономической, политической, научной и образовательной деятельности, а также активности потребителей. Правительства всего мира признают ценность интернета, однако многие из них накладывают произвольные ограничения на свободные потоки информации или используют подобные меры для подавления деятельности инакомыслящих или оппозиции. В разных странах применяются самые разные методы и формы реализации таких ограничений, равно как и обоснования этих мер, но мы не должны допустить внесение изменений в структуру управления или технической архитектуры интернета, если это может упростить осуществление решений, нарушающих основные свободы или излишне затрудняющих инновации. Эффективное и всестороннее управление интернетом может помочь в обеспечении того, чтобы действия, грубо нарушающие международные нормы допустимого управления сетями, не облегчались технической структурой или структурой управления. Сохранение, облегчение и расширение доступа к открытому глобальному интернету являются отчетливым политическим приоритетом. Соединенные Штаты продолжат движение к этим целям в рамках разнообразных контактов, включая работу в соответствующих многосторонних институтах и организациях, а также межправительственных и неправительственных организациях;

• **сохраним безопасность и стабильность глобальной сети, в том числе систему доменных имен (*DNS*).** Учитывая важность интернета для мировой экономики, представляется существенным, чтобы эта «сеть сетей» и лежащая в ее основе инфраструктура (*DNS*) оставались стабильными и безопасными. Для сохранения и поддержания стабильности и безопасности совершенно необходимо, чтобы США и остальные страны мира и дальше признавали вклад всего спектра заинтересованных сторон, в первую очередь тех организаций и технических экспертов, чья работа жизненно важна для функционирования интернета. Соединенные Штаты осознают, что эффективная координация этих ресурсов способствовала успеху интернета, и продолжат поддерживать указанные эффективные многосторонние процессы;

• **будем создавать площадки для многосторонних дискуссий по вопросам управления интернетом и содействовать работе этих площадок.** Сама архитектура интернета являет собой модель социальной и технической организации – децентрализованной, скоординированной и многоуровневой. Каждая из этих характеристик фундаментальна с точки зрения преимуществ и выгод интернета. Такая архитектура питает свободу инноваций, содействующую экономическому росту. Она питает свободу слова и объединений, которые способствуют социальному и политическому развитию и функционированию демократических обществ по всему миру. Соединенные Штаты по-прежнему убеждены в том, что, если международное сообщество проводит заседания с целью обсуждения целого спектра вопросов, связанных с управлением интернетом, то такие дискуссии должны проводиться с привлечением многих сторон. Мы и дальше будем оказывать поддержку эффективным площадкам, например, Форуму по управлению интернетом (*IGF*), который отражает открытую и всестороннюю природу самого интернета, давая возможность участникам, не представляющим государства, вносить свой вклад в обсуждение наряду с представителями государств.

Международное развитие: потенциал, безопасность и процветание

Для глобального продвижения преимуществ сетевых технологий, повышения надежности сетей общего пользования и формирования сообщества ответственных участников в киберпространстве мы будем:

• **обеспечивать страны, желающие создать технический потенциал и потенциал в сфере кибербезопасности, необходимыми знаниями, обучением и прочими ресурсами.** Преимущества взаимосвязанного мира не должны ограничиваться национальными границами. Более десяти лет США способствовали ликвидации этого разрыва посредством

поддержки разнообразных программ с целью оказания помощи другим странам в получении ресурсов и навыков для формирования базового потенциала в сфере технологий и кибербезопасности. Наша цель – поделиться с другими странами свои опытом, в частности, «встроить» кибербезопасность в общую канву их национального технического развития. С учетом многообразия потребностей, диапазон наших программ варьируется от поддержки национальных возможностей в сфере управления инцидентами и формирования государственно-частного партнерства до повышения уровня безопасности систем управления, выработки проектов эффективных законов расследования киберпреступлений и наказания виновных, а также разработки и осуществления программ по повышению уровня осведомленности и воспитанию культуры в сфере кибербезопасности. Такая работа велась в рамках двусторонних контактов, через программы помощи другим странам, а также через партнерство с инновационными государственно-частными инициативами (к примеру, на базе Американского института повышения квалификации в сфере телекоммуникаций (*USTTI*)). В последние годы мы сумели сделать эту работу приоритетной для таких форумов, как Организация американских государств (*OAS*), Организация Тихоокеанского экономического сотрудничества (*APEC*) и ООН. В ближайшие годы Соединенные Штаты намерены расширять это сотрудничество, работать внутри страны в поддержку инвестиций частного сектора в укрепление потенциала, привлекать внимание к этой исключительно важной потребности и искать новые варианты сотрудничества;

• **неуклонно развивать передовые практические подходы в области международной кибербезопасности и регулярно делиться такими наработками.** В настоящее время странам больше не нужно наращивать потенциал в области кибербезопасности исключительно методом проб и ошибок. Мы располагаем опытом работы с другими странами и множеством многосторонних организаций по разработке и совместному использованию передовых практических подходов, позволяющих государствам делать более взвешенные инвестиции и вырабатывать более эффективные политики. Соединенные Штаты продолжат усилия по определению, разработке и усовершенствованию передовых подходов и технических стандартов в сотрудничестве и тесном партнерстве с отраслью. Более того, мы расширим наши усилия для повышения уровня осведомленности и облегчения доступа к таким подходам и стандартам. Мы и дальше будем поддерживать совместные научные исследования и технические разработки с целью совершенствования инструментария и средств обеспечения кибербезопасности.

• **укреплять возможности государств в плане борьбы с киберпреступностью, в том числе путем обучения правоохранительных органов, судебных специалистов, юристов и законодателей.** Поскольку уголовные дела, касающиеся компьютерных сетей, зачастую связаны с уликами и целями, находящимися по другую сторону океана, правительства находятся в постоянной зависимости друг от друга в том, что касается технического и следственного содействия (зачастую обширного) по вопросам, затрагивающим национальную безопасность и совершение серьезных преступлений. Угрозы со стороны преступников могут исходить из любой страны, подключенной к сети, и многие государства нуждаются в существенной помощи в части развития следственного потенциала, необходимого для сотрудничества в рамках указанных выше расследований. Предоставляя обучение по этим вопросам, мы развиваем весьма важные контакты и помогаем овладевать техническими аспектами правоприменительной практики. Такое вовлечение улучшает перспективы эффективного сотрудничества и взаимопомощи в области обеспечения соблюдения законности. Соединенные Штаты продолжат движение к этой цели, предоставляя обучение во многих регионах мира, включая нашу работу в Африке и сотрудничество с Организацией Тихоокеанского экономического сотрудничества, Ассоциацией государств Юго-Восточной Азии, «Большой восьмеркой» и Организацией американских государств;

• **налаживать отношения с лицами, принимающими политические решения, с целью наращивания технического потенциала, обеспечивая постоянные и продолжительные контакты с экспертами и их коллегами из правительства Соединенных Штатов.** В последние несколько лет развивающееся международное сообщество лиц, принимающих политические решения, вовлеченное в решение вопросов киберпространства, предложило новые направления для диалога, запустило новые инициативы в сфере развития и безопасности и укрепило многочисленные двусторонние контакты. Осуществляя инвестиции в долгосрочное будущее развивающихся стран посредством наращивания технического потенциала и потенциала в сфере кибербезопасности, Соединенные Штаты нацелены на укрепление таких контактов по оказанию помощи до уровня более тесных партнерств по вопросам, представляющим общий интерес. Мы взяли на себя ведущую роль в созыве таких форумов, как, например, Меридиональная конференция, где обсуждаются ключевые вопросы защиты информационной инфраструктуры. США приветствуют тот факт, что все большее число государств присоединяется к диалогу, так как это означает повышение уровня их озабоченности

проблемами будущего киберпространства, и мы продолжим работу по укреплению связей между экспертами и лицами, принимающими ключевые решения.

Свобода интернета: поддержка основных свобод и частной жизни

Для защиты основных свобод и неприкосновенности частной жизни в киберпространстве, мы:

• **будем поддерживать представителей гражданского общества в создании надежных, защищенных и безопасных платформ для свободы слова и объединений.** Мы поощряем использование людьми по всему миру цифровых средств для выражения мнений, распространения информации, контроля выборов, обличения коррупции, организации социальных и политических движений и осуждаем тех, кто преследует лиц, применяющих такие технологии, безосновательно арестовывает их, угрожает им или совершает в их отношении акты насилия. Подобная «культура страха» отбивает у других членов сообщества охоту к использованию новых технологий для распространения информации, создания организаций или обмена мыслями. Такие же защитные меры должны распространяться на интернет-провайдеров и других провайдеров услуг связи, которые точно так же зачастую становятся жертвами правовых норм об опосредованной ответственности, которые переносят роль цензоров на компании. Соединенные Штаты являются неутомимым поборником основных свобод слова и объединений, осуществляемых, в том числе через киберпространство. Наша страна будет работать над обеспечением прав деятелей гражданского общества, правозащитников и журналистов на использование цифровых сред. Мы продолжим стимулировать правительства к противодействию угрозам в киберпространстве вместо возложения на компании ответственности с неприемлемым ограничением либо свободы слова, либо свободы информационных потоков;

• **вместе с гражданским обществом и неправительственными организациями будем работать над мерами по защите их интернет-активности от незаконных цифровых вторжений.** Повышение кибербезопасности в гражданском обществе и среди неправительственных организаций содействует обеспечению более широкого распространения свободы слова и свободы объединений в «цифровую эпоху». Безопасность в киберпространстве особенно важна для активистов, адвокатов и журналистов, находящихся в первых рядах тех, кто может выражать непопулярные мысли и мнения и кто часто становится жертвой взломов ящиков электронной почты, веб-сайтов, мобильных телефонов и систем

хранения данных. США поддерживают усилия, направленные на то, чтобы дать таким пользователям возможности защиты, обеспечить им возможность осуществления прав на свободу слова и объединений с использованием новых технологий XXI века;

• **будем поощрять международное сотрудничество с целью эффективной защиты коммерческих данных.** Защита неприкосновенности частной жизни имеет существенное значение с точки зрения доверия, на котором базируется использование интернета для экономических и социальных целей. Соединенные Штаты обладают большим опытом применения законов о неприкосновенности частной жизни, равно как и опытом стимулирования выработки политики с участием многих сторон. Мы продолжаем укреплять правовые нормы США о защите коммерческой информации, для того чтобы не отстать от стремительного прогресса сетевых технологий. Мы признаем значимость применения основных принципов неприкосновенности частной жизни в коммерческом контексте при поддержании гибкости, необходимой для инноваций. Соединенные Штаты продолжат усилия для продвижения к общему признанию законов, имеющих одни цели и стимулирующих сотрудничество в сфере правоприменения для защиты частной жизни и поощрения инноваций;

• **обеспечим сквозную совместимость для всеобщей доступности интернета.** Пользователи должны быть уверены в том, что информация, которую они передают в интернете, будет получена в том виде, как это задумано, причем в любой точке мира. Не менее важным является ожидание, что при нормальных обстоятельствах данные смогут свободно пересекать границы (вне зависимости от происхождения и адресата). Обеспечение целостности информации, передаваемой по интернету, наполняет пользователей доверием к сети и сохраняет сеть в качестве открытой платформы для инноваций, питающей рост мировой экономики и стимулирующей обмен идеями между людьми по всему миру. Соединенные Штаты продолжат разъяснение преимуществ интернета, глобального по своей природе, и противодействие расщеплению Всемирной паутины на национальные интрасети, что лишит граждан доступа к контенту из-за рубежа.

IV. Движение вперед

<...>

Настоящая стратегия намечает ориентиры, в соответствии с которыми министерства и ведомства Соединенных Штатов смогут лучше

определить и скоординировать свое место и роль в нашей международной политике в сфере киберпространства, с тем чтобы выбрать конкретный путь движения вперед и спланировать его реализацию. Это призыв к частному сектору, гражданскому обществу и пользователям для умножения усилий через партнерство, повышение осведомленности и конкретные действия. Что еще более важно – это приглашение другим государствам и народам присоединиться к нам в реализации представленного видения процветания, безопасности и открытости нашего сетевого мира. Эти идеалы являются краеугольными для сохранения того киберпространства, которое мы знаем, и для достижения совместными усилиями того будущего, которого мы хотим достичь.

ГОСУДАРСТВЕННЫЙ ДЕПАРТАМЕНТ О ДОКЛАДЕ ООН ПО ВОПРОСАМ КИБЕРБЕЗОПАСНОСТИ И КИБЕРПРОСТРАНСТВА

8 июня 2013 г.

ГОСУДАРСТВЕННЫЙ ДЕПАРТАМЕНТ США
Офис пресс-секретаря
7 июня 2013 г.
2013/0705

ЗАЯВЛЕНИЕ ПРЕСС-СЕКРЕТАРЯ ДЖЕН ПСАКИ

Заявление о консенсусе, достигнутом Группой правительственных экспертов ООН по вопросам киберпространства

Соединенные Штаты приветствуют публикацию знакового консенсусного доклада по итогам заседания Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, состоявшегося на этой неделе.

Посредством этих дискуссий Соединенные Штаты стремились к достижению взаимопонимания по вопросам киберпространства, имеющим ключевое национальное и международное значение, в частности: необходимость обеспечения международной стабильности, прозрачности и доверия в киберпространстве; поведение государств

в отношении использования киберпространства должно определяться действующим международным правом; и как международное сообщество может способствовать наращиванию потенциала менее развитых стран в области кибербезопасности. Наша делегация покидает Нью-Йорк с уверенностью в том, что комплексный консенсусный доклад, опубликованный Группой, поможет добиться существенного прогресса по всем этим вопросам.

Группа согласилась, что меры по укреплению доверия, такие как контакты на высоком уровне и своевременный обмен информацией, могут повысить доверие и уверенность среди всех стран и способствовать снижению риска возникновения конфликта благодаря повышению предсказуемости и устранению ошибочных представлений. Группа согласилась, что наращивание потенциала для расширения глобального сотрудничества в области обеспечения безопасности киберпространства имеет жизненно важное значение. Группа вновь подтвердила важность открытости и доступности киберпространства, поскольку это обеспечивает экономическое и социальное развитие. Также Группа согласилась, что совокупность всех этих усилий будет способствовать укреплению безопасности киберпространства.

Кроме того, Группа подтвердила, что на киберпространство распространяется действие международного права, в частности, Устава ООН.

Все страны-участницы ООН разделяют общую приверженность делу защиты мира. Мы все являемся сторонами Устава ООН, направленного на предотвращение любых войн. Мы также поддерживаем Женевские конвенции и Право вооруженных конфликтов, целью которых является уменьшение страданий гражданского населения при возникновении вооруженного конфликта. Эти нормы – краеугольный камень международных отношений, и они особенно важны для киберпространства, где межгосударственная деятельность получает все большее распространение.

Соединенные Штаты с удовлетворением присоединяются к консенсусу, подтверждающему применимость международного права к киберпространству. Вместе с этим четким заявлением данный консенсусный доклад направляет мощный сигнал: государства должны действовать в киберпространстве, следуя установленным международным правилам и принципам, которые определяли их действия на протяжении десятилетий в мирное время и во время конфликтов.

Соединенные Штаты надеются на будущий диалог с международным сообществом по этим вопросам.

2.3. Финляндия

СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ ФИНЛЯНДИИ[1]

(Постановление Правительства от 24 января 2013 г.)

(Извлечения)

Кибербезопасность означает желательное конечное состояние, в котором киберпространство является надежным и в котором обеспечивается ее функционирование.

1. Введение

Обеспечение безопасности общества является ключевой задачей органов государственной власти, и жизненно важные функции нашего общества должны быть защищены во всех ситуациях. Будучи информационным обществом, Финляндия зависит от информационных сетей и систем, и, следовательно, чрезвычайно уязвима в плане нарушений, которые влияют на их функционирование. Киберпространство является международным термином для такой взаимозависимой, многоцелевой среды обработки электронных данных.

Растущая информационная интенсивность общества, увеличение иностранной собственности и аутсорсинга, интеграция информационных технологий и технологий связи, использование открытых сетей, а также растущая зависимость от электроэнергии определяют совершенно новые требования к защите жизненно важных функций общества в нормальных условиях, в условиях серьезных нарушений нормальных условий, и в чрезвычайных ситуациях.

Угрозы для киберпространства влекут все более существенные последствия для физических лиц, предприятий и общества в целом. Преступники стали более профессиональными, нежели раньше, и угрозы на сегодняшний день даже включают в себя государственные службы. Кибератаки могут использоваться в качестве средства политического и экономического давления; давление во время серьезного кризиса может оказываться в качестве инструмента влияния наряду с традиционными средствами военной силы.

Киберпространство следует рассматривать и как возможность, и как ресурс. Безопасное киберпространство упрощает планирование своей

[1] Finland's Cyber security Strategy. – URL: http://www.yhteiskunnanturvallisuus.fi/en/materials (неофициальный перевод О.В. Демидова и М.Б. Касеновой).

деятельности как для частных лиц, так и для организаций, что в свою очередь стимулирует экономическую деятельность. Надлежащим образом функционирующая среда также повышает привлекательность Финляндии для иностранных инвесторов. В дополнение к этому, кибербезопасность сама по себе является новым и крепнущим направлением предпринимательской деятельности. В дополнение к увеличению возможностей для работы и налоговым поступлениям, общество получает выгоды от данного крепнущего сектора бизнеса различными путями. Национальная кибербезопасность взаимосвязана с успехом финских компаний.

Настоящая Стратегия определяет ключевые цели и руководящие принципы, используемые для реагирования на угрозы киберпространству и обеспечивающие его функционирование. Соблюдая руководящие принципы Стратегии кибербезопасности и требуемые меры, Финляндия может управлять умышленными или непреднамеренными нарушениями в киберпространстве, а также реагировать и восстанавливаться после них.

Меры комплексной безопасности определены в постановлении Правительства от 5 декабря 2012 года, в то время как Стратегия безопасности для общества (2010 г.) определяет принципы обеспечения функций, жизненно важных для общества. Жизненно важные функции включают в себя управление делами в ведении Правительства, международную деятельность, военный потенциал Финляндии, внутреннюю безопасность, функционирование экономики и инфраструктуры, гарантию получения дохода населением и способность к функционированию, а также психологическую устойчивость к кризису. Процесс реализации Стратегии кибербезопасности является элементом реализации Стратегии безопасности для общества. Процесс реализации стратегии кибербезопасности является частью реализации Стратегии безопасности для общества; Стратегия кибербезопасности соответствует принципам и определениям Стратегии безопасности для общества и постановлению Правительства о безопасности поставок. Постановление Правительства (2013 г.) определяет ключевые направления и цели для безопасности поставок. Стратегия учитывает ожидаемое постановление Правительства по мерам комплексной безопасности.

Кибербезопасность не предназначена для того, чтобы являться правовой концепцией, принятие которой приведет к предоставлению новых компетенций органам власти или другим официальным учреждениям. В связи с этим не предлагаются какие-либо изменения к основам мероприятий для чрезвычайных ситуаций или к регламентам в отношении компетенций органов власти.

Стратегия представляет видение, подход и стратегические руководящие принципы кибербезопасности. В предварительном пакете документации Стратегии отражены объекты, значимые для стратегических руководящих принципов, такие как киберпространство, его быстрое развитие и потенциально вытекающие из этого угрозы, а также требуемые контрмеры для защиты функций, жизненно важных для общества. В дополнение к этому в пакете документации описываются принципы управления кибербезопасностью и меры контроля в случае нарушений, а также положения, относящиеся к кибербезопасности, и принципы подготовки плана действий для Стратегии кибербезопасности.

Готовящийся план действий будет охватывать практические меры, порученные административным органам и субъектам. Это создает условия для реализации стратегических руководящих принципов, а также видение достижения желательного конечного состояния, включая совместно согласованные меры в масштабе общества.

2. Видение кибербезопасности

Будучи небольшой, обладающей потенциалом и принимающей участие в совместных проектах страной, Финляндия обладает отличными возможностями для того, чтобы быть в авангарде кибербезопасности. Мы обладаем значительной базой знаний и большим экспертным опытом, давней традицией тесного государственно-частного сотрудничества, основанного на доверии, а также межотраслевого сотрудничества.

Видение кибербезопасности Финляндии заключается в следующем:

• Финляндия способна защитить свои жизненно важные функции от киберугроз во всех ситуациях.

• Граждане, органы власти и коммерческие компании могут эффективно пользоваться безопасным киберпространством и компетенцией, вытекающей из мер кибербезопасности, как в государственном, так и в международном масштабе.

• К 2016 году Финляндия станет общемировым лидером в вопросах готовности к киберугрозам и контроля нарушений, вызванных такими угрозами.

<...>

3. Управление кибербезопасностью и национальный подход

Изменения, которые происходят в киберпространстве, наступают быстро, и их последствия трудно прогнозировать. Цикл разработки

программного обеспечения для информационных технологий короток, и такая же тенденция распространяется на различные формы кибератак и вредоносные программные средства. Подготовленность к киберугрозам и киберзащита требуют все более быстрых, прозрачных и согласованных действий всех сторон общества как в плане индивидуальных, так и коллективных усилий.

Правительство представляет собой наивысший уровень управления кибербезопасностью. Правительство несет ответственность за обеспечение политического руководства и стратегические руководящие принципы в отношении кибербезопасности, а также за принятие требуемых решений в отношении ресурсов и предварительных условий их распределения.

Управление кибербезопасностью и устранение нарушений требуют, чтобы Правительство и различные субъекты располагали надежной картиной кибербезопасности в реальном времени в отношении состояния жизненно важных функций общества, а также нарушений, влияющих на их функционирование. Каждое министерство и административное учреждение отвечает за кибербезопасность и устранение нарушений в рамках своих полномочий. Киберпространство и характер угроз подчеркивают важность сотрудничества, а также эффективной и гибкой координации. Стратегические задачи кибербезопасности министерств и связанные с ними требования к разработке основываются на анализе выявленных киберугроз, а также на требованиях к устранению нарушений, определенных на основе указанного анализа. Каждое министерство в рамках своей сферы ответственности должно проконтролировать выполнение стратегических задач, определенных на основе желательных конечных состояний.

Устойчивость государства к киберугрозам будет предусматриваться таким образом, чтобы обеспечить готовность и прогностический потенциал, требуемый целями комплексной безопасности, а также содействию работоспособности во время кибернарушений и периода восстановления после нарушений.

Национальный подход к управлению кибербезопасностью Финляндии основывается на следующих принципах.

1. В соответствии с постановлением Правительства в отношении задач, поручаемых министерствам, вопросы, которые относятся к кибербезопасности, входят, как правило, в круг задач Правительства. Каждое министерство отвечает в своем секторе за подготовку к вопросам, связанным с кибербезопасностью, и соответствующую организацию административных дел.

2. Поскольку кибербезопасность является важной частью комплексной безопасности общества, подход к ее реализации соответствует принципам и процедурам, установленным в Стратегии безопасности для общества.

3. Кибербезопасность зависит от мер информационной безопасности общества в целом. Кибербезопасность зависит от соответствующих и достаточных решений по безопасности информационно-коммуникационных технологий и сетей телекоммуникаций, устанавливаемых каждым субъектом, действующим в кибернетическом мире. Различные совместные меры и мероприятия способствуют и поддерживают их реализации.

4. Подход к реализации кибербезопасности основывается на эффективном и широкомасштабном сборе информации, анализе и системе сбора данных, а также на общей и совместной осведомленности о ситуации, национальном и международном сотрудничестве в отношении готовности. Для этого требуется создание Центра кибербезопасности, а также разработки мер информационной безопасности для всего общества, действующего круглосуточно на протяжении всей недели.

5. Меры кибербезопасности соответствуют разделению обязанностей между органами власти, компаниями и организациями в соответствии с законодательными актами и согласованным сотрудничеством. Быстрая адаптируемость, а также способность пользоваться новыми возможностями и реагировать на непредвиденные ситуации требуют осознания стратегической гибкости и соблюдения правовых норм со стороны субъектов по мере того, как они продолжают развиваться и управлять мерами, нацеленными на достижение кибербезопасности.

6. Кибербезопасность выстраивается в соответствии с функциональными и техническими требованиями к ней. В дополнение к национальным действиям вносится вклад в международное сотрудничество, а также принимается участие в международных НИОКР и проектах. Реализация НИОКР и образования в сфере кибербезопасности на различных уровнях не только укрепляет национальный экспертный опыт, но и поддерживает Финляндию в качестве информационного общества.

7. В ходе развития кибербезопасности будут осуществлены значительные инвестиции в научно-исследовательские и опытно-конструкторские работы, занятость и разработку продукции, с тем чтобы Финляндия могла стать одной из ведущих стран в сфере кибербезопасности.

8. Для обеспечения развития кибербезопасности Финляндия проконтролирует наличие соответствующего законодательства и стимулов для поддержки коммерческой деятельности и ее развития в данной

сфере. Основные ноу-хау в данной области поступают через коммерческую деятельность.

4. Стратегические руководящие принципы кибербезопасности

Национальная киберстратегия будет разработана в соответствии со стратегическими руководящими принципами. Они создают условия для реализации видения национальной кибербезопасности. В отдельно подготовленном плане действий будут описывать меры, которые обеспечивают осуществление целей национальной кибербезопасности. Программа реализации будет включать в себя планы различных субъектов и административных учреждений, а также межотраслевые мероприятия, вытекающие из планов.

Осуществление стратегических руководящих принципов укрепит государственно-частное сотрудничество, что рассматривается в качестве сильной стороны сообщества по вопросам безопасности Финляндии. Такое сотрудничество может наилучшим образом послужить обществу и поддержать субъектов, обеспечивающих его жизненно важные функции. Задача заключается в том, чтобы поддерживать бесперебойный и безопасный поток различных функций в повседневной жизни и во время нарушений.

Кибербезопасность строится на развитии достаточного потенциала в долгосрочной перспективе, его своевременного и гибкого использования, а также устойчивости жизненно важных функций общества к нарушениям кибербезопасности. Компетентные министерства будут развивать возможности кибербезопасности органов власти в рамках своих соответствующих административных направлений, как, например, путем определения стратегических задач министерств в сфере кибербезопасности. Большая часть обязанностей по кибербезопасности и развитие соответствующего потенциала также требуют действий и ресурсов других министерств, региональных и местных органов власти, а также предпринимательского сообщества и организаций. Министерства всегда должны учитывать разные уровни административного управления, а также роль предпринимательского сообщества и организаций применительно к развитию и использованию функциональных возможностей. Создаваемый Комитет по безопасности будет играть активную роль в сфере комплексной безопасности, и будет действовать в качестве постоянного органа сотрудничества для планирования действий в чрезвычайных ситуациях. Будут выпущены отдельные положения в отношении задач Комитета по безопасности.

СТРАТЕГИЧЕСКИЕ РУКОВОДЯЩИЕ ПРИНЦИПЫ

Создать эффективную модель сотрудничества между органами власти и другими субъектами с целью продвижения национальной кибербезопасности и киберзащиты.

Стратегические руководящие принципы Стратегии кибербезопасности реализуются путем усиления активного сотрудничества между субъектами, цель которого заключается в достижении общей осведомленности о ситуации и эффективной защите от угроз. Готовность различных секторов к защите жизненно важных функций в нарушенных условиях будет совершенствоваться путем организации регулярных учений. Каждый субъект будет развивать свое национальное и международное участие в учениях. Субъекты будут совершенствовать использование передовой практики и уроков, извлеченных из международных учений, путем совершенствования обмена информацией и взаимной координации. Цель учений заключается в улучшении возможностей участников по выявлению уязвимостей собственных действий и систем, развитии функциональных возможностей и обучении своего персонала. Киберзащита будет реализовываться путем стимулирования обмена информацией и нормативными актами, а также посредством сотрудничества между органами власти и предпринимательским сообществом.

Повысить знание ситуации относительно комплексной кибербезопасности среди ключевых субъектов, участвующих в защите жизненно важных функций общества.

Цель заключается в том, чтобы повысить ситуационную осведомленность различных субъектов, предоставляя им информацию в реальном времени для совместного доступа, и проанализированную информацию относительно уязвимостей, нарушений и их последствий. Отображение ситуации будет включать в себя оценки угроз, возникающих в кибернетическом мире. Прогнозирование киберугроз требует анализа политической, военной, социальной, культурной, технической и технологической, а также экономической ситуации. В составе Администрации по регулированию связи Финляндии (FICORA) будет создан Центр кибербезопасности для подготовки и отображения совокупной картины ситуации в сфере кибербезопасности.

Центр кибербезопасности будет собирать информацию о киберпроисшествиях и распространять ее среди различных субъектов. Субъекты будут в последующем оценивать последствия нарушения для деятельности, за которую они отвечают. Их анализы будут направляться обратно в Центр кибербезопасности для включения в совокупную картину

ситуации в сфере кибербезопасности. Совокупная картина ситуации будет тиражироваться среди различных субъектов в порядке поддержки для принятия решений.

Центр ситуаций Правительства должен иметь надежную, комплексную и подготовленную в реальном времени полную оценку ситуации с кибербезопасностью в его распоряжении. Оценка охватывает совокупную картину ситуации, подготовленную Центром кибербезопасности, а также оценки последствий киберпроисшествий для жизненно важных функций общества, подготовленные административными органами. Руководство государства обладает доступом к общей оценке ситуации, а также к оценке событий в оперативной обстановке.

Поддерживать и развивать функциональные возможности предприятий и организаций, критичных для жизненно важных функций общества, в плане выявления и отражения киберугроз и устранения нарушений, которые негативно влияют на какую-либо жизненно важную функцию и способности восстановления, в качестве элемента обеспечения непрерывности управления для предпринимательского сообщества.

Предприятия и организации, которые являются критичными для жизненно важных функций общества, будут учитывать в комплексе факторы киберугроз, относящиеся к жизненно важным функциям, а также поддерживать требуемые функциональные возможности киберзащиты в своих планах безопасности и действий в чрезвычайных ситуациях, а также в соответствующих структурах обслуживания. Цель заключается в том, чтобы выявить и определить все нарушения жизненно важных функций, появляющиеся в оценках риска, и реагировать на них в таком порядке, при котором их вредные последствия будут сведены к минимуму. Ключевые субъекты будут развивать свою устойчивости, в том числе планирование действий в чрезвычайных ситуациях и учения, с тем чтобы иметь возможность функционировать под воздействием кибератак. Безопасность снабжения – организация будет поддерживать свою деятельность с помощью отчетов, инструкций и обучения.

Убедиться, что полиция обладает достаточными функциональными возможностями для предотвращения, выявления и раскрытия киберпреступлений.

Полиция является компетентным органом для проведения расследований, связанных с киберпреступностью. Полиция будет готовить проанализированную и отличающуюся высоким качеством картинуситуации с киберпреступностью и распространять ее в качестве части общей картины ситуации, описанной в руководящем принципе 2.

Полиция будет тесно сотрудничать с Центром кибербезопасности. Необходимо обеспечить, чтобы полиция располагала достаточными полномочиями, ресурсами и мотивированным персоналом для профилактики киберпреступлений, тактических полицейских расследований, а также для обработки и анализа цифровых доказательств. Международное оперативное сотрудничество и обмен информацией будут продолжаться и развиваться совместно с соответствующими правоохранительными органами ЕС и других стран, такими как Европол.

Вооруженные силы Финляндии будут создавать комплексный потенциал киберзащиты для выполнения своих задач, установленных законодательными актами.

Военный потенциал киберзащиты охватывает разведку, а также функциональные возможности кибератак и киберзащиты. Вооруженные силы будут защищать свои системы в таком порядке, чтобы они могли выполнять свои задачи, предусмотренные законодательными актами, независимо от угроз в киберпространстве. Гарантирующие функциональные возможности, разведывательные и активные меры в киберпространстве будут развиваться в качестве элементов прочей военной силы. Требуемые положения о полномочиях будут подготовлены для Вооруженных сил под руководством Министерства обороны в порядке содействия реализации вышеупомянутых задач. Все выявленные недостатки в положениях будут скорректированы законодательным путем. Киберзащита будет осуществляться и развиваться совместно с ключевыми органами власти, организациями и субъектами предпринимательского сообщества как в национальном, так и в международном масштабе. Вооруженные силы будут оказывать исполнительное содействие в рамках законодательства.

Укрепление национальной кибербезопасности путем активного и эффективного участия в деятельности международных организаций и форумов сотрудничества, которые являются критичными для кибербезопасности.

Цель международного сотрудничества заключается в обмене информацией и извлеченными уроками, а также в освоении передовой практики для повышения качества национальной кибербезопасности. Реализация готовности и других мер кибербезопасности не достигнет цели в отсутствие эффективного и системно координируемого международного сотрудничества. Все органы власти будут вести сотрудничество в рамках своей сферы компетенции, в частности, с теми государствами и организациями, которые являются общемировыми лидерами в сфере кибербезопасности. Активное сотрудничество будет

осуществляться посредством НИОКР, предварительно согласованных консультаций и совместных действий организаций, а также путем участия в международных учениях.

Европейский союз, а также многие международные организации, такие как ООН, ОБСЕ, НАТО и ОЭСР являются важными местами деятельности для Финляндии в плане развития кибербезопасности. ЕС проявляет растущую активность в сфере кибербезопасности, а также активно сотрудничает с третьими странами. Финляндия принимает активное участие в таком развитии.

Увеличить экспертное понимание кибербезопасности и повысить осведомленность всех субъектов общества.

Будут приняты меры подготовки, использования и обучения в отношении инструкций по кибербезопасности и информационной безопасности в порядке поддержки непрерывного развития компетентности и осведомленности субъектов общества. Мероприятия будут также охватывать коммерческие предприятия и негосударственные организации (НГО), критичные для жизненно важных функций общества, с целью развития комплексной подготовленности общества.

Стратегический головной центр кибербезопасности будет создан в рамках существующего Финского стратегического центра науки, технологии и инноваций (*ICT-SHOK*) (компания *TIVIT*) . Он предоставит возможность участия в эффективном взаимном долгосрочном сотрудничестве для ведущих исследовательских групп и компаний, использующих полученные результаты. Головной центр будет способствовать условиям создания надежного национального кластера кибербезопасности. Увеличатся средства, вкладываемые в НИОКР и образование, а также в мероприятия по улучшению ноу-хау в сфере безопасности в обществе в целом.

Обеспечить предпосылки для реализации эффективных мер киберзащиты через национальное законодательство.

Административные органы и предпринимательское сообщество осуществят совместную работу по подготовке законодательных актов, включая необходимость пересмотра положений, относящихся к киберпространству и кибербезопасности. Результат данной работы будет включать в себя предложения по пересмотру законодательных актов, что будет способствовать достижению целей Стратегии кибербезопасности.

При составлении предложений будут учитываться быстро меняющиеся явления в киберпространстве. Одна из целей заключается в том, чтобы обеспечить компетентные органы и другие субъекты

достаточными силами и полномочиями посредством законодательства для реализации киберзащиты функций, жизненно важных для общества и в особенности для безопасности государства. Будут проанализированы все возможные законодательные препоны, ограничения и обязательства, относящиеся к защите данных, а также те из них, которые вытекают из международных обязательств, препятствующие получению, раскрытию и обмену информацией, полезной для целей киберзащиты. Если речь будет идти об оценке сбора информации и другой обработке данных, следует также оценить, должны ли компетентные органы обладать улучшенными возможностями для сбора информации, обработки данных или информирования о киберугрозах и их источниках, одновременно уделяя внимание обеспечению базовых прав неприкосновенности частной жизни и конфиденциальности электронных коммуникаций.

Основная часть критичной инфраструктуры общества принадлежит частным организациям. Ноу-хау и экспертный опыт, а также услуги и защита киберпространства в основном обеспечиваются компаниями. Национальное законодательство в сфере кибербезопасности должно обеспечивать благоприятную среду для развития коммерческой деятельности. Со своей стороны это позволит создать кластер кибербезопасности, имеющий международное признание, конкурентоспособность и экспортный потенциал. Финляндия в то же время станет привлекательной и кибернетически защищенной средой, достойной производственных капиталовложений и коммерческой деятельности.

Определение задач, связанных с кибербезопасностью, моделей обслуживания и общих стандартов управления кибербезопасностью для органов власти и субъектов делового сообщества.

Развитие кибербезопасности требует четкого распределения обязанностей и задач в соответствии со стратегическими руководящими принципами. На практике это предполагает, что каждое административное учреждение проводит собственную оценку риска и анализ зрелости, которые помогут выявить все значимые уязвимости и риски с точки зрения кибербезопасности, а также уровень управления таковыми. Результаты будут использоваться при подготовке планов действий для каждого административного сектора и для поддержки составления планов действий делового сообщества наряду с безопасностью организации снабжения.

Реализация Стратегии и ее выполнение будут контролироваться.

Министерства и ведомства отвечают за реализацию Стратегии в рамках своих соответствующих административных полномочий,

выполняя задачи, связанные с кибербезопасностью, реализуя и обеспечивая безопасность. Будущий Комитет по безопасности будет контролировать и координировать реализацию Стратегии. Цели координации в сфере кибербезопасности заключаются в том, чтобы избежать ненужного дублирования, выявить возможные недостатки и определить компетентные органы. Компетентные органы будут принимать фактические решения с учетом предусмотренных мер. Государственная дирекция по информационной безопасности (*VAHTI*) будет разрабатывать и координировать выполнение ключевых принципов информационной безопасности и кибербезопасности центрального правительства. Министерства, ведомства и учреждения должны включить ресурсы для реализации Стратегии кибербезопасности в свои рабочие планы и планы финансирования.

Приложение 1

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
Информационная инфраструктура	«Информационная инфраструктура» означает структуры и функции в основе информационных систем, которые осуществляют электронную пересылку, передачу, получение, хранение или иную обработку информации (данных).
Критичная информационная инфраструктура	«Критичная информационная инфраструктура» относится к структурам и функциям в основе информационных систем жизненно важных функций общества, которые осуществляют электронную пересылку, передачу, получение, хранение или иную обработку информации (данных).
Критичная инфраструктура	«Критичная инфраструктура» относится к структурам и функциям, которые являются неотъемлемой частью жизненно важных функций общества. Они включают в себя физические средства и структуры, а также электронные функции и услуги.

Термин	Определение
Кибер	Слово «кибер» практически всегда является приставкой для термина или модификатором для сложного слова, а не самостоятельным словом. Обычно подразумевается, что оно относится к обработке электронной информации (данных), информационной технологии, электронной связи (передаче данных) или информации и компьютерным системам. Только полный термин сложного слова (модификатор + основная часть) можно считать имеющим фактическое знание. В целом считается, что слово «кибер» происходит от древнегреческого глагола *κυβερεω* («киберео»), что означает «направлять, управлять, контролировать».
Киберриск	«Киберриск» означает возможность происшествия или уязвимость в киберпространстве, которая при возникновении или использовании может повредить, причинить вред или нарушить операцию, которая зависит от функционирования киберпространства.
Киберпространство, киберсреда	«Киберпространство» означает область обработки электронной информации (данных), включающую в себя одну или несколько инфраструктур электронных технологий. *Примечание 1* Среда представляет собой использование электроники и электромагнитного спектра с целью хранения, обработки и передачи данных и информации по сетям передачи данных. *Примечание 2* «Обработка информации (данных)» означает сбор, запись, организацию, использование, передачу, раскрытие, хранение, изменение, комбинирование, защиту, удаление, уничтожение и другие аналогичные действия с информацией (данными).

Термин	Определение
Кибербезопасность	«Кибербезопасность» означает желательное конечное состояние, в котором киберпространство является надежным и в котором обеспечивается ее функционирование. *Примечание 1* В желательном конечном состоянии киберпространство не будет негативно влиять, причинять вред или нарушать работу функций, зависящих от обработки электронной информации (данных). *Примечание 2* Надежность киберпространства зависит от его движущих сил, реализующих соответствующие и достаточные процедуры информационной безопасности («безопасность общих данных»). Указанные процедуры могут воспрепятствовать материализации киберугроз, и если таковые все же материализуются, то предотвратить, уменьшить или помочь выдержать их последствия. *Примечание 3* Кибербезопасность включает в себя мероприятия для функций, жизненно важных для общества и критичной инфраструктуры, нацеленные на достижение способности прогностического управления и при необходимости устойчивость к киберугрозам и их последствиям, которые могут причинить значительный вред или угрожать Финляндии или ее населению.
Киберугроза	«Киберугроза» означает вероятность действия или происшествия в киберпространстве, которое в случае ее материализации негативно повлияет на какую-либо операцию, зависящую от информационного мира. *Примечание* Киберугрозы представляют собой угрозы для информации, которые в случае

Термин	Определение
	материализации негативно сказываются на надлежащем или предполагаемом функционировании информационной системы.
Информационная система	«Информационная система» означает систему, включающую в себя персонал, оборудование для обработки информации, оборудование для передачи данных и компьютерные программы, предназначенные для того, чтобы сделать определенную операцию более эффективной, простой, или даже возможной путем обработки информации (данных).
Сохранение тайны	«Сохранение тайны» означает защиту от незаконного или вредоносного вторжения в неприкосновенность частной жизни. Сохранение тайны включает в себя право на неприкосновенность частной жизни и все соответствующие права в отношении обработки персональных данных. «Персональные данные» означают любую информацию о частном лице и любую информацию о его (ее) личных характеристиках или личных обстоятельствах, которые являются идентифицируемыми в отношении его (ее), членов его (ее) семьи или домохозяйства.
Безопасность информации (данных)	«Информационная безопасность» означает административные и технические меры, предпринимаемые для обеспечения наличия, целостности и конфиденциальности данных.
UTVA	Комитет по внешней политике и политике безопасности Кабинета.
VAHTI	Государственная дирекция по информационной безопасности.
YTS	Стратегия безопасности для общества, Постановление Правительства от 16 декабря 2010 года.

2.4. Индия

НАЦИОНАЛЬНАЯ ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ

(Дели, 2 июля 2013 г.)

Преамбула

1. Киберпространство является сложной средой, состоящей из взаимодействий между людьми, программным обеспечением и услугами, поддерживаемых распространением устройств и сетей информационно-коммуникационных технологий (ИКТ) в общемировом масштабе.

2. Благодаря многочисленным преимуществам, привнесенным технологическими усовершенствованиями, киберпространство в настоящее время является общим ресурсом, который используется гражданами, коммерческими предприятиями, критической информационной инфраструктурой, военными и правительствами таким образом, что проведение четких границ между столь разнообразными группами становится затруднительной задачей. Ожидается, что в обозримом будущем киберпространство станет более высокоорганизованным, а количество подключенных к нему сетей и устройств многократно возрастет.

3. Информационные технологии (ИТ) являются одной из важнейших отраслей экономики, которая зависит от киберпространства и находится в нем. Она возникла в качестве одного из самых значительных катализаторов роста индийской экономики. В дополнение к активизации экономики Индии, данная отрасль также оказывает положительное воздействие на жизнь ее населения, прямо и косвенно влияя на различные социально-экономические параметры, в числе которых находятся занятость, уровень жизни и разнообразие. Эта отрасль сыграла существенную роль в трансформации образа Индии в качестве глобального игрока, который предоставляет технологические решения и деловые ИТ-услуги мирового класса Правительство. стало ключевым драйвером роста проникновения ИТ-продукции и ИТ-услуг в органы государственного управления (государственные услуги для граждан, идентификация граждан, системы передачи данных общего пользования), здравоохранение (телемедицина, дистанционное консультирование, мобильные клиники), образование (электронное обучение, виртуальные классы и т.д.) и в финансовые услуги (мобильный банкинг / платежные шлюзы) и т.д. Такие инициативы позволили увеличить использование ИТ в стране посредством отраслевых реформ и национальных программ,

которые привели к созданию масштабной ИТ-инфраструктуры с корпоративным / частным участием.

4. В свете роста национальной ИТ-отрасли, амбициозных планов стремительной социальной трансформации и обеспечения сбалансированного роста, а также ощутимой роли Индии на глобальном ИТ-рынке, обеспечение правильного направления усилий на создание безопасной вычислительной среды, а также формирования соответствующего доверия и конфиденциальности электронных транзакций, программного обеспечения, услуг, устройств и сетей стало одним из крайне необходимых для страны приоритетов. Такое направление позволит создать подходящую экосистему кибербезопасности в стране, синхронизированную с глобальной сетевой средой.

5. Киберпространство является уязвимым для широкого спектра инцидентов, будь то предумышленных или случайных, техногенных или природных. Как национальные государства, так и негосударственные акторы могут использовать обмен данных в киберпространстве для преступных целей. Кибератаки, нацеленные на инфраструктуру или подрывающие экономическое благополучие национального государства, могут существенно сократить имеющиеся у государства ресурсы и подорвать доверие к структурам, которые поддерживают их. Связанный с киберпространством инцидент национального значения может принимать любую форму: организованная кибератака; неконтролируемое компьютерное вторжение посредством компьютерного вируса, вируса-червя или любого вредоносного программного кода; стихийное бедствие со значительными последствиями для киберпространства или другие соответствующие инциденты, способные нанести существенный ущерб информационной инфраструктуре или ключевым активам. Широкомасштабные компьютерные инциденты могут вывести из строя ресурсы и услуги государственного, общественного и частного секторов в результате нарушения функционирования критических информационных систем. Осложнения после разрушений такого масштаба могут угрожать жизням, экономике и национальной безопасности. Быстрое определение, обмен информацией, расследование и скоординированное реагирование и устранение последствий могут уменьшить ущерб, причиняемый вредоносной деятельностью в киберпространстве. Некоторыми примерами киберугроз для частных лиц, компаний и государства могут служить хищение персональных данных, фишинг, социальная инженерия, хакерская деятельность в политических целях (хактивизм), кибертерроризм, комплексные угрозы, нацеленные на мобильные устройства и смартфоны, ском-

прометированные цифровые сертификаты, целенаправленные постоянные угрозы, атаки типа отказ в обслуживании, ботнеты, атаки на цепочки поставок, утечка данных и т.д. Защита информационной инфраструктуры и обеспечение конфиденциальности, целостности и доступности информации является важным условием защищенного киберпространства.

6. Реализуются разнообразные мероприятия и программы правительства, которые нацелены на решение проблем кибербезопасности и которые внесли значительный вклад в создание платформы, способной в настоящее время поддерживать и подкреплять усилия по защите киберпространства. Вследствие того, что киберпространство имеет динамический характер, в настоящее время возникает необходимость объединить такие действия в рамках **Национальной политики кибербезопасности**, с комплексным видением и рядом устойчивых и согласованных стратегий для реализации.

7. Политика кибербезопасности является развивающейся задачей и учитывает потребности всего спектра пользователей и провайдеров ИКТ, в число которых входят домашние пользователи, малые, средние и крупные предприятия, государственные и негосударственные учреждения. Она служит общей рамочной основой для определения и руководства действиями, относящимися к безопасности киберпространства. Она также позволяет отдельным отраслям и организациям разрабатывать соответствующую их потребностям политику кибербезопасности. Политика дает общее представление о том, что следует делать для эффективной защиты информации, информационных систем и сетей, а также предоставляет информацию о подходе и стратегии правительства для защиты киберпространства на национальном уровне. Она также обозначает в общих чертах ориентиры, которые позволяют всем ключевым игрокам в государственном и частном секторах вести совместную работу для обеспечения защиты национальных информации и информационных систем. Таким образом, данная политика нацелена на создание рамочной основы кибербезопасности, которая предполагает конкретные действия и программы, нацеленные на повышение качества сил и средств обеспечения безопасности киберпространства страны.

I. Видение

Построение защищенного и устойчивого киберпространства для граждан, частного сектора и государства.

II. Миссия

Защищать информацию и информационную инфраструктуру в киберпространстве, наращивать потенциал для предотвращения киберугроз и реагирования на них, сокращать уязвимость и минимизировать ущерб от киберинцидентов посредством сочетания институциональных структур, людей, процессов, технологий и сотрудничества.

III. Цели

1) Создать защищенную экосистему киберпространства в стране, сформировать соответствующие доверие и конфиденциальность в ИТ-системах и электронных транзакциях в киберпространстве, тем самым расширяя проникновение ИТ во все отрасли экономики.

2) Создать гарантирующую рамочную основу для разработки политики безопасности, для реализации и обеспечения возможности осуществления действий по соблюдению общемировых стандартов безопасности и передовых практик путем оценки соответствия (продукции, процессов, технологии и людей).

3) Усилить нормативно-правовую базу для обеспечения защищенной экосистемы киберпространства.

4) Улучшить и сформировать национальные и отраслевые работающие в режиме 24/7 механизмы для получения стратегической информации в отношении угроз для ИКТ-инфраструктуры, разработки сценариев реагирования, разрешения и антикризисного управления посредством эффективных прогностических, профилактических, защитных действий, действий по реагированию и восстановлению после инцидентов.

5) Усилить защиту и устойчивость критической информационной инфраструктуры государства путем управления в режиме 24/7 Национальным центром защиты критической информационной инфраструктуры (НЦЗКИИ) и принятия практических мер безопасности, относящихся к проектированию, приобретению, развитию, использованию и технической эксплуатации информационных ресурсов.

6) Разработать соответствующие отечественные технологии обеспечения безопасности посредством проведения передовых технологических исследований, направленных на нахождение решений исследований, подтверждения концепции, пилотного внедрения, переходного процесса, распространения и коммерциализации, которые ведут к широкомасштабному проникновению защищенной продукции / процессов ИКТ в целом с учетом требований национальной безопасности.

7) Улучшить видимость целостности продуктов и услуг ИКТ через создание инфраструктуры для тестирования и подтверждения их безопасности.

8) В течение следующих пяти лет подготовить 500 специалистов, обладающих компетенциями в сфере обеспечения кибербезопасности посредством наращивания потенциала, развития навыков и обучения.

9) Предоставить налоговые льготы предприятиям для внедрения общепринятых практик и процессов обеспечения безопасности.

10) Ввести в действие защиту информации во время подготовки, обработки, хранения и передачи для обеспечения конфиденциальности данных граждан и для уменьшения экономических потерь по причине киберпреступлений или кражи данных.

11) Способствовать эффективному предотвращению, расследованию и преследованию киберпреступности и повысить правоохранительный потенциал с помощью соответствующей нормотворческой деятельности.

12) Сформировать культуру кибербезопасности и неприкосновенности личной жизни, которая обеспечит ответственное поведение и действия пользователей посредством эффективной стратегии коммуникации и продвижения.

13) Развивать эффективные государственно-частные партнерства и взаимодействия посредством технического и оперативного сотрудничества и вклада в повышение безопасности киберпространства.

14) Усиливать глобальное сотрудничество, способствуя общему пониманию и развивая отношения, способствующие обеспечению безопасности в киберпространстве.

IV. Стратегии

A. Создание безопасной экосистемы киберпространства

1) Определить правительственное учреждение, которое будет отвечать за координацию связанных с кибербезопасностью вопросов на национальном уровне, с четко определенными ролями и обязанностями.

2) Способствовать тому, чтобы все организации, как частные, так и государственные, назначали члена высшего руководящего состава, который будет отвечать за действия и инициативы в сфере кибербезопасности, например, в качестве главного директора по информационной безопасности.

3) Стимулировать все организации к разработке политики информационной безопасности, интегрированной с их бизнес-планами,

а также реализовывать такую политику в соответствии с передовыми международными практиками. Такая политика должна включать в себя создание стандартов и механизмов для защищенного информационного потока (во время обработки, сортировки, хранения и передачи), план кризисного управления, оценки активных сил и средств обеспечения безопасности, а также информационную инфраструктуру с экспертным опытом.

4) Принять необходимые меры для того, чтобы все организации предусмотрели в своих бюджетах средства на реализацию инициатив в сфере кибербезопасности, а также на осуществление действий в чрезвычайных ситуациях вследствие киберинцидентов.

5) Предусмотреть налоговые схемы и стимулы для поощрения организаций к формированию, укреплению и обновлению информационной инфраструктуры с учетом требований кибербезопасности.

6) Предотвращать проявление и повторное появление киберинцидентов посредством стимулирования разработки технологий, соблюдения норм кибербезопасности и проактивных действий.

7) Создавать механизмы обмена информацией, обнаружения и реагирования на инциденты в сфере кибербезопасности, а также сотрудничества по восстановлению последствий инцидентов.

8) Поддерживать организации в принятии основополагающих принципов для закупки проверенной ИКТ-продукции, а также обеспечивать закупку ИКТ-продукции, чувствительной с точки зрения безопасности, у отечественных производителей.

***B*. Создание гарантирующей рамочной основы**

1) Способствовать принятию передовых международных практик в области информационной безопасности и обеспечения соблюдения норм, усиливая тем самым силы и средства кибербезопасности.

2) Обеспечивать инфраструктуру для подтверждения соответствия и сертификации соответствия передовым практикам, стандартам и основополагающим принципам кибербезопасности (например, сертификация по ISO 27001 ISMS, аудит системы информационной безопасности, проверка на проникновение / оценка уязвимости, проверка безопасности приложений, проверка безопасности интернета).

3) Предоставить для всех государственных организаций и компаний в критических отраслях возможность использования передовых общемировых практик обеспечения безопасности в процессах формальной оценки рисков и управления рисками, управления непрерывностью деятельности и планирования кризисного управления

во время киберинцидентов с целью сокращения рисков нарушений и улучшения сил и средств обеспечения безопасности.

4) Определить и классифицировать средства и активы информационной инфраструктуры на уровне организации с учетом восприятия рисков для принятия соответствующих защитных мер безопасности.

5) Стимулировать разработку защищенных приложений / программного обеспечения с учетом передовых общемировых практик.

6) Создать рамочную основу проверки соответствия для периодической верификации соблюдения передовых практик, стандартов и основополагающих принципов кибербезопасности.

7) Содействовать тому, чтобы все организации периодически проверяли и оценивали достаточность и эффективность мер технического и операционного контроля безопасности, реализованных в ИТ-системах и сетях.

***C.* Поддержка использования открытых стандартов**

1) Стимулировать использование открытых стандартов для обеспечения совместимости, а также обмен данными между различными продуктами или услугами.

2) Способствовать объединению государственного и частного сектора для расширения предложения проверенных и сертифицированных ИТ-продуктов, основанных на открытых стандартах.

***D.* Укрепление нормативно-правовой базы**

1) Разработать динамичную нормативно-правовую базу и периодически пересматривать ее для учета вызовов кибербезопасности, возникающих вследствие технологических разработок в киберпространстве (таких как облачные вычисления, мобильные вычисления, зашифрованные службы и социальные сети), и ее гармонизацию с международными нормами, в том числе относящимися к управлению интернетом.

2) С учетом нормативно-правовой базы проводить периодический аудит и оценку достаточности и эффективности обеспечения безопасности информационной инфраструктуры в соответствующих случаях.

3) Обеспечить условия, просвещать и способствовать осведомленности о нормативно-правовой базе.

***E.* Создание механизмов раннего оповещения об угрозах для безопасности, управления уязвимостями и реагирования на угрозы безопасности**

1) Создать на национальном уровне системы, процессы, структуры и механизмы для выработки требуемых ситуационных сценариев су-

ществующих и потенциальных угроз кибербезопасности, позволяющие проводить своевременный обмен информацией для проактивных, превентивных и защитных мер отдельных субъектов.

2) Управлять работающей в режиме 24/7 национальной Компьютерной группы реагирования на чрезвычайные ситуации (*CERT*-Индия), которая выступает в качестве координатора всех мер реагирования на чрезвычайные ситуации и антикризисного управления в сфере кибербезопасности. Группа *CERT*-Индия будет действовать в качестве зонтичной организации, в которой могут быть созданы и задействованы отраслевые группы *CERT*, а также способствовать осуществлению коммуникаций и координации действий при разрешении кризисных ситуаций в киберпространстве.

3) Ввести в действие функционирующие в режиме 24/7 отраслевые группы *CERT* для осуществления коммуникаций и координации действий в соответствующих отраслях с целью эффективного реагирования, разрешения инцидентов и управления кризисными ситуациями в киберпространстве.

4) Реализовать План управления кризисной ситуацией в киберпространстве для действия в случае киберинцидентов, влияющих на критические национальные процессы или угрожающие безопасности населения и безопасности государства, путем хорошо согласованного комплексного подхода на уровне государства, отраслей и организаций.

5) Проводить и содействовать проведению регулярных учений и тренировок по вопросам кибербезопасности на национальном, отраслевом и организационном уровне для обеспечения возможности оценки сил и средств обеспечения безопасности и степени готовности к чрезвычайным ситуациям для сопротивления и разрешения инцидентов в сфере кибербезопасности.

***F.* Обеспечение безопасности услуг электронного управления**

1) Предусмотреть внедрение передовых общемировых практик обеспечения безопасности, управление непрерывностью деятельности и план управления в ситуациях киберинцидентов для всех инициатив электронного управления в стране, уменьшить риск нарушения и улучшить силы и средства обеспечения безопасности.

2) Содействовать более активному использованию инфраструктуры открытого ключа (ИОК) в правительственных учреждениях для обеспечения защищенной связи и операций.

3) Привлечь профессиональных специалистов / организации в сфере информационной безопасности для содействия инициативам элек-

тронного управления и обеспечения соответствия передовым практикам обеспечения безопасности.

***G.* Защита и устойчивость критической информационной инфраструктуры**

1) Разработать план обеспечения защиты критической информационной инфраструктуры и его интеграции с бизнес-планом на уровне организации, а также реализовать такой план. Такие планы должны включать в себя создание механизмов для обеспечения защиты информационного потока (во время обработки, сортировки, хранения и передачи), основополагающих принципов и стандартов, плана кризисного управления, оценки активных сил и средств обеспечения безопасности и информационной инфраструктуры с экспертным опытом.

2) Управлять работой Национальным центром защиты критической информационной инфраструктуры (НЦЗКИИ), действующим в качестве ключевой организации по защите критической информационной инфраструктуры в стране.

3) Содействовать определению, расстановке приоритетов, оценке и защите критической инфраструктуры и ключевых ресурсов, основанных на плане для защиты критической информационной инфраструктуры.

4) Предусмотреть внедрение всеми организациями критических отраслей передовых общемировых практик обеспечения безопасности, управления непрерывностью деятельности и плана кризисного управления при киберинцидентах для сокращения рисков и улучшения сил и средств обеспечения безопасности.

5) Способствовать и предписывать в случае необходимости использование проверенной и сертифицированной ИТ-продукции.

6) Предусматривать периодический аудит критической информационной инфраструктуры.

7) Обеспечить сертификацию всех должностей по обеспечению безопасности от уровня Главного директора по информационной безопасности/Главного директора по безопасности до лиц, занимающихся эксплуатацией критической информационной инфраструктуры.

8) Предусмотреть процессы разработки защищенных приложений / программного обеспечения (от проектирования до вывода из эксплуатации) с учетом передовых общемировых практик.

***H.* Содействие НИОКР в сфере кибербезопасности**

1) Осуществить программы НИОКР для рассмотрения всех аспектов развития, нацеленного на краткосрочные, среднесрочные и дол-

госрочные цели. Программы НИОКР должны учитывать все аспекты, в том числе разработку защищенных систем, их тестирование, развертывание и техническое обслуживание в течение всего срока эксплуатации, включая НИОКР по передовым технологиям безопасности.

2) Поощрять НИОКР для выработки экономичных, индивидуализированных отечественных решений для обеспечения безопасности, соответствующих более широкому спектру вызовов кибербезопасности и нацеленных на экспортные рынки.

3) Способствовать переходу, распространению и коммерциализации результатов НИОКР в коммерческие продукты и услуги для использования в государственном и частном секторах.

4) Формировать Центры передового опыта по направлениям стратегической важности с точки зрения безопасности киберпространства.

5) Принимать участие в совместных проектах НИОКР с бизнесом и академическим сообществом по передовым технологиям и исследованиям, ориентированным на нахождение решения.

***I.* Сокращение рисков системы снабжения**

1) Создавать и поддерживать инфраструктуру и средства проведения испытаний для осуществления оценки уровня ИТ-безопасности продукта и проверки соответствия общемировым стандартам и практикам.

2) Выстраивать доверительные отношения с поставщиками продукции / систем и провайдерами услуг для улучшения комплексной безопасности системы снабжения.

3) Обеспечивать осведомленность об угрозах, уязвимостях и последствиях нарушений безопасности среди организаций для управления рисками системы снабжения, связанными с закупкой ИТ (продукции, систем или услуг).

***J.* Развитие кадрового потенциала**

1) Содействовать развитию программ обучения и тренингов в формальных или неформальных отраслях для обеспечения потребностей государства в кибербезопасности и для наращивания потенциала.

2) Создать образовательную инфраструктуру обеспечения кибербезопасности в масштабах страны посредством достижения государственно-частных договоренностей о партнерстве.

3) Сформировать концептуальные лаборатории кибербезопасности для обеспечения информированности и развития компетенций по ключевым направлениям.

4) Создать институциональные механизмы по наращиванию потенциала для правоохранительных органов.

***K.* Обеспечение информированности о кибербезопасности**

1) Разработать и ввести в действие комплексную национальную программу обеспечения информированности о безопасности киберпространства.

2) Обеспечивать информационную компанию для расширения грамотности в сфере безопасности через электронные средства массовой информации для того, чтобы помочь гражданам получить знания о вызовах кибербезопасности.

3) Проводить, поддерживать и предусматривать тренинги / семинары и сертификацию по кибербезопасности.

***L.* Создание эффективных государственно-частных партнерств**

1) Способствовать сотрудничеству и координации между заинтересованными сторонами, включая частный сектор, в сфере кибербезопасности в целом и обеспечения защиты критической информационной инфраструктуры в частности, в том числе в отношении мер, связанных с киберугрозами, уязвимостями, нарушениями, потенциальными мерами защиты и освоением передовых практик.

2) Создавать модели сотрудничества и участия со всеми соответствующими заинтересованными сторонами.

3) Создать научно-исследовательский центр для получения информации, обсуждения и совещаний по политике кибербезопасности.

***M.* Обмен информацией и сотрудничество**

1) Развитие двусторонних и многосторонних отношений с другими странами в сфере кибербезопасности.

2) Укреплять национальное и глобальное сотрудничество между органами безопасности, группами CERT, военными ведомствами и силами, правоохранительными органами и судебными системами.

3) Формировать механизмы для осуществления диалога по техническим и операционным аспектам с бизнесом для содействия работам по восстановлению и устойчивости систем, включая критическую информационную инфраструктуру.

***N.* Подход к реализации с учетом приоритетов**

Принять подход к осуществлению данной политики с учетом приоритетов для того, чтобы сначала охватить наиболее критические направления.

V. Ввод в действие политики

Данная политика должна быть введена в действие с помощью детализированных основополагающих принципов и планов действий на различных уровнях (национальный, отраслевой, уровень штата, министерства, департамента и предприятия) для того, чтобы учесть проблемные требования к безопасности киберпространства.

Дж. Сатьянарайяна
Секретарь, Департамент электроники и информационных технологий

Дели, 2 июля 2013 г.

Копия:

1. Всем соответствующим министерства и департаментам Правительства Индии.
2. Секретариату Кабинета министров.
3. Управлению руководства программами.
4. Комиссии по планированию.
5. Главному финансовому инспектору и аудитору Индии.
6. Совместному секретарю и Финансовому директору. Департаменту электроники и информационных технологий.
7. Внутренняя рассылка.

Дж. Сатьянарайяна
2 июля 2013 г.

Предмет: Уведомление о Национальной политике кибербезопасности 2013 г. (НПКБ-2013)

3. Международное сотрудничество государств

СОГЛАШЕНИЕ МЕЖДУ ПРАВИТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ И ПРАВИТЕЛЬСТВОМ ФЕДЕРАТИВНОЙ РЕСПУБЛИКИ БРАЗИЛИИ О СОТРУДНИЧЕСТВЕ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ И КОММУНИКАЦИОННОЙ БЕЗОПАСНОСТИ

(Москва, 14 мая 2010 г.)

Правительство Российской Федерации и Правительство Федеративной Республики Бразилии, далее именуемые Сторонами,

учитывая развитие отношений между Российской Федерацией и Федеративной Республикой Бразилией на основе взаимного доверия и сотрудничества,

отмечая, что в развитии и внедрении новейших информационно-коммуникационных технологий и средств коммуникаций достигнут значительный прогресс,

выражая озабоченность угрозами, связанными с возможностями использования таких технологий и средств как в гражданской, так и в военной сферах в целях, не совместимых с задачами поддержания международного мира, безопасности и стабильности,

придавая важное значение международной информационной и коммуникационной безопасности как одному из ключевых элементов системы международной безопасности,

принимая во внимание важную роль информационной и коммуникационной безопасности в обеспечении прав и основных свобод человека и гражданина,

учитывая Резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»,

стремясь противостоять угрозам международной информационной и коммуникационной безопасности, обеспечить интересы информационной и коммуникационной безопасности Сторон и способство-

вать созданию международной информационной среды, для которой характерны мир, сотрудничество и гармония,

желая создать правовые и организационные основы сотрудничества Сторон в области обеспечения международной информационной и коммуникационной безопасности и подчеркивая важность такого сотрудничества для дальнейшего развития двустороннего стратегического партнерства,

согласились о нижеследующем:

Статья 1
Терминология

1. Для целей взаимодействия Сторон в ходе выполнения настоящего Соглашения используются основные понятия, Перечень которых приведен в Приложении, являющемся неотъемлемой частью настоящего Соглашения.

2. Приложение может по мере необходимости дополняться, уточняться и обновляться по согласованию Сторон по дипломатическим каналам.

Статья 2
Основные угрозы в области обеспечения международной информационной и коммуникационной безопасности

Реализуя сотрудничество в соответствии с настоящим Соглашением, Стороны исходят из наличия следующих основных угроз в области обеспечения международной информационной и коммуникационной безопасности:

1) использование информационных и коммуникационных средств и технологий в международных конфликтах во враждебных целях как в гражданской, так и в военной сферах, включая выведение из строя критически важных инфраструктур;

2) использование информационных и коммуникационных средств и технологий для осуществления террористической деятельности и в террористических целях;

3) использование информационных и коммуникационных средств и технологий для осуществления преступной деятельности и в преступных целях;

4) использование доминирующего положения в сфере информационных и коммуникационных средств и технологий в ущерб интересам и безопасности других государств;

5) стихийные бедствия и технологические аварии, влияющие на безопасное и стабильное функционирование глобальных и национальных информационных и коммуникационных инфраструктур.

Статья 3
Основные направления сотрудничества

В соответствии с настоящим Соглашением, Стороны осуществляют сотрудничество по следующим основным направлениям:

1) определение, согласование и осуществление необходимых совместных мер в области обеспечения международной информационной и коммуникационной безопасности;

2) создание совместной структуры предупреждения, обнаружения, устранения и реагирования на угрозы, указанные в статье 2 настоящего Соглашения;

3) проведение экспертиз, исследований и оценок в области обеспечения информационной и коммуникационной безопасности, включая техническое и научное сотрудничество между Сторонами;

4) развитие взаимодействия в рамках форумов по управлению Интернетом по вопросам, связанным с информационной и коммуникационной безопасностью;

5) обеспечение информационной и коммуникационной безопасности национальных критически важных инфраструктур;

6) разработка и осуществление согласованной политики по вопросу использования электронной цифровой подписи и защиты информации в ходе международного информационного обмена;

7) обмен информацией о законодательстве Российской Федерации и законодательстве Федеративной Республики Бразилии по вопросам, связанным с обеспечением информационной и коммуникационной безопасности;

8) развитие и совершенствование международно-правовой базы и практических механизмов сотрудничества Сторон в укреплении международной информационной и коммуникационной безопасности;

9) взаимодействие в рамках международных организаций и форумов по проблемам обеспечения международной информационной и коммуникационной безопасности;

10) обмен опытом, подготовка специалистов, проведение рабочих встреч, конференций, семинаров и других, форумов уполномоченных представителей и экспертов Сторон в области информационной и коммуникационной безопасности.

Стороны могут по взаимной договоренности определять другие направления сотрудничества.

Статья 4
Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество в рамках настоящего Соглашения таким образом, чтобы эта деятельность способствовала социальному и экономическому развитию и поддержанию международного мира и безопасности, соответствовала общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека.

2. Каждая Сторона имеет равные права на защиту информационных ресурсов и критически важных инфраструктур своего государства от угроз, указанных в статье 2 настоящего Соглашения.

Статья 5
Реализация

1. В течение шестидесяти дней с даты вступления настоящего Соглашения в силу Стороны обменяются данными о компетентных органах Российской Федерации и Федеративной Республики Бразилии, ответственных за реализацию настоящего Соглашения, и каналах прямого обмена информацией по конкретным направлениям сотрудничества.

2. В целях рассмотрения хода выполнения настоящего Соглашения, обмена информацией, анализа и совместной оценки возникающих угроз информационной и коммуникационной безопасности, а также определения, согласования и координации совместных мер реагирования, Стороны проводят на регулярной основе консультации своих уполномоченных представителей и компетентных органов Российской Федерации и Федеративной Республики Бразилии (далее – консультации).

3. Очередные консультации проводятся, как правило, два раза в год, в Российской Федерации и в Федеративной Республике Бразилии на основе ротации.

4. Любая из Сторон может предложить проведение дополнительных консультаций с указанием сроков, места проведения, а также повестки дня.

5. Практическое взаимодействие по конкретным направлениям сотрудничества, предусмотренным настоящим Соглашением, может осуществляться компетентными органами Российской Федерации и Федеративной Республики Бразилии, ответственными за его реализацию.

6. В целях регулирования сотрудничества по конкретным направлениям компетентные органы Российской Федерации и Федеративной Республики Бразилии могут заключать соответствующие дополнительные соглашения.

Статья 6
Защита информации

1. Настоящее Соглашение не налагает на Стороны обязательств по предоставлению информации в рамках сотрудничества в соответствии с настоящим Соглашением и не является основанием для передачи информации в рамках этого сотрудничества, если раскрытие такой информации может нанести ущерб национальным интересам.

2. Меры по защите секретной информации, передача которой в конкретных случаях может считаться необходимой для целей исполнения настоящего Соглашения, регулируются соответствующими договорами, подписанными Сторонами.

3. Информация, передаваемая или созданная в ходе сотрудничества в рамках настоящего Соглашения, не раскрывается и не передается без письменного согласия Стороны, являющейся источником такой информации.

Статья 7
Финансовые и другие ресурсы

1. Стороны самостоятельно несут расходы по участию их представителей и экспертов в мероприятиях, связанных с исполнением настоящего Соглашения.

2. Стороны могут согласовывать иной порядок финансирования в каждом отдельном случае в соответствии с законодательством Российской Федерации и законодательством Федеративной Республики Бразилии.

3. Все мероприятия в рамках настоящего Соглашения проводятся при наличии соответствующих финансовых, кадровых и других ресурсов каждой из Сторон.

Статья 8
Отношение к другим международным договорам и национальному законодательству

1. Настоящее Соглашение не затрагивает прав и обязательств Сторон по другим международным договорам, участниками которых являются их государства.

2. Вся деятельность в рамках настоящего Соглашения осуществляется в соответствии с национальным законодательством и нормативно-правовыми актами, действующими для каждой из Сторон.

Статья 9
Разрешение споров

Стороны решают спорные вопросы, которые могут возникнуть в связи с толкованием или применением положений настоящего Соглашения, путем переговоров и консультаций между компетентными органами и, в случае необходимости, по дипломатическим каналам.

Статья 10
Рабочие языки

Рабочими языками при осуществлении сотрудничества в рамках настоящего Соглашения являются русский, португальский и английский языки.

Статья 11
Вступление в силу, срок действия, прекращение действия и поправки

1. Настоящее Соглашение вступает в силу на тридцатый день с даты получения по дипломатическим каналам последнего письменного уведомления о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу.

2. Настоящее Соглашение заключается на неопределенный срок.

3. В настоящее Соглашение могут быть в любое время внесены изменения на основе письменного согласия обеих Сторон, которые будут оформлены по дипломатическим каналам. Вступление в силу изменений, внесенных в настоящее Соглашение, должно быть оформлено на основе такой же процедуры, как при вступлении в силу настоящего Соглашения.

4. Действие настоящего Соглашения может быть прекращено по истечении девяноста дней после получения в любое время одной из Сторон по дипломатическим каналам письменного уведомления другой Стороны о ее намерении прекратить действие Соглашения.

5. В случае прекращения действия настоящего Соглашения для Сторон остаются обязательными положения статьи 6 в отношении любой информации, полученной в соответствии с Соглашением. Прекращение действия настоящего Соглашения не должно препятствовать осуществлению совместной деятельности в рамках настоящего Соглашения, не завершенной к моменту прекращения его действия, если только это не происходит в результате договоренности обеих Сторон.

Совершено в г. Москве 14 мая 2010 г. в двух экземплярах, каждый на русском, португальском и английском языках, причем все тексты имеют одинаковую силу. В случае разногласий в толковании положений настоящего Соглашения предпочтение отдается тексту на английском языке.

(Подписи)

Приложение
к Соглашению между
Правительством Российской Федерации
и Правительством Федеративной Республики Бразилии
о сотрудничестве в области обеспечения международной
информационной и коммуникационной безопасности

ПЕРЕЧЕНЬ ОСНОВНЫХ ПОНЯТИЙ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ И КОММУНИКАЦИОННОЙ БЕЗОПАСНОСТИ

1. Информационная и коммуникационная безопасность – состояние защищенности личности, общества, государства и их интересов от существующих и потенциальных угроз в сфере информационных и коммуникационных средств и технологий, включая меры, направленные на обеспечение доступности, целостности, конфиденциальности и подлинности информации.

2. Угроза информационной и коммуникационной безопасности – факторы, создающие опасность для личности, общества, государства и их интересов в сфере информационных и коммуникационных средств и технологий.

3. Информационная и коммуникационная инфраструктура – совокупность технических средств, систем, объектов и персонала, вовлеченных в формирование, создание, преобразование, передачу, использование и хранение информации.

4. Информационные ресурсы – информационная инфраструктура, а также собственно информация и ее потоки.

5. Критически важные инфраструктуры – объекты, системы, службы и институты, разрушение или выведение из строя которых может нанести серьезный ущерб социальному, экономическому или политическому порядку, или национальной безопасности.

6. Международная информационная и коммуникационная безопасность – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в сфере информационных и коммуникационных средств и технологий.

ПИСЬМО ПОСТОЯННЫХ ПРЕДСТАВИТЕЛЕЙ КИТАЯ, РОССИЙСКОЙ ФЕДЕРАЦИИ, ТАДЖИКИСТАНА И УЗБЕКИСТАНА ПРИ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ОТ 12 СЕНТЯБРЯ 2011 г. НА ИМЯ ГЕНЕРАЛЬНОГО СЕКРЕТАРЯ ООН[1]

В последние годы был достигнут значительный прогресс в деле разработки и внедрения новейших информационных и телекоммуникационных технологий, которые потенциально могу использоваться в целях, противоречащих с задачами обеспечения международной стабильности и безопасности. Чрезвычайно важно решать общие проблемы в сфере информационной безопасности на основе международного сотрудничества и в духе взаимного уважения. С этой целью Китай, Россия, Таджикистан и Узбекистан совместно выработали в виде возможной резолюции Генеральной Ассамблеи «Правила поведения

[1] URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement. См. также: http://www.un.org/russian/news/story.asp?NewsID=18471

в области обеспечения международной информационной безопасности» и призывают международное сообщество в рамках Организации Объединенных Наций рассмотреть эти правила с целью в ближайшее время попытаться выработать консенсус в отношении международных норм и правил, регулирующих действия государств в информационном пространстве (см. приложение).

Были бы весьма признательны Вам за распространение настоящего письма и приложения к нему в качестве документа шестьдесят шестой сессии Генеральной Ассамблеи по пункту 93 предварительной повестки дня.

Ли Баодун
Постоянный представитель Китайской
Народной Республики
при Организации Объединенных Наций
Виталий Чуркин
Постоянный представитель Российской Федерации
при Организации Объединенных Наций
Сироджидин Аслов
Постоянный представитель Таджикистана
при Организации Объединенных Наций
Мурад Аскаров
Постоянный представитель Узбекистана
при Организации Объединенных Наций

Приложение к письму постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 года на имя Генерального секретаря

[Подлинный текст на английском, китайском и русском языках]

ПРАВИЛА ПОВЕДЕНИЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Генеральная Ассамблея,

ссылаясь на свои резолюции о роли науки и техники в контексте международной безопасности, в которых, в частности, признается,

что достижения науки и техники могут иметь как гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях,

отмечая значительный прогресс, достигнутый в разработке и внедрении новейших информационных технологий и средств телекоммуникации,

признавая необходимость предотвращения возможности использования информационно-коммуникационных технологий в целях, которые не совместимы с задачами обеспечения международной стабильности и безопасности и способны оказать отрицательное воздействие на целостность государственных инфраструктур, нанося ущерб их безопасности,

подчеркивая необходимость усиления координации и укрепления сотрудничества между государствами в борьбе с преступным использованием информационных технологий и в этом контексте отмечая ту роль, которую могут сыграть Организация Объединенных Наций и другие международные и региональные организации,

подчеркивая важность безопасного, непрерывного и стабильного функционирования Интернета и необходимость защиты Интернета и других сетей информационно-коммуникационных технологий от возможного неблагоприятного воздействия и подверженности рискам; подтверждая необходимость общего понимания вопросов безопасности Интернета и дальнейшего сотрудничества на национальном и международном уровнях,

вновь подтверждая, что политические полномочия по связанным с Интернетом вопросам государственной политики являются суверенным правом государств, государства имеют права и обязанности в отношении связанных с Интернетом вопросов государственной политики международного уровня,

признавая, что доверие и безопасность в использовании информационнокоммуникационных технологий относятся к главным опорам информационного общества и что необходимо поощрять, формировать, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности, как отмечается в резолюции 64/211 Генеральной Ассамблеи от 21 декабря 2009 года «Создание глобальной культуры кибербезопасности и оценка национальных усилий позащите важнейших информационных инфраструктур»,

отмечая необходимость активизации усилий по преодолению цифрового разрыва путем облегчения передачи информационно-коммуникационных технологий развивающимся странам и наращивания

их потенциала в вопросах передовой практики и профессиональной подготовки в области кибербезопасности, как отмечается в резолюции 64/211,

принимает следующие Правила поведения в области обеспечения международной информационной безопасности:

Цели и область применения

Основная цель настоящих Правил заключается в определении прав и обязанностей государств в информационном пространстве, стимулировании их конструктивного и ответственного поведения и укреплении сотрудничества между ними для противостояния общим вызовам и угрозам в информационном пространстве, с тем чтобы информационно-коммуникационные технологии, включая сети, использовались только для полномасштабного социального и экономического развития и благосостояния народов и не противоречили целям обеспечения международного мира и безопасности.

Правила открыты для присоединения любых государств на добровольной основе.

Правила поведения

Каждое государство, добровольно соблюдающее настоящие Правила, обязуется:

a) соблюдать Устав Организации Объединенных Наций и общепризнанные нормы международного права, которые включают, помимо прочего, уважение суверенитета, территориальной целостности и политической независимости всех государств, уважение прав и основных свобод человека, а также уважение многообразия истории, культуры и социального устройства всех стран;

b) не использовать информационно-коммуникационные технологии, включая сети, для осуществления враждебных действий, актов агрессии, создания угроз международному миру и безопасности или распространения информационного оружия или соответствующих технологий;

c) сотрудничать в борьбе с преступной или террористической деятельностью с использованием информационно-коммуникационных технологий, включая сети, и сдерживать распространение информации террористического, экстремистского и сепаратистского характера, а также подрывающей политическую, экономическую и социальную стабильность государств, их культурный и духовный уклад;

d) прикладывать усилия к обеспечению безопасности на всех этапах поставок продукции и предоставления услуг в сфере информационно-коммуникационных технологий, предотвращать использование другими государствами своих ресурсов, объектов критической инфра-

структуры, ключевых технологий и иных преимуществ для подрыва права государств, принявших настоящие Правила поведения, на независимый контроль над сферой информационно-коммуникационных технологий или для создания угроз политической, экономической и социальной безопасности других стран;

e) подтверждать права и обязанности каждого государства, в соответствии с надлежащими нормами и правилами, в отношении законной защиты воего информационного пространства и критической информационной инфраструктуры от ущерба в результате угроз, вмешательства, атак и актов агрессии;

f) в полной мере уважать права и свободы в информационном пространстве, в том числе на поиск, получение, передачу и распространение информации в соответствии с национальным законодательством каждого государства;

g) содействовать созданию многосторонних, прозрачных и демократических международных механизмов управления Интернетом, которые позволят беспечить справедливое распределение ресурсов, способствовать доступу для всех, а также гарантировать стабильное и безопасное функционирование Интернета;

h) способствовать углублению осознания всеми элементами общества, в том числе через государственно-частное партнерство в области информационно-коммуникационных технологий, своей ответственности за обеспечение информационной безопасности, включая формирование культуры информационной безопасности и поддержку усилий по защите объектов критической информационной инфраструктуры;

i) содействовать развивающимся странам в наращивании их возможностей в сфере информационной безопасности и в ликвидации цифрового разрыва;

j) укреплять двустороннее, региональное и международное сотрудничество, способствовать тому, чтобы Организация Объединенных Наций играла важную роль в таких областях, как стимулирование выработки международных норм в области информационной безопасности, мирное разрешение международных споров, повышение качественного уровня сотрудничества государств в сфере информационной безопасности, а также других сферах и интенсифицировать координацию между соответствующими международными организациями;

k) любой спор, который может возникнуть в ходе деятельности, охватываемой настоящими Правилами, должен разрешаться с помощью процедур мирного урегулирования, воздерживаясь от применения военной силы или угрозы силой.

4. Международные организациии

4.1. Организация Объединенных Наций (ООН)

РЕЗОЛЮЦИЯ, ПРИНЯТАЯ ГЕНЕРАЛЬНОЙ АССАМБЛЕЕЙ 21 ДЕКАБРЯ 2009 ГОДА

[*по докладу Второго комитета (A/64/422/Add.3)*]

64/211. СОЗДАНИЕ ГЛОБАЛЬНОЙ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИИ ОЦЕНКА НАЦИОНАЛЬНЫХ УСИЛИЙ ПО ЗАЩИТЕ ВАЖНЕЙШИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР[1]

Генеральная Ассамблея,

ссылаясь на свои резолюции 55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года о борьбе с преступным использованием информационных

технологий, 57/239 от 20 декабря 2002 года о создании глобальной культуры кибербезопасности и 58/199 от 23 декабря 2003 года о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур,

ссылаясь также на свои резолюции 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года и 63/37 от 2 декабря 2008 года о достижениях в области информационных технологий в контексте международной безопасности, *ссылаясь далее* на итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества, состоявшейся 10–2 декабря 2003 года в Женеве (первый этап) и 16-18 ноября 2005 года в Тунисе (второй этап)[2],

---

[1] URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?OpenElement

[2] См. A/C.2/59/3 и A/60/687.

признавая, что доверие и безопасность в использовании информационно-коммуникационных технологий относятся к главным опорам информационного общества и что необходимо поощрять, формировать, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности, *признавая также* растущий вклад сетевых информационных технологий в выполнение многих важнейших функций в повседневной жизни, торговлю и обеспечение товарами и услугами, научные исследования, инновационную деятельность, предпринимательство и свободную передачу информации между физическими лицами и организациями, правительствами, деловыми кругами игражданским обществом;

признавая далее, что правительства, деловые круги, организации и индивидуальные владельцы и пользователи информационных технологий должны нести ответственность, сообразную их функциям, за обеспечение безопасности этих информационных технологий и принимать надлежащие меры для ее укрепления,

признавая важность мандата Форума по вопросам управления Интернетом как площадки для диалога между многими заинтересованными сторонами для обсуждения различных вопросов, включая вопросы государственной политики в связи с ключевыми элементами управления Интернетом, для содействия обеспечению устойчивого характера, надежности, безопасности, стабильности и развития Интернета и вновь заявляя о том, что все правительства должны иметь равные задачи и обязанности в сфере управления Интернетом на международной основе и обеспечения стабильности, безопасности и непрерывности Интернета,

вновь подтверждая сохраняющуюся необходимость упрочения сотрудничества — с тем чтобы правительства могли на равной основе играть свою роль и выполнять свои обязательства — в решении вопросов международной государственной политики, касающихся Интернета, а не в сфере повседневной деятельности технического и эксплуатационного характера, которая не влияет на вопросы международной государственной политики,

признавая, что каждая страна будет сама определять свои собственные важнейшие информационные инфраструктуры,

вновь подтверждая необходимость использования потенциала информационно-коммуникационных технологий для содействия достижению согласованных на международном уровне целей в области развития, в том числе сформулированных в Декларации тысячелетия, признавая, что отсутствие равного доступа к информационным тех-

нологиям и возможностей их использования государствами может подорвать их экономическое процветание, и вновь подтверждая также эффективность сотрудничества в борьбе с преступным использованием информационных технологий и в создании глобальной культуры кибербезопасности,

подчеркивая необходимость активизации усилий по преодолению «цифровой пропасти» для обеспечения универсального доступа к информационно-коммуникационным технологиям и для защиты важнейших информационных инфраструктур путем облегчения передачи информационных технологий развивающимся странам, особенно наименее развитым странам, и наращивания их потенциала в вопросах передовой практики и профессиональной подготовки в области кибербезопасности,

выражая озабоченность по поводу того, что угрозы надежному функционированию важнейших информационных инфраструктур и целостности информации, передаваемой по этим сетям, приобретают все более изощренный и серьезный характер, отрицательно сказываясь на уровне семейного, национального и международного благополучия,

подтверждая, что обеспечение защищенности важнейших информационных инфраструктур — это обязанность, которую правительства должны систематически выполнять, выступая с соответствующими инициативами на национальном уровне, в координации с заинтересованными сторонами, которые, в свою очередь, должны знать о соответствующих рисках, превентивных мерах и эффективных мерах реагирования, соответствующих возложенным на них функциям,

признавая, что национальные усилия должны подкрепляться обменом информацией и взаимодействием на международном уровне, с тем чтобы можно было эффективно противостоять таким угрозам, приобретающим все более транснациональный характер,

отмечая работу соответствующих региональных и международных организаций по укреплению кибербезопасности и вновь указывая на их роль в поддержании национальных усилий и поощрении международного сотрудничества,

отмечая также подготовленный Международным союзом электросвязи в 2009 году доклад об обеспечении защищенности информационно-коммуникационных сетей и передовой практике в области формирования культуры кибербезопасности, основное внимание в котором уделяется всеобъемлющему национальному подходу к кибербезопасности, не нарушающему свободы слова, свободы передачи информации и надлежащих правовых процедур,

признавая, что периодическая оценка прогресса в рамках национальных усилий по защите важнейших информационных инфраструктур благоприятно отражается на таких усилиях,

1. *предлагает* государствам-членам использовать, если и когда они сочтут это целесообразным, прилагаемый инструмент добровольной самооценки национальных усилий по защите важнейших информационных инфраструктур, призванный помочь им в анализе их усилий в этой области и укреплении кибербезопасности, с тем чтобы выявить области, в которых требуется принятие дополнительных мер, в целях повышения глобальной культуры кибербезопасности;

2. *рекомендует* государствам-членам и соответствующим региональным и международным организациям, разработавшим стратегии действий в области кибербезопасности и защиты важнейших информационных инфраструктур, поделиться сведениями о передовой практике и мерах, которые могли бы помочь другим государствам-членам в их усилиях по содействию обеспечению кибербезопасности, путем представления такой информации Генеральному секретарю для ее обобщения и распространения среди государств-членов.

66-е пленарное заседание,
21 декабря 2009 года

Приложение

ИНСТРУМЕНТ ДОБРОВОЛЬНОЙ САМООЦЕНКИ НАЦИОНАЛЬНЫХ УСИЛИЙ ПО ЗАЩИТЕ ВАЖНЕЙШИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР[1]

Анализ потребностей и стратегий в области кибербезопасности

1. Проанализируйте роль информационно-коммуникационных технологий в Вашей национальной экономике, национальной безопасности, важнейших инфраструктурах (таких, как транспорт, водоснабжение, обеспечение продовольствием, общественное здравоохранение, энергетика, финансы, службы экстренной помощи) и гражданском обществе.

2. Определите риски в области кибербезопасности и защиты важнейших информационных инфраструктур для экономики, национальной

[1] Это добровольный инструмент, который может использоваться государствами-членами (полностью или частично, если и когда они сочтут это целесообразным) и который призван помочь им в анализе их усилий по защите важнейших информационных инфраструктур и укреплению кибербезопасности.

безопасности, важнейших инфраструктур и гражданского общества Вашей страны, которые нуждаются в управлении.

3. Выявите слабые места в используемых сетях, относительные уровни текущих угроз в каждом секторе и существующий план управления; обратите внимание, как на этих расчетах сказываются изменения в экономической ситуации, приоритетах в области национальной безопасности и потребностях гражданского общества.

4. Определите цели национальной стратегии по обеспечению кибербезопасности и защиты важнейших информационных инфраструктур; опишите эти цели, нынешний уровень достижения, существующие меры по оценке достигнутого прогресса, связь стратегии с задачами национальной политики, а также, как эта стратегия вписывается в региональные и международные инициативы.

Роли и обязанности заинтересованных сторон

5. Определите ключевые заинтересованные стороны, участвующие в обеспечении кибербезопасности и защиты важнейших информационных инфраструктур, и опишите роль каждой из них в разработке соответствующих стратегий и операций, включая:

- национальные государственные министерства и ведомства с указанием главных лиц для контактов и обязанностей каждого из них;
- других государственных (местных и региональных) участников;
- неправительственных участников, включая представителей отрасли, гражданского общества и научных кругов;
- отдельных граждан с указанием того, имеют ли рядовые пользователи Интернета доступ к базовой подготовке, позволяющей избегать угроз в Интернете, и проводится ли национальная кампания распространения информации по вопросу кибербезопасности.

Стратегические процессы и участие

6. Перечислите существующие в настоящее время формальные и неформальные механизмы взаимодействия между правительством и отраслью в разработке стратегий и операций в области кибербезопасности и защиты важнейших информационных инфраструктур; определите участников, роль(и) и задачи, методы мобилизации и анализа вклада в эту деятельность и то, насколько он обеспечивает достижение соответствующих целей в области кибербезопасности и защиты важнейших информационных инфраструктур.

7. Определите другие форумы или структуры, которые могут понадобиться для интеграции позиций правительства и неправительствен-

ных участников и их знаний, что необходимо для достижения национальных целей в области кибербезопасности и защиты важнейших информационных инфраструктур.

Сотрудничество между государственным и частным секторами

8. Представьте сводную информацию о всех принятых мерах и планах по развитию сотрудничества между правительством и частным сектором, включая любые механизмы распространения информации и реагирования на инциденты.

9. Представьте сводную информацию о всех осуществляемых и запланированных инициативах по отстаиванию общих интересов и решению общих проблем как среди участников важнейших инфраструктур, так и среди представителей частного сектора, в равной степени зависящих от пользования одними и теми же взаимосвязанными важнейшими инфраструктурами.

Деятельность в связи с инцидентами и восстановление после сбоев

10. Укажите государственное ведомство, выполняющее функции координатора деятельности в связи с инцидентами, включая возможные функции наблюдения, предупреждения, реагирования и восстановления;

сотрудничающие с ним государственные ведомства; сотрудничающих неправительственных участников, включая представителей отрасли и других партнеров; и любые существующие механизмы сотрудничества и обмена достоверной информацией.

11. Отдельно укажите общенациональный механизм реагирования на компьютерные сбои, включая любую группу реагирования на компьютерные сбои, выполняющую общенациональные функции, и перечислите ее функции и обязанности, в том числе опишите существующий инструментарий и процедуры защиты правительственных компьютерных сетей и существующие инструменты и процедуры распространения информации о деятельности в связи с инцидентами.

12. Укажите сети и процессы международного сотрудничества, которые могут укрепить потенциал реагирования на инциденты и планирования на случай чрезвычайных ситуаций, отдельно выделив в соответствующих случаях партнеров и механизмы двустороннего и многостороннего сотрудничества.

Правовые рамки

13. Проанализируйте и обновите список правовых органов (в том числе занимающихся вопросами киберпреступности, охраны личной

информации, защиты данных, коммерческого права, цифровых подписей и шифрования), которые могут устареть или утратить актуальность в результате быстрого развития новых информационно-коммуникационных технологий и формирования зависимости от них, используя в ходе этого рассмотрения региональные и международные конвенции, механизмы и прецеденты. Установите, разработала ли Ваша страна необходимое законодательство для расследования киберпреступлений и преследования лиц, виновных в их совершении, обратив внимание на существующие механизмы, например на резолюции 55/63 и 56/121 Генеральной Ассамблеи о борьбе с преступным использованием информационных технологий и на региональные инициативы, включая Конвенцию Совета Европы о киберпреступности.

14. Определите нынешнее состояние национальных органов по борьбе с киберпреступностью и соответствующих процедур, включая правовые органы и национальные группы по борьбе с киберпреступностью, и уровень взаимопонимания между прокурорами, судьями и законодателями, занимающимися вопросами киберпреступности.

15. Оцените, насколько существующие правовые кодексы и правовые органы соответствуют задаче решения существующих и будущих проблем киберпреступности и киберпространства в целом.

16. Изучите уровень национального участия в международной деятельности по борьбе с киберпреступностью, такой как круглосуточно функционирующая Сеть контактных пунктов по киберпреступности.

17. Определите потребности национальных правоохранительных органов в сотрудничестве с международными коллегами при расследовании транснациональных киберпреступлений в тех случаях, когда инфраструктура или лица, обвиняемые в совершении этих преступлений, находятся на Вашей национальной территории, а жертва находится за пределами Вашей страны.

Формирование глобальной культуры кибербезопасности

18. Представьте сводную информацию о принятых мерах и планах по формированию национальной культуры кибербезопасности, о которой говорится в резолюциях 57/239 и 58/199 Генеральной Ассамблеи, включая реализацию плана кибербезопасности для систем, управление которыми осуществляет правительство, национальных программ повышения уровня осведомленности и распространения знаний среди, в частности, детей и индивидуальных пользователей, а также о потребностях в профессиональной подготовке в области национальной кибербезопасности и защиты важнейших информационных инфраструктур.

РЕЗОЛЮЦИЯ, ПРИНЯТАЯ ГЕНЕРАЛЬНОЙ АССАМБЛЕЕЙ 3 ДЕКАБРЯ 2012 ГОДА

[*по докладу Первого комитета (a/67/404)*]

67/27. ДОСТИЖЕНИЯ В СФЕРЕ ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИЙ В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ[1]

Генеральная Ассамблея,

ссылаясь на свои резолюции 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года, 63/37 от 2 декабря 2008 года, 64/25 от 2 декабря 2009 года, 65/41 от 8 декабря 2010 года и 66/24 от 2 декабря 2011 года,

ссылаясь также на свои резолюции по вопросу о роли науки и техники в контексте международной безопасности, в которых, в частности, признается, что достижения науки и техники могут иметь как гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях,

отмечая значительный прогресс, достигнутый в разработке и внедрении новейших информационных технологий и средств телекоммуникации,

подтверждая, что она видит в этом процессе широчайшие позитивные возможности для дальнейшего развития цивилизации, расширения возможностей взаимодействия на общее благо всех государств, увеличения созидательного потенциала человечества и дополнительных сдвигов к лучшему в распространении информации в глобальном сообществе,

напоминая в этой связи о подходах и принципах, которые были намечены на конференции «Информационное сообщество и развитие», состоявшейся в Мидранде, Южная Африка, 13–15 мая 1996 года,

учитывая итоги Совещания на уровне министров по проблеме терроризма, которое состоялось в Париже 30 июля 1996 года, а также принятые на нем рекомендации[2],

---

[1] URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N12/480/24/PDF/N1248024.pdf?OpenElement

[2] См. A/51/261, приложение.

учитывая также результаты Всемирной встречи на высшем уровне по вопросам информационного общества (первый этап – Женева, 10–12 декабря 2003 года, второй этап – Тунис, 16–18 ноября 2005 года)[1],

отмечая, что распространение и использование информационных технологий и средств затрагивают интересы всего международного сообщества и что широкое международное взаимодействие способствует обеспечению оптимальной эффективности,

выражая озабоченность тем, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на целостность инфраструктуры государств, нарушая их безопасность применительно как к гражданской, так и к военной сферам,

считая необходимым предотвратить использование информационных ресурсов или технологий в преступных или террористических целях,

отмечая вклад государств-членов, представивших Генеральному секретарю свои оценки по вопросам информационной безопасности в соответствии с пунктами 1–3 резолюций 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45, 61/54, 62/17, 63/37, 64/25, 65/41 и 66/24,

принимая к сведению доклады Генерального секретаря, содержащие эти оценки[2],

отмечая с удовлетворением инициативу Секретариата и Института Организации Объединенных Наций по исследованию проблем разоружения по проведению в Женеве в августе 1999 года и в апреле 2008 года международных встреч экспертов по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также результаты этих встреч,

считая, что оценки государств-членов, содержащиеся в докладах Генерального секретаря, а также международные встречи экспертов способствовали лучшему пониманию существа проблем международной информационной безопасности и связанных с ними понятий,

учитывая, что во исполнение резолюции 60/45 Генеральный секретарь учредил в 2009 году на основе справедливого географического распределения группу правительственных экспертов, которая в соответствии со своим мандатом рассмотрела существующие и потенци-

[1] A/C.2/59/3, приложение, и A/60/687.

[2] A/54/213, A/55/140 и Corr.1 и Add.1, A/56/164 и Add.1, A/57/166 и Add.1, A/58/373, A/59/116 и Add.1, A/60/95 и Add.1, A/61/161 и Add.1, A/62/98 и Add.1, A/64/129 и Add.1, A/65/154, A/66/152 и Add.1 и A/67/167.

альные угрозы в сфере информационной безопасности и возможные совместные меры по их устранению, а также провела исследование соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем,

с удовлетворением отмечая результативную работу Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и соответствующий доклад, препровожденный Генеральным секретарем[1],

принимая к сведению оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов,

1. *призывает* государства-члены и далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных стратегий по рассмотрению угроз, возникающих в этой сфере, исходя из необходимости сохранить свободный поток информации;

2. *полагает,* что целям таких стратегий соответствовало бы продолжение изучения соответствующих международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем;

3. *просит* 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, 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 выше;

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

4. *приветствует* начало работы Группы правительственных экспертов, уполномочивает Группу продолжить с учетом оценок и рекомендаций, содержащихся в упомянутом выше докладе, исследование существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, включая

[1] См. A/65/201.

нормы, правила или принципы ответственного поведения государств и меры укрепления доверия в информационном пространстве, а также концепций, упомянутых в пункте 2 выше, и просит Генерального секретаря представить Генеральной Ассамблее на ее шестьдесят восьмой сессии доклад о результатах этого исследования;

5. постановляет включить в предварительную повестку дня своей шестьдесят восьмой сессии пункт, озаглавленный «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

48-е пленарное заседание,
3 декабря 2012 года

ДОСТИЖЕНИЯ В СФЕРЕ ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИЙ В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ[1]

(Генеральная Ассамблея ООН, 68-я сессия,
4 октября 2013 г. – 6 ноября 2013 г., Нью-Йорк.
Аргентина, Бразилия, Египет, Казахстан, Китай,
Корейская Народно-Демократическая Республика, Куба,
Кыргызстан, Лаосская Народно-Демократическая Республика,
Мадагаскар, Мали, Российская Федерация,Сербия,
Сирийская Арабская Республика, Туркменистан,
Угандаи Украина: проект резолюции)

Генеральная Ассамблея,

ссылаясь на свои резолюции 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года, 63/37 от 2 декабря 2008 года, 64/25 от 2 декабря 2009 года, 65/41 от 8 декабря 2010 года, 66/24 от 2 декабря 2011 года и 67/27 от 3 декабря 2012 года,

ссылаясь также на свои резолюции по вопросу о роли науки и техники в контексте международной безопасности, в которых, в частности, признается, что достижения науки и техники могут иметь как

[1] URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/520/55/PDF/N1352055.pdf?OpenElement

гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях,

отмечая значительный прогресс, достигнутый в разработке и внедрении новейших информационных технологий и средств телекоммуникации,

подтверждая, что она видит в этом процессе широчайшие позитивные возможности для дальнейшего развития цивилизации, расширения возможностей взаимодействия на общее благо всех государств, увеличения созидательного потенциала человечества и дополнительных сдвигов к лучшему в распространении информации в глобальном сообществе,

напоминая в этой связи о подходах и принципах, которые были намечены на конференции «Информационное сообщество и развитие», состоявшейся в Мидранде, Южная Африка, 13–15 мая 1996 года,

учитывая итоги Совещания на уровне министров по проблеме терроризма, которое состоялось в Париже 30 июля 1996 года, а также принятые на нем рекомендации[1],

учитывая также результаты Всемирной встречи на высшем уровне по вопросам информационного общества (первый этап – Женева, 10–12 декабря 2003 года, второй этап – Тунис, 16–18 ноября 2005 года)[2],

отмечая, что распространение и использование информационных технологий и средств затрагивают интересы всего международного сообщества и что широкое международное взаимодействие способствует обеспечению оптимальной эффективности,

выражая озабоченность тем, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на целостность инфраструктуры государств, нарушая их безопасность применительно как к гражданской, так и к военной сферам,

считая необходимым предотвратить использование информационных ресурсов или технологий в преступных или террористических целях,

отмечая важность уважения прав человека и основных свобод в сфере использования информационно-коммуникационных технологий,

отмечая вклад государств-членов, представивших Генеральному секретарю свои оценки по вопросам информационной безопасности

[1] См. A/51/261, приложение.

[2] A/C/2/59/3, приложение, и A/60/687.

в соответствии с пунктами 1–3 резолюций 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45, 61/54, 62/17, 63/37, 64/25 и 65/41, 66/24 и 67/27,

принимая к сведению доклады Генерального секретаря, содержащие эти оценки[1],

отмечая с удовлетворением инициативу Секретариата и Института Организации Объединенных Наций по исследованию проблем разоружения по проведению в Женеве в августе 1999 года и в апреле 2008 года международных встреч экспертов по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также результаты этих встреч,

считая, что оценки государств-членов, содержащиеся в докладах Генерального секретаря, а также международные встречи экспертов способствовали лучшему пониманию существа проблем международной информационной безопасности и связанных с ними понятий,

учитывая, что во исполнение резолюции 66/24 Генеральный секретарь учредил в 2012 году на основе справедливого географического распределения группу правительственных экспертов, которая в соответствии со своим мандатом рассмотрела существующие и потенциальные угрозы в сфере информационной безопасности и возможные совместные меры по их устранению, включая нормы, правила или принципы ответственного поведения государств и меры укрепления доверия в информационном пространстве, а также провела исследование соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем,

с удовлетворением отмечая результативную работу Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и подготовленный в итоге соответствующий доклад, препровожденный Генеральным секретарем[2],

принимая к сведению оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов,

1. *призывает* государства-члены и далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных

[1] A/54/213, A/55/140 и Corr.1 и Add.1, A/56/164 и Add.1, A/57/166 и Add.1, A/58/373, A/59/116 и Add.1, A/60/95 и Add.1, A/61/161 и Add.1, A/62/98 и Add.1, A/64/129 и Add.1, A/65/154, A/66/152 и Add.1 и A/67/167.

[2] См. A/68/98.

стратегий по рассмотрению угроз, возникающих в этой сфере, исходя из необходимости сохранить свободный поток информации;

2. *полагает*, что целям таких стратегий соответствовало бы продолжение изучения соответствующих международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем;

3. *просит* 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, 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 выше;

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

4. *просит* Генерального секретаря с помощью группы правительственных экспертов, которая должна быть создана в 2014 году на основе справедливого географического распределения, продолжить с учетом оценок и рекомендаций, содержащихся в упомянутом выше докладе, в целях содействия выработке общего понимания исследование 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, вопросов использования информационно-коммуникационных технологий в конфликтах и того, как международноеправо применяется к использованию информационно-коммуникационных технологий государствами, а также концепций, упомянутых в пункте 2 выше, и представить доклад о результатах данного исследования Генеральной Ассамблее на ее семидесятой сессии;

5. *постановляет* включить в предварительную повестку дня своей шестьдесят девятой сессии пункт, озаглавленный «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В ЦИФРОВУЮ ЭПОХУ[1]

(Проект резолюции Генеральной Ассамблеи ООН, подготовленный Бразилией и Германией)
(*2013 г.*)

Генеральная Ассамблея,

Вновь подтверждая цели и принципы Устава Организации Объединенных Наций,

Вновь подтверждая также права человека и основные свободы, сформулированные во Всеобщей декларации прав человека и в соответствующих международных договорах по правам человека, в том числе в Международном пакте о гражданских и политических правах и Международном пакте об экономических, социальных и культурных правах,

Вновь подтверждая Венскую Декларацию и Программу действий,

Отмечая, что быстрые темпы технологического развития позволяют людям во всем мире пользоваться новыми информационно-коммуникационными технологиями и в то же время увеличивают возможности правительств, компаний и отдельных граждан по слежению, перехвату и сбору данных, что может привести к нарушению прав человека, в частности права на неприкосновенность частной жизни, как оно сформулировано в статье 12 Всеобщей декларации прав человека и в статье 17 Международного пакта о гражданских и политических правах, и вследствие этого становится предметом растущей обеспокоенности,

Подтверждая права человека на неприкосновенность частной жизни и недопустимость произвольного или незаконного вмешательства в его личную и семейную жизнь, произвольного или незаконного посягательства на неприкосновенность его жилища или тайну его корреспонденции, а также подтверждая его право на защиту закона от такого вмешательства или таких посягательств и признавая, что реализация права на неприкосновенность частной жизни является базовым условием для реализации свободы выражения мнений и права беспрепятственно придерживаться своих мнений и составляет одну из основ демократического общества,

Подчеркивая важность полного уважения свободы личности искать, получать и распространять информацию, в том числе огром-

[1] URL: http://www.auswaertiges-amt.de/cae/servlet/contentblob/660692/publicationFile/186833/131127_Right2Privacy_EN.pdf (неофициальный перевод О.В. Демидова и М.Б. Касеновой).

ное значение доступа к информации и участию в демократическом процессе,

Положительно оценивая Доклад Специального докладчика ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение[1], представленный Совету по правам человека на его 23-м заседании и содержащий оценку возможных негативных последствий, которые могут возникнуть на пути реализации права на неприкосновенность частной жизни от осуществления государствами слежения за коммуникациями и перехвата персональных данных,

Обращая особое внимание на то, что незаконное слежение за коммуникациями и их перехват, как и незаконный сбор персональных данных, представляют собой действия, которые вызывают опасения и нарушают права на неприкосновенность частной жизни и права на свободу выражения мнений и могут представлять угрозу для основ демократического общества,

Отмечая, что хотя сбор и защита определенных видов чувствительной информации и могут быть оправданы соображениями общественной безопасности, государства при этом должны обеспечить полное соблюдение своих обязательств, вытекающих из международного права в области прав человека,

Выражая глубокую озабоченность нарушениями и злоупотреблениями в отношении прав человека, которые могут возникнуть в результате слежения за коммуникациями, включая транснациональное слежение, их перехвата, равно как и при сборе персональных данных, в частности при массированных слежении, перехвате и сборе данных (новое),

Напоминая, что государства при осуществлении мер против терроризма должны обеспечить соблюдение норм международного права, в частности прав человека, прав беженцев и гуманитарного права,

1. *Вновь подтверждает* права, сформулированные в Международном пакте о гражданских и политических правах, в частности права человека на неприкосновенность частной жизни и недопустимость произвольного или незаконного вмешательства в его личную и семейную жизнь, произвольного или незаконного посягательства на неприкосновенность его жилища или тайну его корреспонденции, а также подтверждая его право на защиту закона от такого вмешательства или таких посягательств в соответствии со статьей 12 Всеобщей декларации прав человека и статьей 17 Международного пакта о гражданских и политических правах;

[1] A/HRC/23/40 and Corr.1.

2. *Признает*, что быстрое развитие информационных и коммуникационных технологий, включая глобальный и открытый характер Интернета, является движущей силой ускорения прогресса по пути развития в его различных формах;

3. *Подтверждает*, что те же права, которые человек имеет в оффлайновой среде, должны также защищаться и в онлайновой среде, в частности право на неприкосновенность частной жизни;

4. *Призывает* все государства:

(*a*) Уважать и защищать права человека, упомянутые в параграфе 1 выше, включенные в контекст цифровых коммуникаций;

(*b*) принимать все необходимые меры для пресечения нарушений этихправ и создавать условия для предотвращения таких нарушений, в том числе путем обеспечения того, чтобы соответствующее национальное законодательство соответствовало международным обязательствам государств в области прав человека;

(*c*) Пересмотреть процедуры, практики и законодательство относительно слежения за коммуникациями, их перехвата и сбора персональных данных, включая массированное осуществление слежения за коммуникациями, их перехвата и сбора персональных данных, для обеспечения права на неприкосновенность частной жизни и полного и эффективного соблюдения всех обязательств государств в рамках международного права в области прав человека;

(*d*) Сформировать независимые национальные контролирующие механизмы, позволяющие обеспечить прозрачность и подотчетность действий государства в отношении слежения за коммуникациями, их перехвата и сбора персональных данных;

5. *Предлагает* Верховному Комиссару ООН по правам человека представить на 69-й сессии Генеральной Ассамблеи Организации Объединенных Наций промежуточный отчет по вопросам обеспечения права на неприкосновенность частной жизни в рамках национальных и транснациональных действий, включая массированные, по слежению за коммуникациями, их перехвату и сбору персональных данных, а на 70-й сессии – окончательный отчет, в котором должны содержаться соображения и рекомендации, предназначенные для рассмотрения государствами –членами ООН, целью которых является определение и прояснение принципов, стандартов и передовых практик по обеспечению национальной безопасности при соблюдении государствами своих обязательств в рамках международного права в области прав человека и при полном уважении прав человека, в частности, относительно слежения за цифровыми коммуникациями и использования

других разведывательных технологий, которые могут привести к нарушению прав человека на неприкосновенность частной жизни, прав на свободу мнений и их свободное выражение;

6. *Принимает* решение рассмотреть вопрос как приоритетный на своей 69-й сессии под подзаголовком «Вопросы прав человека, включая альтернативные подходы к улучшению и эффективному использованию индивидуумами прав человека и основных свобод» в разделе, озаглавленном «Поощрение и защита прав человека».

ДОКЛАД ГРУППЫ ПРАВИТЕЛЬСТВЕННЫХ ЭКСПЕРТОВ ПО ДОСТИЖЕНИЯМ В СФЕРЕ ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИЙ В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ[1]

(июль 2010 г.)
Документ A/65/201

Резюме

Существующие и потенциальные угрозы в сфере информационной безопасности относятся к числу наиболее серьезных проблем XXI века.

[1] URL: www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33_Russian.pdf

Как отмечается во введении к изданию ООН, подготовленного в 2012 г. в рамках Информационной программы ООН по разоружению и содержащему настоящий доклад второй группы правительственных экпертов, «вопрос «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» остается в повестке дня Организации Объединенных Наций с 1998 года, когда Российская Федерация внесла на рассмотрение Первого комитета Генеральной Ассамблеи Организации Объединенных Наций проект резолюции, принятый без голосования.

С этого момента Генеральный секретарь ежегодно представляет Генеральной Ассамблее доклады, в которых государства — члены Организации Объединенных Наций выражают свои мнения по этому важному вопросу и подчеркивают необходимость коллективных действий.

До сегодняшнего дня были созданы две группы правительственных экспертов (ГПЭ). Первая группа проводила свои заседания в 2004 и 2005 годах. Вторая группа начала работу в 2009 году и завершила обсуждения в 2010 году. Обе группы занимались рассмотрением существующих и потенциальных угроз из киберпространства и изучением озможных коллективных мер по их устранению. Учитывая сравнительную «новизну» киберпространства и сложность связанных с ним вопросов, первая группа не могла достичь консенсуса в отношении заключительного доклада. Второй группе, которая работала позднее, удалось согласовать доклад, который был издан в 2010 году».

Угрозы исходят из широкого круга сточников и проявляются в подрывной деятельности, направленной в равной степени против физических и юридических лиц, национальной инфраструктуры и правительств. Ее последствия сопряжены со значительным риском для общественной безопасности, безопасности стран и стабильности объединенного в глобальную сеть международного сообщества в целом.

В результате роста применения информационных и коммуникационных технологий (ИКТ) в критически важной инфраструктуре возникают новые уязвимые места и возможности для совершения подрывных действий. В силу сложной взаимосвязанности телекоммуникационных сетей и Интернета любое устройство ИКТ может служить источником или объектом все более изощренных злонамеренных действий. Поскольку в силу самого характера ИКТ они могут использоваться двояко, те же технологии, которые применяются для обеспечения надежной системы электронной торговли, могут также использоваться в целях создания угрозы международному миру и национальной безопасности.

Установить источник подрывных действий, личность виновного в их совершении или мотивацию таких действий может быть нелегко. Во многих случаях виновных в совершении такой деятельности можно определить лишь по объекту этих действий, их последствиям или другим косвенным уликам, и они могут совершать такие действия, фактически где бы они ни находились. Эти факторы содействуют использованию ИКТ в целях осуществления подрывной деятельности. Неопределенность в плане выявления источника действия и отсутствие общепринятого понимания создают риск нестабильности и неправильного восприятия.

Поступает все больше сообщений о том, что государства разрабатывают ИКТ в качестве инструментов ведения войны и разведки и для применения в политических целях. Все большее беспокойство вызывают физические лица, группы или организации, включая преступные организации, которые выполняют посреднические функции в осуществлении подрывной сетевой деятельности от имени других. Растущая изощренность и масштабы преступной деятельности повышают вероятность оказания вредного воздействия. Хотя число свидетельств использования террористами ИКТ в целях ведения подрывных операций невелико, в будущем масштабы такого использования ИКТ могут возрасти.

Решение проблем XXI века зависит от успешного сотрудничества между партнерами, придерживающимися одинаковых убеждений. Сотрудничество между государствами и между государствами, частным сектором и гражданским обществом имеет важное значение, а для обеспечения эффективности мер по повышению информационной безопасности

необходимо широкое международное сотрудничество. В докладе Группы правительственных экспертов выносятся рекомендации в отношении ведения дальнейшего диалога между государствами в целях снижения риска и защиты критической национальной и международной инфраструктуры.

Предисловие Генерального секретаря

Десятилетие назад мы не могли себе представить, как глубоко информационные технологии и телекоммуникации войдут в нашу повседневную жизнь и сколь широко мы будем полагаться на их использование. Эти технологии привели к созданию объединенного в глобальную сеть международного сообщества, и хотя такое объединение создает огромные преимущества, оно порождает также уязвимость и риск.

В области принятия мер в связи с последствиями, обусловливаемыми новыми технологиями, достигнут значительный прогресс. Однако это трудная задача, и мы только начали разрабатывать нормы, законы и формы сотрудничества, необходимые в этой новой информационной среде.

С учетом этого я назначил группу правительственных экспертов из 15 государств для исследования существующих и потенциальных угроз в этой области и вынесения рекомендаций в отношении путей их устранения. Я благодарю Председателя Группы и экспертов за их кропотливую и усердную работу, результатом которой стал этот доклад, представляющий собой сжатое изложение проблемы и возможных последующих мер.

Генеральная Ассамблея призвана сыграть важную роль в процессе повышения безопасности информационных технологий и телекоммуникаций как на национальном, так и на международном уровнях. Для разработки общих концепций важное значение будет иметь диалог между государствами-членами. Жизненно важное значение имеет также практическое сотрудничество в целях обмена передовым опытом и информацией и создания потенциала в развивающихся странах, а также снижения риска неправильного восприятия, которое может ограничить возможности международного сообщества по принятию мер в случаях серьезных происшествий в киберпространстве.

Это насыщенная повестка дня будущей работы. Подготовка настоящего доклада призвана послужить первым шагом в направлении создания международной системы обеспечения безопасности и стабильности, необходимой в связи с этими новыми технологиями. Я предлагаю содержащийся в этом докладе анализ и рекомендации вниманию государств-членов и широкой мировой аудитории.

Препроводительное письмо

16 июля 2010 г.

Имею честь представить настоящим доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Эта Группа была создана в 2009 году в соответствии с пунктом 4 резолюции 60/45 Генеральной Ассамблеи. В качестве Председателя Группы я с удовлетворением сообщаю вам, что по этому докладу был достигнут консенсус.

В указанной резолюции, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», Генеральная Ассамблея просила создать в 2009 году Группу правительственных экспертов на основе справедливого географического распределения с тем, чтобы продолжить исследование существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, а также концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем. Генеральная Ассамблея просила Генерального секретаря представить ей доклад о результатах данного исследования на ее шестьдесят пятой сессии.

В соответствии с положениями данной резолюции были назначены эксперты из 15 государств: Беларуси, Бразилии, Германии, Израиля, Индии, Италии, Катара, Китая, Республики Корея, Российской Федерации, Соединенного Королевства Великобритании и Северной Ирландии, Соединенных Штатов Америки, Франции, Эстонии и Южной Африки. Список экспертов приводится ниже.

Группа правительственных экспертов провела четыре сессии: первую сессию с 24 по 26 ноября 2009 года в Женеве, вторую — с 11 по 15 января 2010 года в Центральных учреждениях Организации Объединенных Наций, третью — с 21 по 25 июня 2010 года в Женеве и четвертую — с 12 по 16 июля в Центральных учреждениях Организации Объединенных Наций.

В Группе состоялся всесторонний и углубленный обмен мнениями по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности. Кроме того, Группа приняла во внимание мнения, изложенные в ответах, направленных государствами-членами во исполнение резолюций 60/45, 61/54, 62/17 и 63/37 Генеральной Ассамблеи, соответственно озаглавленных «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», а также материалы и справочные документы, предоставленные отдельными членами Группы.

Группа хотела бы выразить свою признательность за внесенный вклад Институту Организации Объединенных Наций по исследованию проблем разоружения, который консультировал Группу и был представлен в лице Джеймса Льюиса и Керстина Вигнарда.

Группа хотела бы также выразить свою признательность сотруднику по вопросам информации Сектора информации и пропаганды Управления по вопросам разоружения Секретариата Юэну Бьюканану, который исполнял обязанности Секретаря Группы, и другим должностным лицам Секретариата, оказавшим содействие Группе.

Андрей Владимирович Крутских
Председатель Группы

I. Введение

1. Существующие и потенциальные угрозы в сфере информационной безопасности относятся к числу наиболее серьезных проблем XXI века. Реализация этих угроз может нанести серьезный ущерб экономике и национальной и международной безопасности. Угрозы исходят из широкого круга источников и проявляются в подрывной деятельности, направленной в равной степени против физических и юридических лиц, национальной инфраструктуры и правительств. Ее последствия сопряжены со значительным риском для общественной безопасности, безопасности стран и стабильности объединенного в глобальную сеть международного сообщества в целом.

2. Информационные и коммуникационные технологии (ИКТ) обладают особенностями, которые затрудняют принятие мер в связи с угрозами, с которыми могут сталкиваться государства и другие пользователи. ИКТ распространены повсеместно и широко доступны. По своей сути они не являются чисто гражданскими или чисто военными технологиями, и цель их использования диктуется главным образом мотивами, которыми руководствуются пользователи. Во многих случаях владельцами и операторами сетей являются частный сектор или физические лица. В силу сложной взаимосвязанности телекоммуникационных сетей и Интернета любое устройство ИКТ может служить источником или объектом все более изощренных злонамеренных действий. Злоумышленное использование ИКТ можно легко скрыть. Установить источник подрывных действий, личность виновного в их совершении или мотивацию может быть нелегко. Во многих случаях виновных в совершении такой деятельности можно определить лишь по объекту этих действий, их последствиям или другим косвенным уликам. Исполнители угроз

могут действовать в значительной степени безнаказанно, практически где бы они ни находились. Эти факторы содействуют использованию ИКТ в целях осуществления подрывной деятельности.

3. С учетом последствий использования рассматриваемых достижений для международной безопасности Генеральная Ассамблея Организации Объединенных Наций просила Генерального секретаря с помощью правительственных экспертов провести исследование как угроз в сфере информационной безопасности, так и соответствующих международных концепций и предложить возможные совместные меры, осуществление которых могло бы укрепить безопасность глобальных информационных и коммуникационных систем.

II. Угрозы, риски и уязвимые места

4. Глобальная сеть ИКТ стала ареной для осуществления подрывной деятельности. Мотивы осуществления подрывной деятельности весьма разнообразны: начиная с простой демонстрации технического мастерства и кончая кражей денежных средств и информации или совершением такой деятельности в качестве дополнительной формы конфликта с государством. К источникам таких угроз относятся такие негосударственные субъекты, как преступные элементы и, потенциально, террористы, а также сами государства. ИКТ могут использоваться для целей нанесения ущерба информационным ресурсам и инфраструктурам. Поскольку в силу своего характера они могут использоваться двояко, те же ИКТ, которые применяются для обеспечения надежной системы электронной торговли, могут также использоваться в целях создания угрозы международному миру и национальной безопасности.

5. Многие вредоносные инструменты и методологии являются порождением усилий преступников и хакеров. Растущая изощренность и масштабы преступной деятельности повышают вероятность оказания вредного воздействия.

6. До настоящего времени число свидетельств попыток террористов поставить под угрозу или вывести из строя инфраструктуру ИКТ или провести операции с использованием ИКТ было невелико, хотя в будущем такие попытки могут активизироваться. В настоящее время террористы используют эти технологии по большей части для обмена сообщениями, сбора информации, вербовки сторонников, организации деятельности, пропаганды своих идей и действий и сбора средств, однако в конечном счете они могут начать применять ИКТ для совершения нападений.

7. Поступает все больше сообщений о том, что государства разрабатывают ИКТ в качестве инструментов ведения войны и разведки и для применения в политических целях. Неопределенность в плане определения источника действия и отсутствие общепринятого понимания того, какие действия государства в этой связи приемлемы, могут создать риск нестабильности и неправильного восприятия.

8. Все большее беспокойство вызывают физические лица, группы или организации, включая преступные организации, которые выполняют посреднические функции в осуществлении подрывной сетевой деятельности от имени других. Такие посредники, руководствуясь либо финансовой выгодой, либо другими причинами, могут предлагать государственным и негосударственным субъектам целый набор наносящих умышленный вред услуг.

9. В результате как роста применения ИКТ в критических инфраструктурах, так и расширения использования устройств мобильной связи и сетевых услуг возникают новые уязвимые места и возможности для совершения подрывных действий.

10. Государства обеспокоены также тем, что система поставок ИКТ может подвергнуться такому влиянию или быть нарушена таким образом, что это скажется на обычном, безопасном и надежном использовании ИКТ. Включение в ИКТ вредоносных скрытых функций может подорвать доверие к товарам и услугам, вызвать недоверие к торговле и сказаться на национальной безопасности.

11. Различия в степени оснащенности ИКТ и их безопасности в разных государствах повышают уязвимость глобальной сети. Различия в национальных законодательствах и практике могут создать проблемы на пути формирования безопасной и быстро восстанавливающейся цифровой среды.

III. Совместные меры

12. Риски, связанные с объединенными в глобальную систему сетями, требуют принятия согласованных мер. На протяжении прошедшего десятилетия государства-члены неоднократно подтверждали необходимость осуществления международного сотрудничества в области принятия мер в связи с угрозами в сфере безопасности ИКТ для борьбы со злонамеренным применением информационных технологий в преступных целях, создания глобальной культуры кибербезопасности и поощрения других важных мер, которые могут уменьшить риск.

13. В течение прошедшего десятилетия усилия по борьбе с угрозой киберпреступности прилагались на международном уровне, в частности в рамках Шанхайской организации сотрудничества, Организации американских государств, Форума азиатско-тихоокеанского экономического сотрудничества, Регионального форума Ассоциации государств Юго-Восточной Азии (АСЕАН), Экономического сообщества западноафриканских государств, Африканского союза, Европейского союза, Организации по безопасности и сотрудничеству в Европе и Совета Европы, а также в форме двусторонних усилий государств.

14. Следует уделять надлежащее внимание сферам непреступного применения ИКТ транснационального характера. Сюда относится риск неправильного восприятия в результате отсутствия общепринятого понимания международных норм, касающихся государственного использования ИКТ, что может сказаться на принятии мер в кризисных ситуациях, возникающих в результате серьезных происшествий. Это требует разработки мер, направленных на углубление сотрудничества в тех областях, где это возможно. Такие меры могут быть также направлены на обмен информацией и передовыми методами, устранение последствий происшествий, создание доверия, снижение риска и повышение транспарентности и стабильности.

15. Очевидно, что, поскольку подрывная деятельность с использованием информационно-коммуникационных технологий приобретает все более сложный и опасный характер, ни одно государство не может справиться с этими угрозами в одиночку. Решение проблем XXI века зависит от успешного сотрудничества между партнерами, придерживающимися одинаковых убеждений. Сотрудничество между государствами и между государствами, частным сектором и гражданским обществом имеет важное значение, и для обеспечения эффективности мер по повышению информационной безопасности необходимо широкое международное сотрудничество. В связи с этим международному сообществу следует изучить вопрос о необходимости осуществления совместных действий и создания совместных механизмов.

16. Существующие соглашения включают нормы, касающиеся использования ИКТ государствами. С учетом особенностей ИКТ со временем могут быть разработаны дополнительные нормы.

17. Создание потенциала имеет жизненно важное значение для достижения успеха в обеспечении глобальной безопасности ИКТ, оказания помощи развивающимся странам в их усилиях по повышению безопасности их критических национальных информационных инфраструктур и устранения нынешней пропасти в уровне безопасности

ИКТ. Для создания потенциала в государствах, которым может быть необходима помощь в решении вопросов безопасности их ИКТ, потребуется тесное международное сотрудничество.

IV. Рекомендации

18. С учетом существующих и потенциальных угроз, рисков и уязвимых мест в области информационной безопасности Группа правительственных экспертов считает полезным рекомендовать дальнейшие шаги по разработке мер укрепления доверия и прочих мер в целях снижения риска возникновения неправильного восприятия в результате дезорганизации или нарушений, связанных с применением ИКТ:

i) продолжение диалога между государствами в целях обсуждения норм, касающихся государственного использования ИКТ, сокращения коллективного риска и защиты критической национальной и международной инфраструктуры;

ii) принятие мер по укреплению доверия, обеспечению стабильности и уменьшению рисков в связи с последствиями государственного использования ИКТ, включая обмен мнениями стран по вопросу об использовании ИКТ в конфликтах;

iii) осуществление обмена информацией о национальных законах и национальных стратегиях обеспечения безопасности информационно-коммуникационных технологий и технологиях, принципах и передовых методах;

iv) определение мер оказания содействия созданию потенциала в менее развитых странах;

v) нахождение возможностей для выработки общей терминологии и определений в связи с положениями резолюции 64/25 Генеральной Ассамблеи.

Список членов Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Г-н Владимир Герасимович
Начальник Управления международной безопасности
и контроля над вооружениями
Министерство иностранных дел
Беларусь

Г-н Александр Пономарев (третья сессия)
Советник Постоянного представительства
Республики Беларусь при Отделении
Организации Объединенных Наций в Женеве

Г-н Александр Мариано Фейтоза, Командующий
Корпус морской пехоты, Военно-морской флот Бразилии
Управление политики, стратегии и по международным делам
Министерство обороны
Бразилия

Г-н Ли Сун (первая и вторая сессии)
Заместитель Генерального директора
Департамент по контролю над вооружениями и разоружению
Министерство иностранных дел
Китай

Г-н Кан Юн (третья и четвертая сессии)
Заместитель Генерального директора
Департамент по контролю над вооружениями и разоружению
Министерство иностранных дел
Китай

Г-н Линнар Вик
Адъюнкт-профессор Эстонского информационно-технологического колледжа
Эстония

Г-н Аймерик Симон
Международные отношения
Национальное управление безопасности информационных систем
Генеральный секретариат национальной обороны и безопасности
Франция

Г-н Грегор Кёбель
Начальник Отдела по контролю над обычными вооружениями
Федеральное министерство иностранных дел
Германия

Г-н Б. Дж. Сринатх
Старший директор
Группа быстрого реагирования на нарушения
компьютерной безопасности Индии
Министерство информационных технологий
Индия

Г-жа Родика Радиан-Гордон
Директор
Департамент по контролю над вооружениями
Министерство иностранных дел
Израиль

Г-н Винченцо Делла Корте (первая и третья сессии)
Директор Сектора безопасности систем связи
Аппарат при Председателе Совета министров
Италия

Г-н Вальтер Меккиа (вторая и четвертая сессии)
Сектор безопасности систем связи
Аппарат при Председателе Совета министров
Италия

Г-н Рашид А. Аль-Моханнади (первая сессия)
Командир роты связи сухопутных сил
Войска связи эмира
Катар

Г-н Саад М. Р. Аль-Кааби
Подполковник (инженер)
Министерство обороны
Катар

Г-н Лю Кван-чхуль
Посол
Министерство иностранных дел и торговли
Республика Корея

Г-н Андрей Владимирович Крутских
Заместитель директора
Департамент по вопросам новых вызовов и угроз
Министерство иностранных дел
Российская Федерация

Г-жа Пализа Банда (первая сессия)
Заместитель директора, Отдел регулирования Интернета
Министерство связи
Южная Африка

Генерал-майор Марио Сильвино Браццоли
Сотрудник Государственного управления информационных технологий
Министерство обороны
Южная Африка

Г-н Гавин Уиллис
Группа по международным отношениям
Национальное техническое управление информационной безопасности
Соединенное Королевство Великобритании и Северной Ирландии

Г-жа Мишель Маркофф
Старший советник по политическим вопросам
Управление по вопросам киберпространства
Государственный департамент США
Соединенные Штаты Америки

ДОКЛАД ГРУППЫ ПРАВИТЕЛЬСТВЕННЫХ ЭКСПЕРТОВ ПО ДОСТИЖЕНИЯМ В СФЕРЕ ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИЙ В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ[1]

(июнь 2013 г.)
Документ A/68/98

Резюме

Появление информационно-коммуникационных технологий (ИКТ) оказало существенное воздействие на положение дел в области международной безопасности. Эти технологии позволяют получать огромные экономические и социальные выгоды. Они также могут использоваться в целях, несовместимых с поддержанием международного мира и безопасности, в силу чего в последние годы заметно повысился уровень риска в связи с использованием ИКТ для совершения преступлений и других подрывных действий. Злонамеренное использование ИКТ злоумышленниками, которые нередко действуют в условиях безнаказанности, легко скрыть, а выявление конкретного злоумышленника может быть сопряжено с трудностями. В результате создаются условия, в которых эти злоумышленники могут осуществлять все более сложные вредоносные действия.

Государства-члены неоднократно заявляли о необходимости совместных действий, направленных на ликвидацию угроз, обусловленных злонамеренным использованием ИКТ. Международное сотрудничество – важный фактор снижения рисков и укрепления безопасности. Дальнейший прогресс в деле налаживания сотрудничества на международном уровне требует принятия мер по созданию мирных, безопасных, открытых – и благоприятных для развития сотрудничества – условий для использования ИКТ. Совместные меры, которые могут повысить стабильность и укрепить безопасность, включают в себя нормы, правила и принципы ответственного поведения государств, добровольные меры по повышению транспарентности, укреплению доверия в межгосударственных отношениях и наращиванию потенциала. Государства должны играть лидирующую роль в этом процессе, вместе с тем активное участие частного сектора и гражданского общества могло бы способствовать повышению эффективности такого сотрудничества.

Признавая всеобъемлющий характер данной проблемы, учитывая существующие и потенциальные угрозы и руководствуясь рекомендациями,

[1] URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=R

См. также примечание к предыдущему документу.

содержащимися в опубликованном в июле 2010 года докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций вконтексте международной безопасности (A/65/201), Группа правительственных экспертов представляет в настоящем докладе свои рекомендации по оказанию содействия укреплению мира и стабильности применительно к использованию государствами ИКТ.

В докладе отмечается, что применение норм, основанных на положениях международного права, в отношении деятельности государств, связанной с использованием ИКТ, — необходимая предпосылка для снижения риска нарушения международного мира, безопасности и стабильности. В докладе рекомендуется продолжать исследования в целях содействия формированию общего понимания того, как эти нормы применяются к поведению государств и использованию государствами ИКТ. В докладе говорится, что с учетом уникальных особенностей ИКТ со временем могут быть разработаны дополнительные нормы.

Доклад отражает сделанный Группой вывод о том, что международное право, и в частности Устав Организации Объединенных Наций, применимо и имеет важное значение для поддержания мира и стабильности и создания открытой, безопасной, мирной и доступной информационной среды. Группа также пришла к выводу, что государственный суверенитет и международные нормы и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием ИКТ, а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории; государства должны выполнять свои международные обязательства в отношении приписываемых им международно противоправных деяний. В докладе содержатся рекомендации в отношении добровольных мер укрепления доверия и транспарентности, а также международного сотрудничества в сфере наращивания потенциала в области безопасности ИКТ, особенно в развивающихся странах. В соответствии с рекомендациями Группы регулярный институциональный диалог по этим вопросам под эгидой Организации Объединенных Наций, а также регулярный диалог в рамках других форумов будут способствовать повышению эффективности таких мер. Государства-члены должны внимательно изучить настоящий доклад и подумать над возможными путями доработки и осуществления указанных рекомендаций.

Предисловие Генерального секретаря

В настоящее время информационно-коммуникационные технологии (ИКТ) являются непременным атрибутом повседневной жизни.

И хотя все страны отдают должное значительным преимуществам ИКТ, получил широкое признание тезис о том, что неправильное использование таких технологий угрожает международному миру и безопасности.

В настоящем докладе содержатся разработанные Группой правительственных экспертов из 15 государств рекомендации по устранению связанных с использованием ИКТ существующих и потенциальных угроз со стороны государств, субъектов, действующих в их интересах, или негосударственных игроков. Настоящий доклад подготовлен на основе рекомендаций предыдущей группы экспертов, которые были приняты в 2010 году и включали в себя указание на необходимость дальнейшей проработки норм, регулирующих использование государствами ИКТ, способов повышения доверия и мер по укреплению потенциала.

Я с удовлетворением отмечаю, что в этом докладе подчеркивается ключевая роль Устава Организации Объединенных Наций и международного права, а также важность ответственного поведения государств. Содержащиеся в нем рекомендации указывают на то, как увязать вопросы безопасности ИКТ с существующими нормами международного права и договоренностями, которые регулируют межгосударственные отношения и служат основой для международного мира и безопасности.

Как отмечает Группа, Организация Объединенных Наций играет лидирующую роль в налаживании диалога между государствами-членами по проблеме безопасности в сфере использования ИКТ и в дальнейшем развитии международного сотрудничества в этой области.

Я благодарю Председателя Группы и экспертов за их добросовестный труд. Настоящий доклад станет прочной основой для будущих усилий по укреплению безопасности и стабильности в сфере использования ИКТ. Я передаюрекомендации Группы на рассмотрение Генеральной Ассамблее и считаю их важным шагом в направлении наращивания глобальных усилий по минимизации рисков, связанных с использованием ИКТ, и одновременному повышению их ценности.

Препроводительное письмо

7 июня 2013 года

Имею честь настоящим препроводить доклад Группы правительственных экспертов по достижениям в сфере информатизации и теле-

коммуникаций в контексте международной безопасности. Эта Группа была создана в 2012 году в соответствии с пунктом 4 резолюции 66/24 Генеральной Ассамблеи. В качестве Председателя Группы я с удовлетворением сообщаю Вам, что по этому докладу был достигнут консенсус.

В своей резолюции, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», Генеральная Ассамблея просила создать в 2012 году на основе справедливого географического распределения Группу правительственных экспертов, с тем чтобы продолжить исследование 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, а также концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем. Группе было также предложено принять во внимание оценки и рекомендации, содержащиеся в докладе предыдущей группы правительственных экспертов (A/65/201). К Генеральному секретарю была обращена просьба представить Генеральной Ассамблее на ее шестьдесят восьмой сессии доклад о результатах этого исследования.

В соответствии с положениями данной резолюции были назначены эксперты из 15 государств: Австралии, Аргентины, Беларуси, Германии, Египта, Индии, Индонезии, Канады, Китая, Российской Федерации, Соединенного Королевства Великобритании и Северной Ирландии, Соединенных Штатов Америки, Франции, Эстонии и Японии. Список экспертов приводится в приложении.

Группа провела всесторонний и углубленный обмен мнениями по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности. Всего Группа провела три сессии: первую сессию с 6 по 10 августа 2012 года в Центральных учреждениях Организации Объединенных Наций; вторую – с 14 по 18 января 2013 года в Женеве; третью – с 3 по 7 июня в Центральных учреждениях Организации Объединенных Наций.

Группа хотела бы выразить свою признательность за внесенный вклад Институту Организации Объединенных Наций по исследованию проблем разоружения, который консультировал Группу и от которого в ее работе участвовали Джеймс Льюис, Керстин Вигнард (на второй и третьей сессиях) и Бен Бейсли Уокер (на первой сессии). Группа хотела бы также выразить свою признательность сотруднику Управления

по вопросам разоружения Секретариата Юэну Бьюканану, который исполнял обязанности Секретаря Группы, и другим должностным лицам Секретариата, оказавшим содействие Группе.

Дебора Стоукс
Председатель Группы

I. Введение

1. Появление информационно-коммуникационных технологий (ИКТ) оказало существенное воздействие на положение дел в области международной безопасности. Эти технологии позволяют получать огромные экономические и социальные выгоды; они также могут использоваться в целях, несовместимых с поддержанием международного мира и безопасности. Уровень риска в последние годы заметно повысился в связи с использованием ИКТ для совершения преступлений и осуществления подрывной деятельности.

2. Международное сотрудничество является важным фактором снижения риска и укрепления безопасности. По этой причине Генеральная Ассамблея просила Генерального секретаря с помощью Группы правительственных экспертов продолжить изучение возможных совместных мер по устранению существующих и потенциальных угроз (резолюция 66/24) и представить доклад о результатах этой работы на шестьдесят восьмой сессии Ассамблеи. Настоящий доклад подготовлен на основе доклада 2010 года (A/65/201), подготовленного предыдущей группой правительственных экспертов, которая рассмотрела эту тему и вынесла рекомендации относительно дальнейшей работы.

3. В докладе 2010 года государствам было рекомендовано продолжать диалог в целях обсуждения норм, касающихся использования государствами ИКТ, уменьшения коллективного риска и защиты критически важной национальной и международной инфраструктуры. Группа призвала принимать меры по укреплению доверия, обеспечению стабильности и уменьшению риска, включая обмен национальными мнениями по вопросу об использовании ИКТ в конфликтах, и осуществлять обмен информацией о национальных законах, стратегиях обеспечения безопасности ИКТ, а также о соответствующих технологиях, принципах и передовых методах. В докладе 2010 года была подчеркнута важность создания потенциала в государствах, которым может потребоваться помощь в обеспечении безопасности их ИКТ, и было рекомендовано продолжить работу по выработке общей терминологии и определений.

4. Многочисленные двусторонние, региональные и многосторонние инициативы, осуществленные после 2010 года, свидетельствуют о том, что сейчас все большее значение придается укреплению безопасности при использовании ИКТ и самих ИКТ, снижению рисков для общественной безопасности, укреплению безопасности государств и упрочению глобальной стабильности. Все страны заинтересованы в поощрении использования ИКТ в мирных целях. Страны также заинтересованы в предотвращении конфликтов, возникающих в результате использования ИКТ. Общее понимание в отношении норм, правил и принципов, применимых к использованию ИКТ государствами, и добровольные меры укрепления доверия могут играть важную роль в поддержании мира и безопасности. Несмотря на то что деятельность международного сообщества по противодействию этой угрозе международному миру и безопасности находится на начальном этапе, тем не менее уже сейчас можно наметить для дальнейшего рассмотрения ряд мер, касающихся норм, правил и принципов ответственного поведения государств.

Угрозы, риски и факторы уязвимости

5. ИКТ являются технологиями двойного назначения, которые могут использоваться как в законных, так и в злонамеренных целях. Любое устройство ИКТ может стать источником или объектом злонамеренных действий. Злонамеренное использование ИКТ легко скрыть, а выявление конкретного злоумышленника может быть сопряжено с трудностями, в связи с чем злоумышленники, которые нередко действуют в условиях безнаказанности, могут осуществлять все более сложные вредоносные действия. Эту проблему также усугубляет глобальный охват сетей ИКТ. Глобальный доступ, уязвимые технологии и фактор анонимности облегчают использование ИКТ в целях осуществления подрывной деятельности.

6. Угрозы частным лицам, компаниям, национальной инфраструктуре и государственным органам приобретают все более острый характер, и соответствующие инциденты имеют все более тяжелые последствия. В качестве источников таких угроз выступают как государственные, так и негосударственные субъекты. Кроме того, отдельные лица, группы или организации, включая преступные сообщества, совершающие злонамеренные действия, связанные с использованием ИКТ, могут действовать в интересах государств. Возможность создания и широкомасштабного применения государствами или негосударственными

субъектами сложных вредоносных инструментов и средств – таких, например, как бот-сети – повышает риск ошибочной идентификации и непреднамеренной эскалации. Отсутствие общих представлений о приемлемом поведении государства в вопросах использования ИКТ ведет к усилению угрозы международному миру и безопасности.

7. Террористические группы используют ИКТ для поддержания контактов, сбора информации, вербовки сторонников, организации, планирования и координации террористических актов, пропаганды своих идей и действий и сбора финансовых средств. Если такие группы получат в свое распоряжение средства нападения, они смогут вести подрывную деятельность с помощью ИКТ.

8. Государства обеспокоены возможностью включения в ИКТ скрытых вредоносных функций, которые могут использоваться для подрыва безопасности и надежности использования ИКТ и всей системы производства и сбыта информационных товаров и информационно-технических услуг, а также для подрыва доверия между контрагентами в сфере торговли и причинения ущерба национальной безопасности.

9. Более широкое использование ИКТ на ключевых инфраструктурных объектах и в системах управления производственными процессами открывает новые возможности для подрывных действий. Стремительное расширение масштабов использования устройств мобильной связи, сетевых услуг, социальных сетей и услуг по обработке данных в удаленной среде расширяет круг проблем в сфере безопасности.

10. В условиях глобальной взаимосвязанности нашего мира неравенство возможностей государств в плане обеспечения безопасности ИКТ ведет к усилению уязвимости. Злоумышленники используют в своих целях слабозащищенные сети вне зависимости от их местоположения. Эту уязвимость усугубляют различия в национальном законодательстве, нормативных положениях и практических методах обеспечения безопасности ИКТ.

II. Укрепление сотрудничества в целях создания мирной, безопасной, устойчивой и открытой информационной среды

11. Государства-члены неоднократно заявляли о необходимости совместных действий, направленных на ликвидацию угроз, обусловленных злонамеренным использованием ИКТ. Чтобы добиться новых успехов в деле развития сотрудничества на международном уровне, необходимо осуществить комплекс мер, направленных на создание мирной, безопасной, открытой и основанной на сотрудничестве ин-

формационной среды. Необходимо рассмотреть совместные меры по укреплению международного мира, стабильности и безопасности. Такие меры включают выработку общего понимания в отношении применения соответствующих норм международного права и вытекающих из них норм, правил и принципов ответственного поведения государств.

12. Государства должны играть лидирующую роль в решении указанных вопросов, вместе с тем активное участие частного сектора и гражданского общества могло бы способствовать повышению эффективности сотрудничества.

13. Организация Объединенных Наций должна играть ведущую роль в поощрении диалога между государствами-членами для выработки общего понимания в отношении безопасности при использовании ИКТ и самих ИКТ, поощрять региональные усилия, меры по укреплению доверия и повышению транспарентности, а также способствовать наращиванию потенциала и распространению передового опыта.

14. В дополнение к работе, проводимой в рамках системы Организации Объединенных Наций, ценные усилия прилагают такие международные организации и региональные структуры, как Африканский союз, Региональный форум Ассоциации государств Юго-Восточной Азии (АСЕАН), Азиатско-Тихоокеанский форум экономического сотрудничества, Совет Европы, Экономическое сообщество западноафриканских государств (ЭКОВАС), Европейский союз, Лига арабских государств, Организация американских государств (ОАГ), Организация по безопасности и сотрудничеству в Европе (ОБСЕ) и Шанхайская организация сотрудничества. В будущем работа по вопросам безопасности в сфере использовании ИКТ должна вестись с учетом этих усилий.

15. Признавая всеобъемлющий характер данной проблемы, учитывая существующие и потенциальные угрозы, риски и факторы уязвимости и руководствуясь оценками и рекомендациями, содержащимися в опубликованном в июле 2010 года докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/65/201), Группа рекомендует следующие меры.

III. Рекомендации в отношении норм, правил и принципов ответственного поведения государств

16. Применение норм, основанных на положениях международного права, в отношении деятельности государств, связанной с использова-

нием ИКТ, – необходимая предпосылка для снижения риска нарушения международного мира, безопасности и стабильности. Необходимо продолжать исследования для выработки общего понимания того, как эти нормы применяются к поведению государств и использованию государствами ИКТ. С учетом уникальных особенностей ИКТ со временем могут быть разработаны дополнительные нормы.

17. Группа рассмотрела мнения и оценки государств-членов относительно достижений в сфере информатизации и телекоммуникаций в контексте международной безопасности, которые были представлены по просьбе Генеральной Ассамблеи, изложенной в ее резолюциях 64/25, 65/41 и 66/24, а также другие меры, предусмотренные в резолюциях 55/63, 56/121, 57/239, 58/199 и 64/211.

18. Группа отметила документ A/66/359, распространенный Генеральным секретарем по просьбе постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана и содержащий проект правил поведения в области обеспечения международной информационной безопасности, к числу авторов которого впоследствии присоединились Казахстан и Кыргызстан.

19. Международное право, и в частности Устав Организации Объединенных Наций, применимо и имеет важное значение для поддержания мира и стабильности и создания открытой, безопасной, мирной и доступной информационной среды.

20. Государственный суверенитет и международные нормы и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием ИКТ, а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории.

21. Предпринимаемые государством усилия по обеспечению безопасности ИКТ должны гармонично сочетаться с уважением прав человека и основных свобод, закрепленных во Всеобщей декларации прав человека и других международных инструментах.

22. Государства должны активизировать сотрудничество в борьбе с использованием ИКТ в преступных или террористических целях, надлежащим образом согласовывать свои правовые подходы и развивать практическое сотрудничество между соответствующими правоохранительными органами и органами прокуратуры.

23. Государства должны выполнять свои международные обязательства в отношении приписываемых им международно противоправных деяний. Государства не должны использовать посредников для совершения международно противоправных деяний. Государства должны

стремиться не допускать того, чтобы негосударственные субъекты использовали их территорию для применения ИКТ в незаконных целях.

24. Государствам следует содействовать тому, чтобы частный сектор и гражданское общество играли надлежащую роль в укреплении безопасности при использовании ИКТ и самих ИКТ, включая безопасность всей системы производства и сбыта информационных товаров и информационно-технических услуг.

25. Государствам-членам следует изыскивать оптимальные формы сотрудничества в области осуществления вышеупомянутых норм и принципов ответственного поведения с учетом потенциальной роли частного сектора и организаций гражданского общества. Эти нормы и принципы дополняют усилия Организации Объединенных Наций и региональных групп и служат основой для дальнейшей работы по укреплению доверия и взаимопонимания.

IV. Рекомендации в отношении мер укрепления доверия и обмена информацией

26. Добровольные меры укрепления доверия могут способствовать установлению доверительных отношений между государствами и повышению степени доверия, а также уменьшают риск возникновения конфликтов благодаря обеспечению большей предсказуемости и снижению вероятности возникновения недопонимания. Они могут внести ценный вклад в решение вызывающих озабоченность государств проблем в связи с использованием ИКТ и стать важным шагом на пути к укреплению международной безопасности. Государствам следует рассмотреть вопрос о разработке, в частности, следующих практических мер по укреплению доверия для повышения транспарентности, обеспечения большей предсказуемости и развития сотрудничества:

a) добровольный обмен мнениями и информацией о национальных стратегиях и политике, передовом опыте, процессах принятия решений, соответствующих национальных организациях и мерах, направленных на развитие международного сотрудничества. Степень подробности такой информации будет определяться предоставляющими государствами. Обмен такой информацией может осуществляться на двусторонней основе, в рамках региональных групп или на других международных форумах;

b) создание двусторонних, региональных и многосторонних консультативных рамок для укрепления доверия, в частности проведение практикумов, семинаров и других учебных мероприятий, в целях

содействия рассмотрению на национальном уровне вопросов о том, каким образом можно предотвратить деструктивные инциденты с использованием ИКТ, каким образом эти инциденты могут возникать и как им можно противодействовать;

c) улучшение обмена информацией между государствами об инцидентах, связанных с безопасностью ИКТ, посредством более эффективного использования существующих каналов или создания соответствующих новых каналов и механизмов для получения, сбора, анализа и распространения информации об инцидентах, связанных с использованием ИКТ, для своевременного реагирования на такие инциденты и осуществления мероприятий по устранению и смягчению последствий. Государствам следует рассмотреть возможность обмена информацией о национальных контактных центрах для расширения и улучшения существующих каналов связи, предназначенных для использования в целях управления в кризисных ситуациях, а также рассмотреть возможность оказания содействия усилиям по созданию или укреплению механизмов раннего предупреждения;

d) двусторонний обмен информацией и налаживание взаимодействия между национальными группами экстренной готовности к компьютерным инцидентам, а также в рамках объединений таких групп и на других форумах в целях поддержания диалога на политическом и стратегическом уровнях;

e) расширение сотрудничества в деле противодействия инцидентам, которые могут затронуть инфраструктуру ИКТ или объекты критической инфраструктуры, где используются системы управления производственными процессами на основе ИКТ. Сюда могут входить разработка руководящих принципов и налаживание обмена передовым опытом между государствами по противодействию злонамеренным действиям, совершаемым негосударственными субъектами;

f) совершенствование механизмов сотрудничества правоохранительных органов для сокращения числа инцидентов, которые могли бы быть неверно истолкованы как враждебные действия со стороны государств, в целях укрепления международной безопасности.

27. Эти первоначальные меры укрепления доверия, позволяющие приобрести практический опыт, могут стать важным ориентиром для определения направлений будущей работы. Государствам следует содействовать закреплению и развитию прогресса, достигнутого на двустороннем и многостороннем уровнях, в том числе в рамках таких региональных групп, как Африканский союз, Региональный форум АСЕАН, Европейский союз, Лига арабских государств, Орга-

низация американских государств, ОБСЕ, Шанхайская организация сотрудничества и др. Опираясь на результаты этих усилий, государства должны содействовать обеспечению взаимодополняемости мер и распространению передового опыта с учетом специфики конкретных стран и регионов.

28. Государства должны играть лидирующую роль в разработке мер укрепления доверия, вместе с тем активное участие частного сектора и гражданского общества могло бы способствовать повышению эффективности таких усилий.

29. Учитывая темпы развития ИКТ и масштабы угрозы, Группа считает, что необходимо способствовать углублению общего понимания и активизации практического сотрудничества. В этой связи она рекомендует поддерживать регулярный институциональный диалог с широким кругом участников под эгидой Организации Объединенных Наций, а также регулярный диалог в рамках двусторонних, региональных и многосторонних форумов и других международных организаций.

V. Рекомендации в отношении мер по наращиванию потенциала

30. Решающим фактором повышения эффективности глобальных совместных усилий по обеспечению безопасности при использовании ИКТ и самих ИКТ является наращивание потенциала. Некоторым государствам может потребоваться помощь в связи с их усилиями по укреплению безопасности критически важной инфраструктуры ИКТ, развитию технических навыков и разработке соответствующего законодательства, стратегий и нормативно-правовой базы для того, чтобы они могли выполнить свои обязанности, а также преодолеть разрыв в уровне потенциала в области безопасности при использовании ИКТ и самих ИКТ.

31. В этой связи государствам, сотрудничающим с международными организациями, в том числе с учреждениями Организацией Объединенных Наций, и частному сектору следует рассмотреть наиболее эффективные способы оказания технической и иной помощи в целях наращивания потенциала в области безопасности при использовании ИКТ и самих ИКТ тем странам, который нуждаются в такой помощи, в особенности развивающимся государствам.

32. Опираясь на результаты работы по осуществлению ранее принятых резолюций, в частности резолюции 64/211, и положений ранее опубликованных докладов Организации Объединенных Наций по воп-

росам наращивания потенциала, государства должны рассмотреть возможность принятия следующих мер:

a) оказание поддержки двусторонним, региональным, многосторонним и международным мерам по наращиванию потенциала в целях обеспечения безопасного использования ИКТ и обеспечения безопасности ИКТ-инфраструктуры; развитие национальной правовой базы, укрепление потенциала правоохранительных органов и обеспечение эффективного осуществления принятых стратегий; борьба с использованием ИКТ в преступных и террористических целях; а также оказание помощи в выявлении и распространении передового опыта;

b) создание и укрепление потенциала реагирования на инциденты, в том числе групп экстренной готовности к компьютерным инцидентам, а также налаживание более тесного сотрудничества между такими группами;

c) содействие развитию и использованию электронных средств обучения, профессиональная подготовка и повышение осведомленности в вопросах безопасности ИКТ для преодоления «цифрового разрыва» и оказания развивающимся странам помощи, необходимой для непрерывного получения информации об изменениях международной стратегии;

d) расширение сотрудничества и передача знаний и технологий для предупреждения инцидентов, касающихся безопасности ИКТ, и ликвидации их последствий, особенно в интересах развивающихся стран;

e) оказание содействия научно-исследовательским институтам и университетам, с тем чтобы они продолжали работать над проблемами обеспечения безопасности ИКТ. С учетом возложенных на такие учреждения конкретных задач по оказанию поддержки государствам-членам и международному сообществу государствам следует рассмотреть вопрос о том, каким образом соответствующие научно-исследовательские и учебные институты Организации Объединенных Наций могли бы внести свой вклад в этом отношении.

33. Группа признала, что прогресс в отношении обеспечения безопасности использования ИКТ, в частности за счет поддержки усилий по созданию потенциала, будет также способствовать достижению восьмой цели в области развития, сформулированной в Декларации тысячелетия («Формирование глобального партнерства в целях развития»).

VI. Заключение

34. Прогресс в области обеспечения международной безопасности при использовании государствами ИКТ будет носить итеративный

характер: каждый шаг основывается на уже достигнутых результатах. Необходимость такого подхода диктуется тем, что развитие технологического пространства происходит под воздействием постоянных изменений и неуклонного увеличения численности пользователей ИКТ. В настоящем докладе содержатся рекомендации, которые основываются на результатах ранее проделанной работы. Их осуществление и доработка будут способствовать укреплению доверия между всеми участниками. Группа рекомендует государствам-членам внимательно изучить настоящий доклад и подумать над возможными путями доработки и осуществления этих рекомендаций.

Приложение

Список членов Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Аргентина
Посол Альфредо Морелли
Координатор, Отдел энергетики и технологий
Министерства иностранных дел и по делам культов, Буэнос-Айрес

Австралия
Г-жа Дебора Стоукс
Первый помощник секретаря,
Министерство иностранных дел и торговли, Канберра

Беларусь
Г-н Владимир Н. Герасимович
Начальник Управления международной безопасности и контроля над вооружениями
Министерства иностранных дел, Минск

Канада
Г-н Майкл Валма
Директор Отдела политического планирования
Министерства иностранных дел и международной торговли, Оттава

Китай
Г-н Лэй Ван (на первой и второй сессиях)
Директор Департамента контроля над вооружениями и разоружения
Министерства иностранных дел, Пекин
Г-жа Чжихуа Дун (на третьей сессии)
Советник Департамента контроля над вооружениями и разоружения
Министерства иностранных дел, Пекин

Египет
Д-р Шериф Хашим
Старший советник по кибербезопасности при Министре коммуникаций и информационных технологий,
Министерство коммуникаций и информационных технологий, Каир

Эстония
Г-н Линнар Вик
Исполняющий обязанности директора
Эстонского информационно-технологического колледжа, Таллинн

Франция
Г-н Жан-Франсуа Бларель
Заместитель генерального секретаря, координатор по вопросам киберпространства,
Министерство иностранных дел, Париж

Германия
Г-н Детлеф Вольтер
Начальник Управления контроля над обычными вооружениями и по вопросам мер доверия и укрепления безопасности
Федерального министерства иностранных дел, Берлин

Индия
Г-н Харш К. Джайн
Общий секретарь и руководитель Отдела электронного управления и информационных технологий
Министерства иностранных дел, Нью-Дели

Индонезия
Г-н Фебриан Руддьярд (на первой сессии)
Директор по вопросам международной безопасности и разоружения,
Министерство иностранных дел, Джакарта
Г-н Анди Рахмианто (на третьей сессии)
Советник-посланник,
Постоянное представительство Индонезии при Организации Объединенных Наций, Нью-Йорк

Япония
Посол Тамоцу Шиноцука (на первой сессии)
Отдел международного сотрудничества в борьбе с терроризмом и международной организованной преступностью и по вопросам киберполитики,
Министерство иностранных дел, Токио
Посол Осаму Имаи (на второй и третьей сессиях)
Отдел международного сотрудничества в борьбе с терроризмом и международной организованной преступностью и по вопросам киберполитики,
Министерство иностранных дел, Токио

Российская Федерация
Г-н Андрей В. Крутских
Специальный координатор по вопросам политического использования ИКТ,
Посол по особым поручениям,
Министерство иностранных дел, Москва

Соединенное Королевство Великобритании и Северной Ирландии
Г-н Николас Хейкок
Помощник директора по международной безопасности,
Управление кибербезопасности и обеспечения сохранности информации, секретариат Кабинета министров, Лондон

Соединенные Штаты Америки
Г-жа Мишель Маркофф
Заместитель координатора по вопросам киберпространства,
Канцелярия Государственного секретаря, государственный департамент Соединенных Штатов Америки, Вашингтон, округ Колумбия

4.2. Международный союз электросвязи (МСЭ) *(International Telecommunication Union, ITU)*

РЕГЛАМЕНТ МЕЖДУНАРОДНОЙ ЭЛЕКТРОСВЯЗИ[1]

(Дубай, 14 декабря 2012 г.)

Преамбула

При полном признании за каждым государством суверенного права регламентировать свою электросвязь, положения настоящего Регламента международной электросвязи (далее именуемого «Регламент») дополняют Устав и Конвенцию Международного союза электросвязи в интересах достижения целей Международного союза электросвязи в деле содействия развитию услуг электросвязи, их наиболее эффективного использования и обеспечения гармоничного развития средств электросвязи во всемирном масштабе.

Государства-Члены подтверждают свою готовность выполнять настоящий Регламент способом, обеспечивающим уважение и соблюдение своих обязательств в отношении прав человека.

В настоящем Регламенте признается право Государств-Членов на доступ к услугам международной электросвязи.

Статья 1
Цель и область применения Регламента

1.1. *a*) В настоящем Регламенте устанавливаются общие принципы, касающиеся оказания и обеспечения услуг международной электросвязи, предоставляемых населению, а также основных средств передачи международной электросвязи, используемых для оказания таких услуг. Настоящий Регламент не затрагивает аспекты электросвязи, относящиеся к контенту.

b) В настоящем Регламенте также содержатся положения, применимые к тем эксплуатационным организациям, которые уполномочены или признаны Государством Членом для организации и обеспечения услуг международной электросвязи и участия в их оказании населению, далее именуемым «уполномоченные эксплуатационные организации».

c) В Статье 13 настоящего Регламента признается право Государств-Членов разрешать заключение специальных соглашений.

[1] Регламент международной электросвязи (РМЭ) и Дополнения к нему приняты Всемирной конференцией по международной электросвязи (Дубай, 2012 г.). – URL: http://www.itu.int/ru/wcit-12/Pages/itrs.aspx

1.2. В настоящем Регламенте термин «население» используется в значении населения в целом, включая правительственные органы и юридические лица.

1.3. Настоящий Регламент разработан с целью способствовать присоединению и функциональной совместимости средств электросвязи в глобальном масштабе и содействовать гармоничному развитию и эффективной эксплуатации технических средств, а также эффективности, полезности и доступности услуг международной электросвязи для населения.

1.4. Ссылки в настоящем Регламенте на Рекомендации Сектора стандартизации электросвязи МСЭ (МСЭ-Т) не означают, что эти Рекомендации имеют такой же юридический статус, как и настоящий Регламент.

1.5. В рамках настоящего Регламента оказание и обеспечение услуг международной электросвязи осуществляются на каждой взаимосвязи по взаимному соглашению между уполномоченными эксплуатационными организациями.

1.6. При применении принципов настоящего Регламента, уполномоченным эксплуатационным организациям следует соблюдать, в максимально возможной степени, соответствующие Рекомендации МСЭ-Т.

1.7. *a*) В настоящем Регламенте признается за каждым Государством-Членом, в зависимости от его национального законодательства и если оно так решит, право потребовать, чтобы уполномоченные эксплуатационные организации, которые действуют на его территории и оказывают населению услуги международной электросвязи, были уполномочены на это Государством-Членом.

b) Заинтересованное Государство-Член должно, в соответствующих случаях, настоятельно рекомендовать поставщикам таких услуг применять соответствующие Рекомендации МСЭ-Т.

c) Государства-Члены, при необходимости, должны сотрудничать в выполнении настоящего Регламента.

1.8. Настоящий Регламент должен применяться вне зависимости от используемых средств передачи, если в Регламенте радиосвязи не указано иное.

Статья 2
Определения

2.1. Для целей настоящего Регламента должны применяться приведенные ниже определения. Однако для других целей применение этих терминов и определений необязательно.

2.2. Электросвязь: Любая передача, излучение или прием знаков, сигналов, письменного текста, изображений и звуков или сообщений любого рода по проводной, радио, оптической или другим электромагнитным системам.

2.3. Услуга международной электросвязи: Предоставление электросвязи между предприятиями или станциями электросвязи любого типа, находящимися в разных странах или принадлежащими разным странам.

2.4. Правительственная электросвязь: Сообщения электросвязи, исходящие от: главы государства; главы правительства или членов правительства; главнокомандующих вооруженными силами, сухопутными войсками, морским флотом или воздушными силами; дипломатических или консульских представителей; Генерального секретаря Организации Объединенных Наций; руководителей основных органов Организации Объединенных Наций; Международного суда, или ответы на упомянутые выше сообщения правительственной электросвязи.

2.5. Служебная электросвязь: Электросвязь, относящаяся к международной электросвязи общего пользования и осуществляемая между:

– Государствами-Членами;

– уполномоченными эксплуатационными организациями; и

– Председателем Совета, Генеральным секретарем, заместителем Генерального секретаря, Директорами Бюро, членами Радиорегламентарного комитета, другими представителями или уполномоченными должностными лицами Союза, включая тех, которые выполняют официальную миссию за пределами местопребывания Союза.

2.6. Международный маршрут: Технические средства и сооружения, расположенные в различных странах и используемые для передачи трафика электросвязи между двумя международными оконечными станциями или предприятиями электросвязи.

2.7 Взаимосвязь: Обмен трафиком между двумя оконечными странами, всегда относящийся к какой-либо конкретной услуге, если между их уполномоченными эксплуатационными организациями имеются:

a) средства для обмена трафиком в этой конкретной услуге:

– по прямым каналам (прямая взаимосвязь), или

– через транзитный пункт какой-либо третьей страны (непрямая взаимосвязь), и

b) как правило, взаиморасчеты.

2.8. Расчетная такса: Такса, применяемая при данной взаимосвязи по согласованию между уполномоченными эксплуатационными организациями и используемая для выставления международных счетов.

2.9. Взимаемая плата: Плата, устанавливаемая и взимаемая уполномоченной эксплуатационной организацией со своих клиентов за использование услуг международной электросвязи.

Статья 3
Международная сеть

3.1. Государства-Члены должны стремиться обеспечивать сотрудничество уполномоченных эксплуатационных организаций по созданию, эксплуатации и техническому обслуживанию международной сети для обеспечения удовлетворительного качества обслуживания.

3.2. Государства-Члены должны стремиться обеспечивать предоставление достаточных средств электросвязи для удовлетворения потребностей в услугах международной электросвязи.

3.3. Уполномоченные эксплуатационные организации должны по взаимному соглашению определять, какие международные маршруты должны быть использованы. В ожидании заключения соглашения и при условии, что между заинтересованными оконечными уполномоченными эксплуатационными организациями не существует прямого маршрута, уполномоченная эксплуатационная организация исходящего вызова имеет право выбирать маршрут своего исходящего трафика электросвязи, принимая во внимание интересы соответствующих транзитных уполномоченных эксплуатационных организаций и уполномоченной эксплуатационной организации назначения.

3.4. В зависимости от национального законодательства любой пользователь, у которого есть доступ к международной сети, имеет право передавать трафик. Удовлетворительное качество обслуживания следует, в максимально возможной степени, поддерживать согласно соответствующим Рекомендациям МСЭ-Т.

3.5. Государства-Члены должны стремиться обеспечивать, чтобы международные ресурсы нумерации международной электросвязи, определенные в Рекомендациях МСЭ-Т, использовались только теми, кому они присвоены, и только в целях, для которых они присвоены, и чтобы не присвоенные ресурсы не использовались.

3.6. Государства-Члены должны стремиться обеспечивать предоставление информации международной идентификации линии вызывающего абонента (ИЛВА) с учетом соответствующих Рекомендаций МСЭ-Т.

3.7. Государствам-Членам следует создать благоприятную среду для внедрения региональных пунктов обмена трафиком электросвязи

в целях повышения качества, расширения возможности установления соединений, повышения устойчивости сетей, стимулирования конкуренции и уменьшения стоимости присоединений в международной электросвязи.

Статья 4
Услуги международной электросвязи

4.1. Государства-Члены должны содействовать развитию услуг международной электросвязи и должны способствовать их доступности для населения.

4.2. Государства-Члены должны стремиться обеспечивать, чтобы уполномоченные эксплуатационные организации сотрудничали в рамках настоящего Регламента для оказания по взаимному соглашению широкого спектра услуг международной электросвязи, которые должны отвечать, в максимально возможной степени, соответствующим Рекомендациям МСЭ-Т.

4.3. В зависимости от национального законодательства Государства-Члены должны стремиться обеспечивать, чтобы уполномоченные эксплуатационные организации предоставляли и поддерживали, в максимально возможной степени, удовлетворительное качество обслуживания, отвечающее соответствующим Рекомендациям МСЭ-Тв отношении:

a) доступа к международной сети со стороны пользователей, использующих оконечные устройства, которые разрешается подключать к этой сети и которые не причиняют вреда техническим средствам и персоналу;

b) средств и услуг международной электросвязи, предоставляемых пользователям для их целевого использования;

c) по крайней мере какого-либо одного вида услуги электросвязи, который является в достаточной мере доступным для населения, в том числе для тех, кто может и не быть абонентом какой-либо конкретной услуги электросвязи; и

d) возможности совместного функционирования, при необходимости, различных услуг для содействия пользованию услугами международной электросвязи.

4.4. Государства-Члены должны способствовать принятию мер по обеспечению того, чтобы уполномоченные эксплуатационные организации своевременно и бесплатно предоставляли конечным пользователям прозрачную, обновленную и точную информацию об услугах

международной электросвязи, в том числе о ценах на международный роуминг и соответствующих связанных с ними условиях.

4.5. Государства-Члены должны способствовать принятию мер по обеспечению того, чтобы услуги электросвязи при нахождении в международном роуминге предоставлялись приезжающим пользователям с удовлетворительным уровнем качества.

4.6. Государствам-Членам следует способствовать сотрудничеству между уполномоченными эксплуатационными организациями, с тем чтобы избегать начисления платы за непреднамеренный роуминг в приграничных областях и смягчать его последствия.

4.7. Государства-Члены должны стремиться содействовать конкуренции при оказании услуг международного роуминга, и им настоятельно рекомендуется разрабатывать стратегии, которые способствуют установлению конкурентоспособных цен на роуминг в интересах конечных пользователей.

Статья 5
Безопасность человеческой жизни и приоритеты электросвязи

5.1. Электросвязь, относящаяся к безопасности человеческой жизни, такая как электросвязь в случае бедствий, должна иметь неотъемлемое право передачи сообщений и там, где это технически возможно, должна пользоваться абсолютным приоритетом по отношению ко всем другим видам электросвязи согласно соответствующим Статьям Устава и Конвенции и с надлежащим учетом соответствующих Рекомендаций МСЭ-Т.

5.2. Правительственная электросвязь, включая сообщения электросвязи, относящиеся к применению некоторых положений Устава Организации Объединенных Наций, там, где это технически возможно, должна пользоваться приоритетом по отношению ко всем другим видам электросвязи, кроме тех, которые указаны в п. 39 (5.1), выше, согласно соответствующим положениям Устава и Конвенции и с надлежащим учетом соответствующих Рекомендаций МСЭ-Т.

5.3. Положения, регламентирующие приоритет любых других услуг электросвязи, содержатся в соответствующих Рекомендациях МСЭ-Т.

5.4. Государствам-Членам следует настоятельно рекомендовать уполномоченным эксплуатационным организациям своевременно и бесплатно сообщать всем пользователям, в том числе при нахождении в роуминге, номер, который должен использоваться для вызова экстренных оперативных служб.

Статья 6
Безопасность и устойчивость сетей

6.1. Государства-Члены, по отдельности и совместно, должны стремиться обеспечивать безопасность и устойчивость сетей международной электросвязи, с тем чтобы добиваться их эффективного использования и непричинения им технического вреда, а также согласованного развития услуг международной электросвязи, предлагаемых населению.

Статья 7
Незапрашиваемые массовые электронные сообщения

7.1. Государствам-Членам следует стремиться принимать необходимые меры для предотвращения распространения незапрашиваемых массовых электронных сообщений и для сведения к минимуму их воздействия на услуги международной электросвязи.

7.2. Государствам-Членам настоятельно рекомендуется сотрудничать в этой области.

Статья 8
Тарификация и расчеты

8.1 Соглашения о международной электросвязи

8.1.1. В соответствии с применимым национальным законодательством условия договоренностей об оказании услуг международной электросвязи могут достигаться с помощью коммерческих соглашений или принципов установления расчетных такс, разработанных согласно национальным нормам.

8.1.2. Государства-Члены должны стремиться содействовать инвестициям в сети международной электросвязи и способствовать установлению конкурентных оптовых цен на трафик, передаваемый по таким сетям электросвязи.

8.2. Принципы установления расчетных такс

Условия

8.2.1. Следующие положения могут применяться, когда условия договоренностей об оказании услуг международной электросвязи определяются с помощью принципов установления расчетных такс, разработанных согласно национальным нормам. Эти положения не применяются к договоренностям, достигаемым с помощью коммерческих соглашений.

8.2.2. Для каждой применяемой при данной взаимосвязи услуги уполномоченные эксплуатационные организации по взаимному соглашению должны устанавливать и пересматривать расчетные таксы, которые применяются между ними, в соответствии с положениями Дополнения 1 и с учетом соответствующих Рекомендаций МСЭ-Т.

8.2.3. Если не имеется других соглашений, стороны, участвующие в оказании услуг международной электросвязи, должны соблюдать соответствующие положения, указанные в Дополнениях 1 и 2.

8.2.4. В отсутствие специальных соглашений, заключаемых между уполномоченными эксплуатационными организациями, денежной единицей, используемой при определении расчетных такс за услуги международной электросвязи и при выставлении международных счетов, должны быть:

– либо денежная единица Международного валютного фонда (МВФ), в настоящее время определенная этой организацией как специальные права заимствования (СПЗ);

– либо свободно конвертируемая валюта или иная денежная единица, согласованная между уполномоченными эксплуатационными организациями.

Взимаемые платы

8.2.5. Плата, взимаемая с клиентов за какую-либо определенную услугу, в принципе должна быть одинаковой при данной взаимосвязи независимо от международного маршрута, использованного для данной услуги. При установлении такой платы Государствам-Членам следует пытаться избегать разницы между платами, взимаемыми на каждом из направлений однойи той же взаимосвязи.

8.3. Налогообложение

8.3.1. Если в соответствии с национальным законодательством какой-либо страны предусматривается налог на взимание платы за услуги международной электросвязи, то этим налогом облагаются, как правило, только те услуги международной электросвязи, счета за которые выставляются клиентам в этой стране, если отсутствуют другие договоренности, заключаемые для конкретных специальных случаев.

8.4. Служебная электросвязь

8.4.1. Уполномоченные эксплуатационные организации могут в принципе отказываться от включения служебной электросвязи в меж-

дународные расчеты согласно соответствующим положениям Устава и Конвенции Международного союза электросвязи и настоящего Регламента и с надлежащим учетом необходимости заключения взаимных договоренностей. Уполномоченные эксплуатационные организации могут предоставлять служебную электросвязь бесплатно.

8.4.2. Общие принципы эксплуатации, тарификации и расчетов, применяемые к служебной электросвязи, должны учитывать соответствующие Рекомендации МСЭ-Т.

Статья 9
Временное прекращение оказания услуг

9.1. Если в соответствии с Уставом и Конвенцией Государство-Член использует свое право частично или полностью временно прекратить оказание услуг международной электросвязи, это Государство-Член должно немедленно уведомить Генерального секретаря о временном прекращении и о последующем восстановлении нормального режима работы, используя наиболее подходящие средства связи.

9.2. Генеральный секретарь должен немедленно довести эту информацию до сведения всех других Государств-Членов, используя наиболее подходящие средства связи.

Статья 10
Распространение информации

10.1. Генеральный секретарь, используя наиболее подходящие и экономичные средства, должен распространять предоставляемую информацию административного, эксплуатационного или статистического характера, касающуюся услуг международной электросвязи. Такая информация должна распространяться согласно соответствующим положениям Устава, Конвенции и настоящей Статьи на основе решений, принятых Советом или компетентными конференциями МСЭ, и с учетом выводов или решений ассамблей МСЭ. Если это санкционировано заинтересованным Государством-Членом, информация может быть передана Генеральному секретарю непосредственно уполномоченной эксплуатационной организацией, а затем должна распространяться Генеральным секретарем. Государствам-Членам следует своевременно передавать такую информацию Генеральному секретарю с учетом соответствующих Рекомендаций МСЭ-Т.

Статья 11
Энергоэффективность/электронные отходы

11.1. Государствам-Членам настоятельно рекомендуется применять передовой опыт в области энергоэффективности и электронных отходов с учетом соответствующих Рекомендаций МСЭ-Т.

Статья 12
Доступность

12.1 Государствам-Членам следует содействовать доступу лицам с ограниченными возможностями к услугам международной электросвязи с учетом соответствующих Рекомендаций МСЭ-Т.

Статья 13
Специальные соглашения

13.1. *a*) В соответствии со Статьей 42 Устава могут быть заключены специальные соглашения по вопросам электросвязи, которые не касаются Государств-Членов в целом. В зависимости от национального законодательства Государства-Члены могут разрешать уполномоченным эксплуатационным организациям или другим организациям или лицам заключать такие специальные взаимные соглашения с Государствами-Членами и уполномоченными эксплуатационными организациями, либо другими организациями или лицами, имеющими на это разрешение в другой стране для организации, эксплуатации и использования специальных сетей, систем и услуг международной электросвязи с целью удовлетворения особых потребностей в международной электросвязи на территориях или между территориями заинтересованных Государств-Членов; эти соглашения могут включать, если необходимо, финансовые, технические или эксплуатационные условия, которые следует соблюдать.

b) Любое из таких специальных соглашений должно стремиться не причинять технический вред эксплуатации средств электросвязи третьих стран.

13.2. Государствам-Членам следует, при необходимости, постоянно рекомендовать сторонам любых специальных соглашений, заключенных в соответствии с п. 58 (9.1), выше, учитывать соответствующие положения Рекомендаций МСЭ-Т.

Статья 14
Заключительные положения

14.1. Настоящий Регламент, неотъемлемой частью которого являются Дополнения 1 и 2, должен вступить в силу 1 января 2015 года и должен применяться с этой даты в соответствии со всеми положениями Статьи 54 Устава.

14.2. Если какое-либо Государство-Член сделает оговорки в отношении применения одного или нескольких положений настоящего Регламента, другие Государства-Члены могут не соблюдать это положение или эти положения в своих отношениях с Государством-Членом, которое сделало такие оговорки.

В УДОСТОВЕРЕНИЕ ЧЕГО делегаты Государств – Членов Международного союза электросвязи, указанные ниже, от имени своих соответствующих компетентных властей подписали один экземпляр настоящих Заключительных актов на английском, арабском, испанском, китайском, русском и французском языках. В случае расхождений или разногласия преимущественную силу имеет французский текст. Этот экземпляр будет депонирован в архивы Союза. Генеральный секретарь должен направить одну заверенную копию каждому Государству – Члену Международного союза электросвязи.

Совершено в Дубае, 14 декабря 2012 года

Дополнение 1
ОБЩИЕ ПОЛОЖЕНИЯ,
КАСАЮЩИЕСЯ РАСЧЕТОВ

1. Расчетные таксы

1.1. Для каждой применяемой при данной взаимосвязи услуги Государства-Члены должны стремиться обеспечивать, чтобы уполномоченные эксплуатационные организации по взаимному соглашению устанавливали и пересматривали расчетные таксы, применяемые ими с учетом Рекомендаций МСЭ-Т и в зависимости от действительных затрат по оказанию конкретной услуги электросвязи, и делили их на оконечные доли, причитающиеся уполномоченным эксплуатационным организациям оконечных стран, и в надлежащих случаях на транзитные доли, причитающиеся уполномоченным эксплуатационным организациям транзитных стран.

1.2. С другой стороны, при взаимосвязях на базе трафика, где в качестве основы могут использоваться результаты исследований затрат, проведенных МСЭ-Т, расчетная такса может определяться в соответствии со следующим методом:

a) уполномоченные эксплуатационные организации должны устанавливать и пересматривать свои оконечные и транзитные доли с учетом Рекомендаций МСЭ-Т;

b) расчетная такса должна быть суммой оконечных долей и любых транзитных долей.

1.3. Если одна или несколько уполномоченных эксплуатационных организаций либо на возмездной основе в виде фиксированной платы, либо любым другим способом получают право на использование части каналов и/или оборудования другой уполномоченной эксплуатационной организации, то они имеют право устанавливать размеры своей доли за использование этой части взаимосвязи в соответствии с положениями пунктов 1.1 и 1.2, указанными выше.

1.4. В случаях, когда по соглашению между уполномоченными эксплуатационными организациями установлены один или несколько международных маршрутов, а трафик в одностороннем порядке направлен уполномоченной эксплуатационной организацией исходящего вызова по международному маршруту, который не был согласован с уполномоченной эксплуатационной организацией назначения, оконечные доли, причитающиеся уполномоченной эксплуатационной организации назначения, должны быть такими же, как если бы трафик был направлен по первому согласованному маршруту, а затраты по транзиту несла уполномоченная эксплуатационная организация исходящего вызова, кроме тех случаев, когда уполномоченная эксплуатационная организация назначения готова согласиться на другую долю.

1.5. В тех случаях, когда трафик направлен через транзитный пункт без разрешения и/или согласования транзитной доли, транзитная уполномоченная эксплуатационная организация имеет право установить уровень транзитной доли для включения в международные счета.

1.6. Если с уполномоченной эксплуатационной организации взимается налог или сбор с ее долей расчетной таксы или других выплат, то она не должна, в свою очередь, взимать какие бы то ни было подобные налоги или сборы с других уполномоченных эксплуатационных организаций.

2. Выставление счетов 1/11

2.1. Если иное не оговорено, уполномоченные эксплуатационные организации, ответственные за сбор платы, должны выставлять ме-

сячные счета с указанием всех причитающихся сумм и направлять их соответствующим уполномоченным эксплуатационным организациям.

2.2. Счета следует высылать как можно скорее с учетом соответствующих Рекомендаций МСЭ-Т, за исключением чрезвычайных обстоятельств, до истечения периода в 50 дней, следующего за месяцем, к которому они относятся, если иное не определено взаимным соглашением.

2.3. В принципе, счет считается акцептированным без особого уведомления об этом направившей его уполномоченной эксплуатационной организации.

2.4. Однако любая уполномоченная эксплуатационная организация имеет право опротестовать счет в течение двух календарных месяцев с даты его получения, но только в той степени, в какой это необходимо для сведения разницы к взаимоприемлемым пределам.

2.5. Для взаимосвязей, по которым не существует специальных соглашений, кредитующая уполномоченная эксплуатационная организация в кратчайший срок должна подготовить квартальный акт сверки расчетов с указанием сальдо по месячным счетам за период, к которому этот акт сверки расчетов относится, и должна направить его дебетующей уполномоченной эксплуатационной организации, которая после проверки должна возвратить один экземпляр акта с отметкой об его акцепте.

2.6. Для непрямых взаимосвязей, когда транзитная уполномоченная эксплуатационная организация выступает как посредник по расчетам между двумя оконечными пунктами, Государства-Члены должны стремиться обеспечить, чтобы уполномоченные эксплуатационные организации включали расчетные данные по транзитному трафику в соответствующий счет за исходящий трафик, который выставляется уполномоченным эксплуатационным организациям, находящимся после нее на данном маршруте, как можно скорее после получения этих данных от уполномоченной эксплуатационной организации исходящего вызова, согласно соответствующим Рекомендациям МСЭ-Т.

3. Оплата сальдо по счетам

3.1. Выбор валюты оплаты

3.1.1. Оплата сальдо по счетам за международную электросвязь должна производиться в валюте, выбранной кредитующей стороной по согласованию с дебетующей стороной. В случае разногласия выбор кредитующей стороны должен быть определяющим во всех случаях при условии соблюдения положений, приведенных ниже в п. 3.1.2. Если кредитующая сторона не указывает определенной валюты, то выбор ее принадлежит дебетующей стороне.

3.1.2. Если кредитующая сторона выбирает валюту, курс которой устанавливается в одностороннем порядке, или валюту, эквивалентный курс которой должен определяться на основе соотношения ее с валютой, курс которой устанавливается также в одностороннем порядке, то применение выбранной валюты должно быть приемлемо для дебетующей стороны.

3.1.3. При условии соблюдении сроков платежей уполномоченные эксплуатационные организации имеют право по взаимному соглашению урегулировать свои сальдо различных видов путем погашения:

a) кредитовых и дебетовых сальдо на своих взаимосвязях с другими уполномоченными эксплуатационными организациями;

b) любых других взаимно согласованных расчетов, в зависимости от случая.

Это правило применяется, в том числе, в случае, если платежи осуществляются через специализированные платежные учреждения на основании соглашений с уполномоченными эксплуатационными организациями.

3.2. Определение суммы оплаты

3.2.1. Сумма оплаты в выбранной валюте, как определено ниже, должна быть эквивалентна сальдо по счету.

3.2.2. Если сальдо по счету выражено в денежной единице МВФ, то сумма в выбранной валюте должна определяться курсом, действующим накануне оплаты, или последним опубликованным МВФ курсом между денежной единицей МВФ и выбранной валютой.

3.2.3. Однако если курс между денежной единицей МВФ и выбранной валютой не опубликован, то на первом этапе сальдо по счету должно конвертироваться в валюту, курс которой опубликован МВФ; при этом применяется курс, действующий накануне оплаты, или последний опубликованный курс. Полученная таким образом сумма на втором этапе должна конвертироваться в эквивалентную сумму в выбранной валюте, при этом применяется последний накануне оплаты курс, или самый последний курс, действующий на официальном или общепризнанном валютном рынке основного финансового центра дебетующей страны.

3.2.4 Если в соответствии со специальным соглашением сальдо по счету не выражено в денежной единице МВФ, то в это соглашение должны быть включены положения, касающиеся оплаты; и:

a) если выбранная валюта совпадает с валютой, в которой выражено сальдо по счету, то сумма оплаты в выбранной валюте должна быть равна величине сальдо по счету;

b) если выбранная для оплаты валюта отличается от той, в которой выражено сальдо по счету, то сумма оплаты должна определяться путем конвертирования сальдо по счету в его эквивалент в выбранной валюте в соответствии с положениями п. 3.2.3, приведенного выше.

3.3. Оплата сальдо

3.3.1. Оплата сальдо по счету должна производиться как можно скорее и, во всяком случае, не позднее чем через два календарных месяца после даты отправки акта сверки расчетов кредитующей уполномоченной эксплуатационной организацией. По истечении этого периода кредитующая уполномоченная эксплуатационная организация может начислять пени, которые, если не оговорено иное, могут достигать размера 6% годовых со дня, следующего за днем исчисления указанного срока, при условии, что было направлено предварительное уведомление в форме окончательного требования об оплате.

3.3.2. Оплата, причитающаяся по акту сверки расчетов, не должна задерживаться в ожидании урегулирования вопроса по поводу соответствующего счета. Согласованные позднее корректировки должны быть включены в следующий счет.

3.3.3. К дате оплаты дебетующая сторона должна перевести сумму в выбранной валюте, рассчитанную, как это указано выше, посредством банковского чека, банковского перевода или каким-либо другим способом, приемлемым для дебетующей и кредитующей сторон. Если кредитующая сторона не указывает предпочитаемого ею способа перевода, то выбор принадлежит дебетующей стороне.

3.3.4. Комиссия за платежи, начисленная в дебетующей стране (налоги, клиринговые наценки, комиссионные сборы и т. п.) должна оплачиваться дебетующей стороной. Любая такая комиссия, начисленная в кредитующей стране, включая комиссию за платеж банков-посредников в третьих странах, должна оплачиваться кредитующей страной.

3.4. Дополнительные положения

3.4.1. Если между моментом отправки денежного перевода (банковского перевода, банковских чеков и т. п.) и моментом его получения (зачислением суммы на счет, инкассированием чеков и т.п.) кредитующей стороной произойдет изменение эквивалентной суммы в выбранной валюте, рассчитанной как указано в п. 3.2, и если разница, вызванная таким изменением, превышает 5% причитающейся суммы, рассчитанной после таких изменений, то общая разница должна быть распределена в равных долях между дебетующей и кредитующей сторонами.

3.4.2. Если произойдет коренное изменение в международной валютной системе, в результате чего утратят силу или перестанут быть применимыми положения одного или нескольких приведенных выше пунктов, уполномоченные эксплуатационные организации имеют право по взаимному соглашению принять на время пересмотра вышеупомянутых положений другую валютную основу и/или другие процедуры оплаты сальдо по счету.

Дополнение 2
ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ, ОТНОСЯЩИЕСЯ К МОРСКОЙ ЭЛЕКТРОСВЯЗИ

1. Общие положения

Положения, содержащиеся в Статье 6 и в Дополнении 1, с учетом соответствующих Рекомендаций МСЭ-Т, должны применяться также к морской электросвязи при выставлении и оплате счетов в соответствии с настоящим Дополнением в той мере, в которой приведенными ниже положениями не предусматривается иное.

2. Расчетная организация

2.1. Платы за морскую электросвязь в морской подвижной и морской подвижной спутниковой службах должны, в принципе и в соответствии с национальным законодательством и действующей практикой, взиматься с обладателя лицензии на морскую подвижную станцию:

a) администрацией, выдавшей эту лицензию; или

b) уполномоченной эксплуатационной организацией; или

c) любой другой организацией или организациями, назначенными для этой цели администрацией, указанной выше в п. *a*).

2.2. В настоящем Дополнении администрация или уполномоченная эксплуатационная организация, или назначенная для этой цели организация или организации, перечисленные в п. 2.1, выше, называются «расчетная организация».

2.3. При применении положений Статьи 6 и Дополнения 1 для морской электросвязи вместо уполномоченной эксплуатационной организации, указанной в Статье 6 и Дополнении 1, следует читать «расчетная организация».

2.4. Для реализации настоящего Дополнения Государства-Члены должны назначить свою соответствующую расчетную организацию

или расчетные организации и сообщить Генеральному секретарю МСЭ их название, опознавательный код и адрес для включения в Список судовых станций и присвоения опознавателей морской подвижной службы. Число таких названий и адресов должно быть ограничено с учетом соответствующих Рекомендаций МСЭ-Т.

3. Выставление счетов

3.1. В принципе, счет должен считаться акцептированным без необходимости особого об этом уведомления направившего его поставщика услуг.

3.2. Однако любая расчетная организация имеет право опротестовать данные счета в течение шести календарных месяцев с даты отправки этого счета, даже если счет уже был оплачен.

4. Оплата сальдо по счетам

4.1. Все счета за международную морскую электросвязь должны оплачиваться расчетной организацией без промедления и, в любом случае, не позднее шести календарных месяцев с даты отправки счета, если только оплата счетов не осуществляется в соответствии с п. 4.3, ниже.

4.2. Если счета за международную морскую электросвязь остаются неоплаченными по истечении шести календарных месяцев, то администрация, выдавшая лицензию подвижной станции, должна по запросу принять меры в рамках применимого национального законодательства для обеспечения оплаты счетов обладателем лицензии.

4.3. Если период между датой отправки и датой получения счета превышает один месяц, то расчетная организация, ожидающая получения счета, должна немедленно сообщить поставщику услуг исходящей страны о том, что возможна задержка запросов по счету и оплаты. Однако эта задержка не должна превышать трех календарных месяцев в отношении оплаты или пяти календарных месяцев в отношении запросов по счету, в обоих случаях начиная с даты получения счета.

4.4. Дебетующая расчетная организация может отказаться от оплаты и корректировки счетов, которые представлены по истечении двенадцати календарных месяцев с даты передачи трафика, к которому относятся эти счета, если иное не предусмотрено в соответствии с национальным законодательством, в каковом случае максимальный предельный срок может составлять до восемнадцати календарных месяце.

РЕЗОЛЮЦИИ МЕЖДУНАРОДНОГО СОЮЗА ЭЛЕКТРОСВЯЗИ[1]

Резолюция PLEN/1

Специальные меры для развивающихся стран, не имеющих выхода к морю, и малых островных развивающихся государств в отношении доступа к международным волоконно-оптическим сетям

(Дубай, 2012 г.)

Всемирная конференция по международной электросвязи (Дубай, 2012 г.),

учитывая

a) резолюцию 65/172 Генеральной Ассамблеи Организации Объединенных Наций от 20 декабря 2010 года о конкретных действиях в связи с особыми потребностями и проблемами развивающихся стран, не имеющих выхода к морю (ЛЛДС);

b) Резолюцию 30 (Переем. Гвадалахара, 2010 г.) Полномочной конференции о специальных мерах, касающихся наименее развитых стран (НРС), малых островных развивающихся государств (СИДС), ЛЛДС и стран с переходной экономикой;

c) Декларацию тысячелетия и итоговый документ Всемирной встречи на высшем уровне 2005 года;

d) решения Женевского (2003 г.) и Тунисского (2005 г.) этапов Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО);

e) Алматинскую декларацию и Алматинскую программу действий: удовлетворение особых потребностей ЛЛДС в новых глобальных рамках для сотрудничества в области транзитных перевозок между не имеющими выхода к морю развивающимися странами и развивающимися странами транзита,

напоминая

a) о Новом партнерстве в интересах развития Африки (НЕПАД), которое является инициативой, направленной на укрепление экономического сотрудничества и развитие на региональном уровне, с учетом того, что многие не имеющие выхода к морю развива-

[1] URL: http://www.itu.int/ru/wcit-12/Pages/itrs.aspx

ющиеся страны и развивающиеся страны транзита расположены в Африке;

b) Декларации министров связи Южноамериканского союза наций (*UNASUR*) и дорожную карту по установлению соединений в Южной Америке в целях ее интеграции, разработанную Рабочей группой по электросвязи Южноамериканского совета по инфраструктуре и планированию (*COSIPLAN*);

c) что в соответствии с мандатом № 7, являющимся следствием решений шестого Саммита стран Северной и Южной Америки, который прошел в Картахене, Колумбия, 14–15 апреля 2012 года, главы государств и правительств стран Северной и Южной Америки решили «способствовать расширению соединений сетей электросвязи в целом, в том числе волоконно-оптических и широкополосных сетей, в странах региона, а также международных соединений, чтобы улучшить возможности установления соединений, повысить динамичность связи между странами Северной и Южной Америки, а также уменьшить затраты на международную передачу данных и, тем самым, способствовать доступу, установлению соединений и конвергенции услуг для всех социальных слоев в странах Северной и Южной Америки»,

вновь подтверждая

a) право стран, не имеющих выхода к морю, на доступ к морю и на свободу транзита через территории стран транзита всеми транспортными средствами в соответствии с применимыми нормами международного права;

b) что страны транзита, осуществляя полный суверенитет над своей территорией, имеют право на принятие всех необходимых мер для обеспечения того, чтобы предоставление определенных прав и объектов странам, не имеющим выхода к морю, никоим образом не ущемляло их собственных законных интересов,

признавая

a) значение электросвязи и новых информационно-коммуникационных технологий (ИКТ) для развития ЛЛДС и СИДС;

b) что трудности, с которыми в настоящее время сталкиваются ЛЛДС и СИДС, продолжают оказывать неблагоприятное воздействие на их развитие,

отмечая,

что доступ ЛЛДС к международным волоконно-оптическим сетям, а также прокладка волоконно-оптического кабеля по территории стран транзита не указаны в Алматинской программе действий в качестве приоритетных направлений развития и обслуживания инфраструктуры,

сознавая,

a) что волоконно-оптический кабель является выгодной транспортной средой электросвязи;

b) что доступ ЛЛДС и СИДС к международным волоконно-оптическим сетям будет содействовать их всеобъемлющему развитию и повысит их потенциал создания собственного информационного общества;

c) что при планировании и прокладке международных волоконно-оптических кабелей требуется тесное сотрудничество между ЛЛДС и странами транзита;

d) что для базовых инвестиций, которые необходимы для прокладки волоконно-оптического кабеля, требуется привлечение капиталовложений,

решает поручить Директору Бюро развития электросвязи

1. исследовать особую ситуацию в области услуг электросвязи/ИКТ в ЛЛДС и СИДС, учитывая значение доступа к международным волоконно-оптическим сетям при разумных затратах;

2. представить Совету МСЭ отчет о мерах, принятых для оказания помощи ЛЛДС и СИДС в соответствии с пунктом 1 раздела решает поручить, выше;

3. оказать ЛЛДС и СИДС помощь, необходимую для разработки требуемых им планов, которые содержали бы практические руководящие указания и критерии для определения устойчивых региональных, субрегиональных, многосторонних и двусторонних проектов, и для содействия таким проектам, которые предоставят им возможность более широкого доступа к международным волоконно-оптическим сетям,

поручает Генеральному секретарю

довести настоящую Резолюцию до сведения Генерального секретаря Организации Объединенных Наций с целью ее доведения до сведения Высокого представителя Организации Объединенных Наций по НРС, ЛЛДС, и СИДС,

предлагает Совету

принять надлежащие меры для обеспечения того, чтобы МСЭ продолжал активное сотрудничество в сфере развития услуг электросвязи/ИКТ в ЛЛДС и СИДС,

предлагает Государствам-Членам

1. сотрудничать с ЛЛДС и СИДС в содействии региональным, субрегиональным, многосторонним и двухсторонним проектам и программам в области интеграции инфраструктуры электросвязи, предоставляющим ЛЛДС и СИДС возможность более широкого доступа к международным волоконно-оптическим сетям;

2. оказывать помощь ЛЛДС и СИДС, а также странам транзита в выполнении проектов и программ в области интеграции инфраструктуры электросвязи,

призывает развивающиеся страны, не имеющие выхода к морю, и *малые островные развивающиеся государства*

продолжать уделять первостепенное внимание видам деятельности в области электросвязи/ИКТ, принимая меры в сфере технического сотрудничества, с тем чтобы содействовать всеобъемлющему социально-экономическому развитию,

предлагает Государствам-Членам, Членам Секторов, Ассоциированным членам и академическим организациям

и далее оказывать поддержку Сектору развития электросвязи МСЭ в исследованиях ситуации в области услуг электросвязи/ИКТ в НРС, ЛЛДС, СИДС и странах с переходной экономикой, которые определены в таком качестве Организацией Объединенных Наций и которым требуются специальные меры для развития электросвязи/ИКТ.

Резолюция PLEN/2
Согласованный на глобальном уровне национальный номер для доступа к экстренным оперативным службам
(Дубай, 2012 г.)

Всемирная конференция по международной электросвязи (Дубай, 2012 г.),

учитывая,

что путешественникам важно знать единый общеизвестный номер доступа к местным экстренным оперативным службам,

отмечая,

что в Рекомендации МСЭ-Т Е. 161.1 относительно Руководящих указаний по выбору номера экстренного вызова для сетей электросвязи общего пользования указываются два согласованных на глобальном уровне номера для экстренного вызова,

решает поручить Директору Бюро стандартизации электросвязи

принять необходимые меры, для того чтобы 2-я Исследовательская комиссия Сектора стандартизации электросвязи МСЭ (МСЭ-Т) продолжила исследование варианта внедрения в будущем единого согласованного на глобальном уровне национального номера для доступа к экстренным оперативным службам,

предлагает Государствам-Членам

внедрить в дополнение к своим существующим национальным номерам экстренного вызова согласованный на глобальном уровне национальный номер для доступа к экстренным оперативным службам с учетом соответствующих Рекомендаций МСЭ-Т.

Резолюция PLEN/3
Обеспечение благоприятной среды для более активного развития интернета

(Дубай, 2012 г.)

Всемирная конференция по международной электросвязи (Дубай, 2012 г.),

признавая

a) итоговые документы Женевского этапа (2003 г.) и Тунисского этапа (2005 г.) Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО);

b) что интернет является основным элементом инфраструктуры информационного общества, который из исследовательского и учебного инструмента превратился в общедоступный глобальный инструмент;

c) значение возможностей широкополосной передачи для содействия предоставлению более широкого диапазона услуг и приложений, поощрения инвестиций и предоставления доступа в интернет по приемлемым ценам как для существующих, так и для новых пользователей;

d) ценный вклад в развитие, функционирование и разработку интернета всех групп заинтересованных сторон в рамках их соответствующих функций, как это признается в пункте 35 Тунисской программы для информационного общества;

e) что, как отмечается в решениях ВВУИО, все правительства должны иметь одинаковые задачи и обязательства в сфере управления использованием интернета на международной основе и обеспечения стабильности, безопасности и целостности существующего интернета и его будущего развития, а также будущего интернета, и что также признается необходимость разработки правительствами государственной политики при консультациях со всеми заинтересованными сторонами;

f) Резолюции 101,102 и 133 (Переем. Гвадалахара, 2010 г.) Полномочной конференции,

решает предложить Государствам-Членам

1. вырабатывать свою соответствующую позицию по касающимся интернета международным вопросам технического характера, развития и государственной политики в рамках мандата МСЭ на различных форумах МСЭ, включая, среди прочего, Всемирный форум по политике в области электросвязи/ИКТ, Комиссию по широкополосной связи в интересах цифрового развития и исследовательские комиссии МСЭ;

2. работать вместе со всеми своими заинтересованными сторонами в этом направлении,

поручает Генеральному секретарю

1. продолжить принимать необходимые меры, для того чтобы МСЭ играл активную и конструктивную роль в развитии широкополосной связи и модели интернета, основанной на участии многих заинтересованных сторон, как это отмечено в пункте 35 Тунисской программы;

2 содействовать участию Государств-Членов и всех заинтересованных сторон, в зависимости от случая, в деятельности МСЭ в этом направлении.

Резолюция PLEN/4
Регулярное рассмотрение Регламента международной электросвязи

(Дубай, 2012 г.)

Всемирная конференция по международной электросвязи (Дубай, 2012 г.),

напоминая

Резолюцию 171 (Гвадалахара, 2010 г.) Полномочной конференции о подготовке к настоящей конференции по Регламенту международной электросвязи (РМЭ),

учитывая,

a) что Рабочая группа Совета МСЭ для подготовки к Всемирной конференции по международной электросвязи 2012 года (ВКМЭ-12) провела подробное обсуждение РМЭ;

b) что во всех регионах МСЭ проводились широкие консультации, в которых участвовали Государства – Члены МСЭ, Члены Секторов, Ассоциированные члены и академические организации – Члены МСЭ,

а также группы гражданского общества, проявившие большой интерес к пересмотру РМЭ;

c) что Члены МСЭ представили большое число входных документов;

d) результаты настоящей конференции,

признавая

a) Статьи 13 и 25 Устава МСЭ;

b) п. 48 (Статья 3) Конвенции МСЭ;

c) что РМЭ является одной из основ, обеспечивающих выполнение миссии МСЭ;

d) что после утверждения РМЭ до его рассмотрения на настоящей Конференции прошло 24 года;

e) что в РМЭ содержатся руководящие принципы высокого уровня, которые не должны требовать частого внесения поправок, но в стремительно развивающемся секторе электросвязи/ИКТ может потребоваться их регулярное рассмотрение,

отмечая,

a) что продолжают возрастать темпы технического развития и спрос на услуги, требующие большой полосы пропускания;

b) что *РМЭ*:

i) устанавливает общие принципы предоставления и эксплуатации международной электросвязи;

ii) способствует присоединению и функциональной совместимости в глобальном масштабе;

iii) содействует эффективности, полезности и доступности услуг международной электросвязи,

решает

предложить Полномочной конференции 2014 года рассмотреть настоящую Резолюцию и принять необходимые меры, если потребуется, по созыву на регулярной основе (например, раз в восемь лет) Всемирной конференции по международной электросвязи для пересмотра РМЭ, принимая во внимание финансовые последствия для Союза,

поручает Генеральному секретарю

1. довести настоящую Резолюцию до сведения Полномочной конференции;

2. предоставить информацию, которая позволит Полномочной конференции рассмотреть финансовые последствия созыва ВКМЭ,

предлагает Государствам-Членам

вносить вклад в работу, определенную в настоящей Резолюции.

Резолюция PLEN/5
Завершение трафика и обмен трафиком услуг международной электросвязи

(Дубай, 2012 г.)

Всемирная конференция по международной электросвязи (Дубай, 2012 г.),

учитывая,

a) что переход от выделенных телефонных сетей и сетей передачи данных к конвергированным сетям на базе *IP* поднимает важные регуляторные, технические и экономические вопросы, которые необходимо принимать во внимание;

b) что многие Государства-Члены заявили о необходимости разработки и реализации коммерческих соглашений между уполномоченными эксплуатационными организациями и поставщиками международных услуг с целью расширения прав и возможностей всех участников новой цепочки создания стоимости,

отмечая,

a) что некоторые Государства-Члены наблюдают ухудшение качества международных услуг и голосового трафика;

b) что мандат 3-й Исследовательской комиссии Сектора стандартизации электросвязи МСЭ (МСЭ-Т) включает изучение вопроса о разработке Рекомендаций, резолюций и руководящих указаний, относящихся к этим вопросам;

c) что необходимо более широкое понимание альтернативных механизмов разрешения споров, вытекающих из коммерческих соглашений;

d) что некоторые Государства-Члены выражают обеспокоенность в отношении предотвращения и смягчения последствий мошенничества в международной электросвязи,

решает предложить заинтересованным Государствам-Членам сотрудничать, чтобы:

i) каждая сторона в переговорах или соглашениях, связанных с вопросами международных соединений или вытекающих из них, могла при использовании альтернативного механизма разрешения споров обратиться за поддержкой к соответствующим органам государства другой стороны;

ii) их нормативно-правовые базы способствовали заключению коммерческих соглашений между уполномоченными эксплуатационными организациями и поставщиками международных услуг, в соответствии с принципами обеспечения добросовестной конкуренции и инноваций,

поручает Директору Бюро стандартизации электросвязи

принять необходимые меры, для того чтобы 3-я Исследовательская комиссия МСЭ-Т провела исследование последних разработок и практики в отношении завершения трафика и обмена трафиком международной электросвязи на основе коммерческих соглашений, с целью разработки Рекомендации, при необходимости, и руководящих указаний для заинтересованных Государств-Членов, предназначенных для использования поставщиками услуг международной электросвязи, в отношении вопросов, которые они считают актуальными, в том числе:

i) условий выставления счетов;

ii) условий отправки счетов;

iii) условий оплаты счетов;

iv) условий разрешения споров;

v) условий предотвращения и смягчения последствий мошенничества;

vi) условий в отношении платы за завершение трафика и обмен трафиком услуг международной электросвязи,

предлагает Государствам-Членам

представлять вклады относительно завершения трафика и обмена трафиком международной электросвязи в 3-юИсследовательскуюкомиссию с целью содействия ее работе,

предлагает Членам Секторов

представлять информацию в 3-ю Исследовательскую комиссию и обмениваться передовым опытом в области завершения трафика и обмена трафиком услуг международной электросвязи, включая, в частности, выставление счетов.

4.3. Совет Европы (СЕ)

ДЕКЛАРАЦИЯ КОМИТЕТА МИНИСТРОВ О ПРИНЦИПАХ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

(Принята Комитетом министров 21 сентября 2011 г. на 1121-м заседании заместителей министров)

1. Интернет представляет собой совокупность широкого спектра идей, технологий, ресурсов и политики, разработанных для установления свободы и на основе коллективных усилий в общих интересах. Государства, частный сектор, гражданское общество и частные лица содействовали созданию динамичного, совместимого и успешного

Интернета, который мы знаем сегодня. Интернет предоставляет пространство свободы, обеспечивающее осуществление и реализацию основных прав, процессы участия и демократические процессы, социальную и коммерческую деятельность.

2. Вышеизложенное способствовало становлению общего понимания управления Интернетом, которое нашло официальное закрепление в Декларации принципов, принятой в ходе Женевского этапа Всемирного саммита по информационному обществу в декабре 2003 года. Тунисская программа, принятая на втором этапе Всемирного саммита по информационному обществу в ноябре 2005 года, сформулировала, что под управлением Интернетом понимается разработка и применение правительствами, частным сектором и гражданским обществом, при выполнении ими своей соответствующей роли, общих принципов, норм, правил, процедур принятия решений и программ, которые формируют условия для развития и использования Интернета.

3. Дискуссии по управлению Интернетом, проходящие на различных национальных и международных форумах, являются ощутимым результатом такого понимания. Это укрепляет диалог между государством, частным сектором и гражданским обществом и способствует формированию общих взглядов на политику в сфере Интернета и, в более широком плане, на управление Интернетом. Стремясь сохранить и закрепить этот подход, интернет-сообщества, международные организации и другие заинтересованные стороны участвуют в работе по закреплению основных ценностей Интернета и разрабатывают рекомендации по различным аспектам управления Интернетом.

4. Совет Европы принимает участие в этих процессах, и 47 государств-членов поддерживают в целом ряде нормативно-правовых актов меры, направленные на обеспечение максимальных прав в сети Интернет при условии минимальных ограничений, предлагая при этом такой уровень безопасности, который люди вправе ожидать. Это вытекает из принятых государствами - членами Совета Европы обязательств обеспечить каждому находящемуся под их юрисдикцией права и свободы, защищаемые Конвенцией о защите прав человека и основных свобод (*ETS* № 5).

5. Для обеспечения устойчивого, социально ориентированного и правозащитного подход к Интернету необходимо подтвердить принципы управления Интернетом, которые признают права человека и основные свободы, демократию и верховенство закона, а также основополагающие принципы интернет-сообществ, поскольку они развивались на базе указанных выше процессов.

6. В качестве вклада в происходящий в настоящее время всесторонний совместный и открытый процесс Комитет министров Совета Европы:

– подтверждает принципы, изложенные ниже, которые основываются на принципах управления Интернетом, постепенно разрабатываемые заинтересованными сторонами и интернет-сообществами;

– заявляет о своей твердой приверженности этим принципам и подчеркивает, что они должны быть поддержаны всеми государствами-членами в контексте разработки национальной и международной политики, связанной с Интернетом;

– призывает другие заинтересованные стороны руководствоваться ими при осуществлении своих собственных обязательств.

Принципы управления Интернетом

1. Права человека, демократия и верховенство закона

Механизмы управления Интернетом должны обеспечивать защиту всех основных прав и свобод и подтверждать их универсальность, неделимость, взаимозависимость и взаимосвязь в соответствии с международным правом прав человека. Они также должны обеспечивать полное соблюдение демократии и верховенства закона и должны способствовать устойчивому развитию. Все участники, государственные и частные, должны признавать и защищать права человека и основные свободы в своей деятельности, а также при разработке новых технологий, услуг и программ. Они должны быть в курсе расширяющихся технических возможностей, ведущих к совершенствованию, но также и к вызовам в отношении основных прав и свобод, и в полной мере участвовать в усилиях, направленных на признание вновь возникающих прав.

2.Многосторонние управления

Разработку и внедрение механизмов управления Интернетом следует обеспечить на открытой, транспарентной и подконтрольной основе, при широком участии правительств, частного сектора, гражданского общества, технического сообщества и пользователей, с учетом их конкретных ролей и обязанностей. Развитие международной политики, связанной с Интернетом политики и механизмов управления Интернетом должно обеспечивать возможность полного и равного участия всех заинтересованных сторон из всех стран.

3. Ответственность государств

Государства имеют права и обязанности в отношении вопросов международной политики по вопросам, связанным с Интернетом.

При осуществлении своих суверенных прав государства должны, с учетом международного права, воздерживаться от любых действий, которые могут прямо или косвенно нанести вред физическим или юридическим лицам вне пределов их территориальной юрисдикции. Кроме того, любые внутригосударственные решения или действия, равносильные ограничениям основных прав, должны соответствовать международным обязательствам и, в частности, должны основываться на законе, быть необходимыми в демократическом обществе и в полной мере уважать принципы пропорциональности и право на обжалование в соответствии с правовыми и процессуальными гарантиями.

4. Расширение прав и возможностей интернет-пользователей

Пользователям должно быть в полной мере дано право реализовывать свои основные права и свободы, принимать обоснованные решения и участвовать в механизмах управления Интернетом, в частности, в механизмах управления и развития политики, связанной с Интернетом, в полной мере.

5. Универсальность Интернета

Политики, связанные с Интернетом, должны признать глобальный характер Интернета и цели всеобщего доступа. Они не должны отрицательно влиять на свободный поток трансграничного интернет-трафика.

6. Целостность Интернета

Безопасность, стабильность, надежность и устойчивость Интернета, а также его способность к развитию должны быть ключевыми целями управления Интернетом. Для того чтобы сохранить целостность и успешность функционирования инфраструктуры Интернета, а также доверие пользователей, необходимо содействовать развитию сотрудничества всех заинтересованных сторон на национальном и международном уровне.

7. Децентрализованное управление

Децентрализованный характер ответственности за оперативное управление Интернетом должен быть сохранен. Органы, ответственные за технические и управленческие аспекты Интернета, а также частный сектор должны сохранять свою ведущую роль в технических и оперативных вопросах при обеспечении транспарентности и подотчетности мировому сообществу в отношении тех действий, которые оказывают влияние на государственную политику.

8. Архитектурные принципы

Открытые стандарты и совместимость Интернета, так же как и принцип сквозной связи, должны быть сохранены.Эти принципы должны стать руководящими принципами для всех заинтересованных сторон

при принятии ими решений, касающихся управления Интернетом. Не должно существовать каких-либо необоснованных барьеров входа для новых пользователей или законного использования Интернета, или лишних обременений, которые могут повлиять на потенциал для инноваций в отношении технологий и услуг.

9. Открытая сеть

Пользователи должны иметь максимально возможный доступ к интернет-контенту, приложениям и услугам по их выбору, вне зависимости от того, на платной или бесплатной основе они предлагаются, с использованием соответствующих устройств по их выбору. Механизмы управления трафиком, которые оказывают влияние на осуществление основных прав и свобод, в частности права на свободу выражения мнения и распространение и получение информации вне государственных границ, а также права на уважение частной жизни, должны соответствовать требованиям международного права, защищающего свободу слова и доступа к информации и право на уважение частной жизни.

10. Культурное и языковое разнообразие

Сохранение культурного и языкового разнообразия и содействие развитию местного контента, независимо от языка или наречия, должны быть основными целями политики, связанной с Интернетом, и международного сотрудничества, так же как и развитие новых технологий.

СТРАТЕГИЯ СОВЕТА ЕВРОПЫ ПО УПРАВЛЕНИЮ ИНТЕРНЕТОМ НА 2012–1015 ГОДЫ

(2012 г.)

(*Извлечения*)

[В документе отмечается, что Стратегия создает целостное представление для устойчивого и долгосрочного подхода к развитию интернета. Успех ее осуществления будет во многом зависеть от многостороннего диалога и поддержки. Она будет дополнением к растущему числу политических нормативных актов, практических инструментов возможностей для мультистекхолдерского сотрудничества, которые содействуют правительствам, частному сектору и гражданскому обществу в защищате и уважении прав человека, принципов верховенства закона и демократии в Интернете.

Также подчеркивается, что Совет Европы в полной мере поддерживает многостороннюю модель управления интернетом (multi-stakeholder model of Internet governance), которая гарантирует универсальность, от-

крытость и инновационный характер интернета и продолжает служить интересам пользователей интернета во всем мире.]

<...>

Цели и задачи

5. Настоящая Стратегия устанавливает приоритеты и определяет цели на последующие четыре года (2012–2015) для укрепления защиты и уважения прав человека, верховенства закона и демократии в интернете. Основные цели Стратегии включают:

– защиту универсальности, целостности и открытости интернета;

– максимальное расширение прав и свобод пользователей интернета;

– совершенствование защиты персональных данных и частной жизни;

– укрепление верховенства закона и взаимодействие в борьбе с киберпреступностью;

– максимизацию потенциала интернета и его потенциала для продвижения демократии и культурного разнообразия;

– защиту и расширение прав и возможностей детей и молодежи.

<...>

7. Стратегия основывается и соответствует Декларации о принципах управления интернетом Комитета Министров 2011 года и его Рекомендации *CM/Rec*(2011)83 по охране и защите универсальности, целостности и открытости интернета.

<...>

ПРОГРАММА ПОДГОТОВКИ СУДЕЙ И ПРОКУРОРОВ ПО ВОПРОСАМ КИБЕРПРЕСТУПНОСТИ: КОНЦЕПЦИЯ[1]

(2009 г.)
(Извлечения)

[Полное содержание документа
1. Краткое содержание
2. Введение

[1] Документ подготовлен Рабочей группой заинтересованных сторон в рамках проекта «Киберпреступность» и Лиссабонской сети Совета Европы по подготовке судей. Опубликован на русском зыке: URL: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/training/2079_train_concept_4_provisional_8oct09_RUS.pdf. Публикацию предваряет оговорка о том, что документ представляет собой технический отчет и необязательно отражает официальную позицию Совета Европы, спонсоров проекта или сторон, на инструменты которых содержит ссылки.

3. Учебные заведения и системы
4. Навыки и знания, необходимые судьям и прокурорам
4.1. Базовые знания
4.2. Знания на продвинутом уровне
4.3. Специализированные знания
5. Текущая подготовка по вопросам киберпреступности и электронных доказательств
5.1. Начальная подготовка
5.2. Переподготовка
6. Предлагаемый подход
6.1. Цель
6.2. Институционализация начальной подготовки
6.3 Институционализация переподготовки
6.4. Стандартизация и тиражирование курсов/модулей
6.5 Доступ к учебным пособиям и материалам для самообучения
6.6 Пилотные центры подготовки на базовом и продвинутом уровнях
6.7. Расширение знаний за счет сетевого взаимодействия
6.8. Государственно-частное сотрудничество
7. Оказание поддержки в реализации настоящей концепции
8. Приложение
8.1. Лиссабонская сеть: связи с юридическими учебными заведениями
8.2. Примеры базовых учебных курсов: структура и тематика
8.2.1. Пример Нидерландов
8.2.2. Пример Германии (Немецкая академия по подготовке судей)
8.2.3. Примеры Совета Европы
8.3. Примеры курсов подготовки на продвинутом уровне: структура и тематика
8.3.1. Пример Нидерландов
8.3.2. Предложение Нидерландов по проведению мастер класса]

1. Краткое содержание

Учитывая то, что общества во всем мире широкого используют информационные и коммуникационные технологии, судьи и прокуроры должны быть подготовлены к рассмотрению дел, связанных с киберпреступностью и использованием электронных доказательств. Несмотря на то, что во многих странах правоохранительные органы имели возможность укрепить свой потенциал знаний для расследования киберпреступлений и использования электронных доказательств, это, судя по всему, в меньшей степени коснулось судей и прокуроров. Опыт показывает, что при ведении большинства дел судьи и прокуроры сталкиваются с трудностями при взаимодействии с новыми реалиями компьютерного мира. В связи с этим, требуются специальные усилия, чтобы судьи и прокуроры могли вести судебное преследование и выносить постановления в отношении киберпреступлений и использовать электронные доказательства благодаря проведению программ повышения квалификации, сетевому взаимодействию и специализации.

Концепция настоящего документа предусматривает оказание поддержки этим усилиям. Она была разработана Советом Европы в Проекте «Киберпреступность» и Лиссабонской сетью Совета Европы по подготовке судей в сотрудничестве с многосторонней рабочей группой заинтересованных сторон в течение 2009 г.

Целью настоящей концепции является оказание помощи учебным заведениям в разработке программ подготовки судей и прокуроров по вопросам киберпреступлений и использования электронных доказательств и включение этих программ в традиционные курсы начальной подготовки и переподготовки (то есть обеспечение их институционализации). Кроме того, это будет способствовать сетевому взаимодействию между судьями и прокурорами в целях повышения их уровня знаний, а также оказания постоянной, а не единовременной поддержки инициативам заинтересованных сторон в области обучения.

Настоящая концепция включает следующие компоненты:

Цели

Существующая система начальной подготовки и переподготовки, как правило, не предоставляет судьям и прокурорам знаний, которые требуются для рассмотрения дел о киберпреступлениях и для использования электронных доказательств.

Таким образом, концепция обучения судей и прокуроров должна преследовать следующие цели:

• Предоставить возможность учебным заведениям проводить программы начальнойподготовки и переподготовки, основанные на международных стандартах;

• Вооружить максимально возможное количество будущих и практикующих судей и прокуроров основными знаниями о киберпреступлениях и использовании электронных доказательств;

• Провести программы повышения квалификации значительного количества судей и прокуроров;

• Оказать помощь в проведении дальнейшей специализации и технической подготовки судей и прокуроров;

• Способствовать расширению знаний с помощью сетевого взаимодействия между судьями и прокурорами;

• Облегчить доступ к различным учебным инициативам и сетям.

Для достижения этих целей следует принять следующие меры:

1. Институционализация начальной подготовки

• Тем странам, где начальная подготовка представляет собой практические занятия на рабочем месте, рекомендуется, чтобы, по меньшей мере, часть этих занятий была связана с вопросами киберпреступлений и использования электронных доказательств;

• В тех странах, где начальная подготовка проводится в юридических учебных заведениях, учебные курсы этих заведений должны включать как минимум один модуль базового уровня по вопросам киберпреступлений и использования электронных доказательств. Эти вопросы должны дополнительно рассматриваться в обязательных модулях, охватывающих вопросы материального и процессуального права. Необходимо также предлагать учащимся факультативные модули для получения знаний по вопросам киберпреступности и использования электронных доказательств на продвинутом уровне;

• Специальные учебные модули следует привести в такое соответствие со стандартами, чтобы их можно было тиражировать и использовать для того, чтобы слушатели могли повышать уровень своих знаний, начиная с базового уровня и кончая продвинутым уровнем.

2. Институционализация переподготовки

• Учебные заведения, проводящие программы переподготовки, должны включать в них, по меньшей мере, один модуль базового уровня по киберпреступности и использованию электронных доказа-

тельств, чтобы вооружить практикующих судей и прокуроров базовыми знаниями, которые они не получили во время начальной подготовки;

• Кроме того, они должны предлагать курсы обучения на продвинутом уровне.

3. Стандартизация и тиражирование курсов/модулей

• Необходимо разработать стандартизированные курсы или модули, которые можно было бы эффективно тиражировать в широких масштабах и использовать для того, чтобы слушатели и практикующие судьи и прокуроры могли повышать уровень своих знаний, начиная с базового уровня и кончая продвинутым уровнем. Следует провести оценку существующих базовых курсов, которые можно было бы включить в учебные планы программ начальной подготовки и переподготовки.

• Стандартный курс можно затем рекомендовать учебным заведениям для программ начальной подготовке и переподготовки.

• Аналогичную оценку можно было бы дать курсам на продвинутом уровне и затем рекомендовать учебным заведениям стандартный курс на продвинутом уровне.

• Преподавателям необходимо пройти такой курс подготовки по преподаванию этих курсов, чтобы обучение могли проводить местные преподаватели на местных языках лишь при ограниченном участии международных преподавателей.

4. Доступность учебных пособий/материалов для самообучения

• Необходимо разработать учебные пособия, соответствующие общим международным стандартам и передовой практике. Они должны быть доступны для учебных заведений с точки зрения экономической выгоды, чтобы обеспечить их распространение на местном уровне;

• Несмотря на то, что судьи и прокуроры должны в первую очередь проходить подготовку по применению национального законодательства, тем не менее, можно разработать стандартизированные учебные пособия таким образом, чтобы в них оставалось достаточно места для отражения особенностей национальных систем и законодательств;

• Следует разработать и обеспечить доступ к онлайновым курсам.

5. Пилотные центры обучения на базовом и продвинутом уровнях

• Необходимо создать ряд пилотных центров для подготовки судей и прокуроров по вопросам киберпреступности и использования электронных доказательств на базовом и продвинутом уровнях, чтобы апробировать эти курсы и затем разработать стандартизированные

курсы и материалы, обеспечить распространение передовой практики, провести исследования процесса обучения, вести реестр преподавателей, проводить подготовку преподавателей, проводить программы обучения в других странах с аналогичными системами и языками;

• Пилотные центры должны координировать свою работу друг с другом при поддержке Совета Европы;

• Судья и следователи, которые прошли подготовку и стали специалистами, должны рассмотреть возможность участия в программах обучения в центрах повышения квалификации для представителей правоохранительных органов и промышленности.

6. Расширение объема знаний за счет сетевого взаимодействия

• Помимо обучения, контактов между коллегами, сетевого взаимодействия между судьями и прокурорами, также крайне важно осуществлять сетевое взаимодействие с широким кругом других заинтересованных сторон;

• Судьи и прокуроры должны использовать существующие сети для судей или прокуроров (например, *GPEN*);

• Совету Европы следует обсудить возможность создания международной сети по киберпреступлености или электронным преступлениям для судей (аналогичной сети *GPEN* для прокуроров);

• Совет Европы и Европейская сеть по подготовке судей должны оказать поддержку взаимодействию между европейскими учебными заведениями, проводящими программы по вопросам киберпреступности и использования электронных доказательств;

• В целях оказания содействия судьям и прокурорам в обеспечении доступа к этим и многим другим сетям, касающимся вопросов киберпреступности, Совет Европы должен составить карту инициатив и информационных сетей и создать портал с соответствующими ссылками, краткой информацией и подробными контактными данными разных сетей. Это также должно способствовать развитию сетевого сотрудничества. Кроме того, это также должно облегчить доступ к существующим учебным материалам и инициативам.

7. Государственно-частное сотрудничество

• Поддержка частного сектора в проведении подготовки судей и прокуроров могла бы быть полезной, учитывая то, что частный сектор обладает соответствующим опытом знания этого предмета. В то же время, судьи и прокуроры должны оставаться независимыми и беспристрастными;

• Учебные заведения по подготовке судей могут использовать опыт частного сектора при разработке учебных программ, подготовке учебных пособий и проведении курсов обучения;

• Поддержка учебных заведений со стороны промышленности не должна быть направлена на принятие потенциально благоприятных решений в суде или на развитие предпринимательства, а гарантировать предоставление судьям и прокурорам адекватной информации, позволяющей им принимать информированные решения;

• Частный сектор мог бы оказывать прозрачную поддержку международным или национальным организациям, научному сообществу, образовательным инициативам или другим третьим сторонам, которые могут в свою очередь помогать независимым учебным заведениям;

• Несмотря на то, что судьи и прокуроры должны иметь общее представление об Интернете и о киберпреступности, не менее важно предоставить им специальную информацию о платформах. Промышленность могла бы предоставить конкретные модули (а не полные курсы) по вопросам функционирования соответствующих платформ.

Лиссабонская сеть Совета Европы одобрила настоящую концепцию в сентябре 2009 г. и рекомендовала ее для широкого распространения и применения учебными заведения по подготовке судей. Она приняла решение привлечь к ней внимание Консультативного совета европейских судей и Консультативного совета европейских прокуроров, а также Европейской комиссии по эффективности правосудия (ЕКЭП), чтобы обеспечить самую широкую поддержку настоящей концепции.

2. Введение

В последние годы общества во всем мире добились огромного прогресса в развитии информационного общества. Информационные и коммуникационные технологии (ИКТ) теперь проникли практически во все сферы жизни людей. При этом более широкое использование ИКТ и, следовательно, зависимость от их использования делают общество уязвимым для таких угроз, как киберпреступность, т.е. преступления, совершенные против компьютерных данных и систем или с их помощью.

Помимо большого количества правонарушений, совершенных против ИКТ или с их помощью, все больше других дел, заканчивающихся в суде, связано с электронными доказательствами, хранящимися в компьютерной системе или на других устройствах.

Таким образом, судьи и прокуроры должны быть готовы к рассмотрению дел, связанных с киберпреступленостью и использованием электронных доказательств. Как заявил Консультативный совет европейских судей[1], «крайне необходимо, чтобы судьи после прохождения полного курса юридического образования получали разнообразные знания и могли эффективно выполнять свои обязанности» (пункт 3), «эта подготовка также гарантирует их независимость и беспристрастность» (пункт 4), в ходе этой подготовки следует «принимать во внимание необходимость социальной информированности и широкого понимания различных предметов, отражающих сложности жизни в современном обществе» (пункт 27). ИКТ играют такую важную роль в жизни современного общества, что судьи и прокуроры должны, по меньшей мере, иметь базовое представление об этих технологиях и связанных с ними проблемах.

Несмотря на то, что во многих странах правоохранительные органы смогли повысить потенциал своих знаний для проведения расследований киберпреступлений и получения электронных доказательств, это, судя по всему, в меньшей степени касается судей и прокуроров, которые, тем не менее, играют важнейшую роль в процессе уголовного правосудия. Опыт показывает, что в большинстве случаев судьи и прокуроры сталкиваются с трудностями при взаимодействии с новыми реалиями компьютерного мира.

В связи с этим, требуются специальные усилия, чтобы судьи и прокуроры могли вести судебное преследование, выносить решения в связи с киберпреступлениями и использовать электронные доказательства благодаря проведению программ повышения квалификации, сетевому взаимодействию и специализации.

Опыт частного сектора в области новых технологий был необходимым условием подготовки работников правоохранительных органов. Он также будет полезен для подготовки судебных работников[2], но его потенциал пока недостаточно используется. В то же время, необходимо сохранить независимость и беспристрастность судей и прокуроров. Таким образом, инновационные подходы требуют сохранения независимости судей и прокуроров и в то же время предоставления

[1] Заключение № 4 о надлежащих программах начальной подготовки и переподготовки судей на национальном и европейском уровнях (ЕКЭП (2003), Заключение № 4).

[2] См. исследование, опубликованное в марте 2009 г.: «Co-operation between LE, Industry and Academia to deliver long term sustainable training to key cybercrime personnel» («Сотрудничество между учебными заведениями, промышленностью и научным сообществом в целях обеспечения долгосрочной устойчивой подготовки основного персонала по вопросам киберпреступности»).

им доступа к опыту частного сектора и обеспечения понимания ими методов функционирования промышленности и технологии. Концепция, предлагаемая в настоящем документе, показывает, каким образом учебные заведении по подготовке судей могут получить пользу от поддержки со стороны промышленности и научного сообщества через стандартизированные учебные программы и за счет использования других средств.

Целью настоящей концепции является оказание помощи учебным заведениям в разработке для судей и прокуроров программ по вопросам киберпреступности и использования электронных доказательств и включении этих программ в традиционные курсы начальной подготовки и переподготовки (то есть, их институализация).

Концепция основана на информации, полученной из учебных заведений Бельгии, Хорватии, Грузии, Германии, Франции, Нидерландов, Польши, Португалии, Румынии, Испании, «бывшей югославской Республики Македония» и Великобритании (ответы на вопросы анкеты, полученные в июне 2009 г.), на практическом семинаре для представителей Бельгии, Ирландии, Италии, Португалии, Нидерландов и Великобритании, а также частного сектора, проходившем в Португалии в июле 2009 г., и на практическом семинаре, состоявшемся в Страсбурге 3–4 сентября при участии представителей учебных заведений, судей и прокуроров из вышеперечисленных стран, частного сектора, а также Европейской сети по подготовке судей и Лиссабонской сети Совета Европы[1].

Этот процесс с участием многочисленных заинтересованных сторон впервые привел к разработке концепции подготовки судей и прокуроров по вопросам киберпреступности и использования электронных доказательств. Коллективный характер этого процесса, несомненно, будет способствовать сотрудничеству между разными заинтересованными сторонами и выработке согласованной стратегии использования знаний и опыта при применении настоящей концепции.

Лиссабонская сеть Совета Европы одобрила настоящую концепцию в сентябре 2009 г. и рекомендовала ее для широкого распространения и применения учебными заведения по подготовке судей. Она приняла решение привлечь к ней внимание Консультативного совета европейских судей и Консультативного совета европейских прокуроров, а также Европейской комиссии по эффективность правосудия (ЕКЭП), чтобы обеспечить самую широкую поддержку настоящей концепции.

[1] Лиссабонская сеть для обмена информацией между частными лицами и юридическими лицами, отвечающими за подготовку судей.

3. Учебные заведения[1] и системы

В Европе, а также в других регионах существуют разнообразные системы подготовки судей и прокуроров[2].

Что касается *начальной* подготовки, то, как правило, эти системы включают один или несколько следующих элементов<...>:

– Система *A*: Слушатели, получившие университетское образование, которые, как правило, после успешной сдачи вступительного экзамена проходят специальный курс подготовки в юридическом учебном центре, чтобы стать судьями и/или прокурорами. Иногда будущие судьи и прокуроры учатся вместе, а иногда в разных учебных заведениях.

– Система *B*: Слушатели, получившие университетское образование, получают практический опыт на рабочем месте (иногда в рамках прохождения официальной стажировки) в прокурорских службах, юридических конторах или в других учреждениях, чтобы затем сдать экзамен на получении квалификации для работы адвокатами, прокурорами и судьями. Это не связано с централизованной подготовкой в специальном учебном заведении[3].

Переподготовка, то есть дальнейшее профессиональное обучение работающих судей и прокуроров, проводится в государственных юри-

---

[1] В целях настоящего документа термин «учебное заведение» относится к любому учреждению, отвечающему за обучение.

[2] Как отмечал Консультативный совет судей Совета Европы в 2003 г., «в европейских странах наблюдаются существенные различия в вопросах начальной подготовки и переподготовки судей. Эти различия отчасти могут быть связаны с особенностями разных судебных систем, но в определенном отношении не представляются неизбежными и необходимыми. В одних странах проводится долгосрочное официальное обучение в специализированных заведениях, за которым следует интенсивная дальнейшая подготовка. В других странах проводится стажировка под контролем опытного судьи, который передает знания и дает профессиональные рекомендации на основании конкретных примеров, показывающих, какой подход следует применять и как следует избегать нравоучительности. Страны прецедентного (общего) права в значительной мере полагаются на продолжительный профессиональный опыт, как правило, в сфере адвокатской практики. Наряду с этими вариантами существует широкий перечень стран, где подготовка в различной мере носит организованный и обязательный характер». – Заключение № 4 Консультативного совета европейских судей (CCJE) для Комитета министров Совета Европы по надлежащей начальной подготовке и переподготовке судей на национальном и европейском уровнях (*CCJE* (2003) Заключение № 4; ноябрь 2003 г.).

[3] Следует упомянуть об особенностях систем общего права. Например, в Великобритании судейназначают на неполное рабочее время сроком не менее одного месяца в год, а затем большинство из них назначают на полную ставку. Кроме того, на неполный рабочий день назначают членов трибуналов (гражданское право) и судов магистрата (в основном, уголовное право). До любого назначения и во время пребывания в должности проводятся отдельные программы подготовки.

дических учебных заведениях, которые также отвечают за начальную подготовку (например, во Франции, Грузии, Нидерландах, Польше, Португалии, Румынии, Испании, «бывшей югославской Республике Македонии», Хорватии), в учебных заведениях, которые специально были созданы для переподготовки кадров (например, в Германии), или в других государственных учреждениях, неправительственных организациях, международных организациях или в частном секторе. В некоторых случаях это предусмотрено в ежегодных учебных планах или в рамках специальных программ. В большинстве случаев переподготовка является необязательной, если только судьи и прокуроры не выполняют свои обязанности в специализированных судах (например, в Румынии).

Учебный план по начальной подготовке и переподготовке в большинстве случаев требует официального рассмотрения и одобрения, хотя в отношении переподготовки применяется более гибкий подход. Например:

– Во Франции учебный кур проводится после консультаций с участием судебного персонала и представителей департаментов министерства юстиции. Затем программу подготовки подают на одобрение Совета директоров учебного заведения.

– В Германии за разработку учебного курса переподготовки в академии отвечает Программная конференция Немецкой академии по подготовке судей, в состав которой входят представители разных административных органов системы правосудия, а также профессиональных ассоциаций судей и прокуроров.

– В Польше к 30 апреля каждого года департаменты министерства юстиции, председатели судов и прокурорские службы подают свои предложения. На основании этих предложений директор Национальной школы представляет Программному совету план учебных мероприятий на следующий год, который должен быть одобрен к 30 июля. После одобрения министра юстиции учебный план направляют в соответствующие департаменты министерства юстиции, председателям апелляционных судов и государственным обвинителям апелляционных судов.

– В Румынии стратегию начальной подготовки и переподготовки утверждает Научный совет Национального института судей и Верховный совет судей.

– В Испании учебные планы и программы разрабатывает педагогический комитет, состоящий из экспертов по правовым вопросам, в рамках консультаций с ассоциациями судей или отдельными судьями. Учебный план по начальной подготовке и переподготовке судей окончательно одобряет Генеральный судейский совет.

– В Португалии учебную программу ежегодно тщательно продумывает и разрабатывает Центр судебных исследований. Программа начальной подготовки предусматривается законом, а программа переподготовки ежегодно меняется с учетом потребностей, выявленных на практике. Учебная программа принимается после консультаций с Верховными советами судей, Налоговыми и Административными судами и Прокурорской службой.

– В Бельгии общие и более специальные образовательные программы ежегодно разрабатывает или контролирует их разработку «Институт подготовки судей» (*Institut de formation judiciaire*). Этот институт был создан недавно в соответствии с законом от 31/01/07 и активно работает с начала 2009 г. Вопросы киберпреступности могут быть включены (нередко факультативно) в программы переподготовки.

– В Нидерландах Совет судей и Совет генеральных прокуроров (которые вместе являются образовательной организаций и обеспечивают работу Института по подготовке прокуроров и судей – *SSR*) принимают решение о наличии бюджета на проведение предлагаемых программ подготовки. Предложения могут поступать, например, от прокуроров, судей или лекторов *SSR*, и при наличии и выделении бюджета учебные программы затем разрабатывают соответствующие эксперты прокурорской службы, судьи и, при необходимости, третьи стороны, например, частные лица.

– В Хорватии учебный план начальной подготовки и планы переподготовки разрабатываются в рамках сотрудничества между Консультативным советом и Программным советом Юридической академии. Программный совет определяет приоритетные направления обучения и подает заявку на разработку проекта годового учебного плана профессиональной подготовки. Консультативный совет одобряет документ и направляет руководящие указания по разработке стратегии профессиональной подготовки. Члены двух советов являются видными экспертами в области права и представителями всех целевых групп Юридической академии.

Учебные заведения могут использовать опыт и знания независимых экспертов, в частности, если речь идет о специализированных или технических предметах, например, о киберпреступности и электронных доказательствах. Например:

В Германии Академия по подготовке судей Германии широко использует привлеченных лекторов, большинство из которых являются профессионалами или исследователями в области права, но иногда для проведения занятий приглашают промышленных экспертов.

– В Нидерландах консультанты и промышленные эксперты принимают участие в разработке учебных курсов и в проведении учебных занятий.

– В Румынии Национальный институт судей пользуется услугами приглашенных преподавателей и лекторов по таким специализированным предметам, как киберпреступность (например, из Совета Европы, министерства юстиции США, ФБР, Секретной службы США, а также из частного сектора – компаний *eBay*, *Visa*, *American Express*, *Amazon*, *PayPal*, *Microsoft*), а также для подготовки преподавателей.

– В Испании Генеральный совет судей подписал договоры с компаниями частного сектора (*CYBEX, Logality*) о проведении подготовки по куберпреступности и киберкриминалистике. Кроме того, эксперты из частного сектора принимают участие в подготовке судебных работников.

– В Португалии большинство преподавателей Центра судебных исследований являются судьями или прокурорами. Для проведения занятий по переподготовке (например, семинаров или кратких курсов) Центр может приглашать преподавателей из частного сектора и других экспертов.

– В Хорватии в разработке и преподавании учебных курсов принимают участие специалисты из полицейских подразделений, которые борются с организованной преступностью и экономическими преступлениями.

– В Бельгии значительный процент бюджета, выделяемого на подготовку судей и прокуроров, находится в распоряжении университетов. Таким образом, у них есть возможность привлекать к проведению некоторых программ экспертов из частного сектора.

Суть подготовки судей и прокуроров по вопросам киберпреступности и электронных доказательств заключается в следующем:

– Судьи и прокуроры, как правило, начинают получать свое образования с изучения права на уровне университета. Следует отметить, что чем больше вопросов, связанных с киберпреступностью и электронными доказательствами, будут регулироваться законом, тем более широкое освещение получат эти вопросы в учебниках и учебных планах в области права. Вместе с тем, возможно, было бы полезно направить предложения по этим вопросам лицам, ответственным за подготовку материалов для университетских курсов.

– В странах, где начальная подготовка проводится в юридических учебных заведениях, было бы целесообразно включить в учебные планы вопросы, связанные с киберпреступностью и электронными доказательствами.

– Это в меньшей степени актуально в тех случаях, когда начальная подготовка проводится на рабочем месте.

– В большинстве стран существуют юридические учебные заведения, которые проводят курсы начальной подготовки, и было бы целесообразно включить в их учебные планы вопросы, связанные с киберпреступностью и электронными доказательствами.

– Учитывая то, что программы переподготовки носят нерегулярный характер, необходимо ввести официальные процедуры одобрения и внесения в учебные планы вопросов, связанных с киберпреступностью и электронными доказательствами и, таким образом придать им официальный статус.

– Программы переподготовки, как правило, носят необязательный характер. Задача заключается в том, чтобы убедить судей и прокуроров в необходимости обучения в таких технических областях, как киберпреступность и электронные доказательства[1].

– Необходимо использовать опыт и знания государственного и частного сектора и учитывать его при разработке учебных курсов, подготовке преподавателей и проведении учебных мероприятий.

4. Навыки и знания, необходимые судьям и прокурорам

Не вызывает сомнения тот факт, что все большее количество уголовных дел, а также многие гражданские и административные дела, рассматриваемые судами, будут в той или иной степени связаны с информационными и коммуникационными технологиями и что большинство судей и прокуроров будут сталкиваться если не с киберпреступностью, то с вопросами, касающимися электронных доказательств. Для этого недостаточно провести специализированную подготовку только судей и прокуроров.

Необходимы широкие *массовые* знания в области киберпреступности и электронных доказательств. Таким образом, всем или максимально возможному количеству судей и прокуроров необходимо пройти, по меньшей мере, базовую подготовку по вопросам, связанным с киберпреступностью и электронными доказательствами. Эти базовые знания необходимо предоставить во время начальной подготовки будущих судей и прокуроров и при проведении программ переподготовки практикующих судей и прокуроров.

[1] В Португалии программы переподготовки являются обязательными (т.е. каждый судья и прокурор должен посетить не менее двух учебных мероприятий в год), а в Румынии переподготовка может быть обязательной при определенных условиях.

В то же время эти вопросы относятся к сфере высоких технологий, которые постоянно развиваются, и мы не можем рассчитывать на то, что судьи и прокуроры в целом смогут быть в курсе технических новинок на протяжении всей жизни. С учетом этого необходимо предоставить знания на продвинутом уровне достаточному количеству судей и прокуроров, которые специализируются на вопросах киберпреступности и электронных доказательств.

4.1 Базовые знания

В большинстве судебных систем невозможно предсказать, какой судья будет рассматривать конкретное дело (принцип естественного права), и поэтому, в конечном счете, все судьи, судьи следственных органов и прокуроры должны обладать базовыми знаниями по вопросам, связанным с киберпреступностью и электронными доказательствами. «Базовые знания» означают, что они должны иметь представление о следующих аспектах:

– Компьютеры и сети: как они работают, базовые принципы функционирования Интернета, роль поставщиков услуг, конкретные задачи судей и прокуроров;

– Киберпреступность: какие информационные и коммуникационные технологии используются для совершения преступления;

– Законодательство о киберпреступности: национальное законодательство (включая прецедентное право) и международные стандарты;

– Юрисдикция и территориальная компетентность;

– Электронные доказательства: технические процедуры и правовые соображения.

В результате прохождения базового курса судьи и прокуроры должны уметь:

– Сопоставлять преступное поведение с положениями национального законодательства;

– Одобрять методы расследования;

– Отдавать распоряжения о поиске и изъятии компьютерных систем для получения электронных доказательств;

– Содействовать международному сотрудничеству;

– Опрашивать свидетелей и экспертов;

– Представлять/обосновывать электронные доказательства.

Ниже приводится пример типичного курса базовой подготовки для судей и прокуроров.

Пример: Подготовка по вопросам киберпреступности и электронным доказательствам – типичный модуль базовых знаний

Цель курса. После окончания курса обучения судьи и прокуроры должны обладать базовыми знаниями о том, что представляет собой киберпреступность и электронные доказательства, как судьи и прокуроры могут рассматривать эти вопросы, какие положения материального и процессуального права, а также какие методы можно применять, насколько оперативными и эффективными были принятие меры и насколько широким было международное сотрудничество.

Занятие 1. О киберпреступности

– Почему киберпреступность вызывает беспокойство?

– Что такое «киберпреступность»?

– Задачи судей и прокуроров.

– Национальное законодательство и международные стандарты.

Занятие 2. Технология

– Функционирование Интернета (базовые принципы)

– Глоссарий терминов

– Протоколы

Занятие 3. Киберпреступление как уголовное преступление в национальном законодательстве

– Преступления против компьютерных данных и систем

– Компьютерное мошенничество и фальсификация

– Преступление, связанные с контентом (детская порнография, ксенофобия, расизм)

– Преступления, связанные с правом на интеллектуальную собственность

– Судебные постановления/прецедентное право

Занятие 4. Электронные доказательства

– Об электронных доказательствах: определения и характеристики

– Требования к электронным доказательствам

– Криминалистическая компьютерная экспертиза

Занятие 5. Процессуальное право/методы расследования

– Юрисдикция и территориальная компетенция

– Оперативное сохранение компьютерных данных

– Судебные приказы/ордеры

– Поиск и изъятие компьютерных данных

– Перехват данных о трафике и контенте

– Меры по обеспечению безопасности

Занятие 6. Взаимодействие с частным сектором

Занятие 7. Международное сотрудничество

– Конвенция о киберпреступности как базовый документ для развития международного сотрудничества

– Общие принципы

– Временные меры и роль круглосуточных контактных пунктов

– Взаимная правовая помощь и роль компетентных органов

Занятие 8. Оценка результатов и выводы

Логистика и материалы. Занятия можно проводить в онлайновом режиме или в аудитории. Если занятия проводятся в аудитории:

– Учебной аудитории с компьютером и проектором для презентаций будет достаточно (поскольку курс не включает практических упражнений, т.е. демонстрации программного обеспечения для криминалистической компьютерной экспертизы или методов расследования, то компьютерная Программа подготовки судей и прокуроров по вопросам киберпреступности: концепция лаборатория не требуется);

– Соответствующие выдержки из национального материального и процессуального законодательства;

– Будапештская конвенция о киберпреступности, включая пояснительный доклад;

– Папка с глоссарием терминов и другой исходной информацией;

– Если лекция читается на иностранном языке, необходимо обеспечить устный перевод и перевод материалов.

4.2 Знания на продвинутом уровне

Иногда для ведения судебного дела о киберпреступлении базовых знаний недостаточно. В таких ситуациях необходимо, чтобы значительное количество судей, судей следственных органов и прокуроров обладали знаниями на продвинутом уровне, чтобы проводить расследование, судебное преследование и выносить решения по сложным делам, связанным в киберпреступлением и электронными доказательствами, или оказать содействия другим прокурорам и судьям.

В одних странах были созданы специализированные судебные подразделения или департаменты (например, в Румынии, Сербии), в других странах более крупные судебные службы имеют в своем распоряжении несколько специально подготовленных прокуроров. В Нидерландах проводится программа *intensiveringsprogramma*, которая, среди прочего, призвана обеспечить наличие, по меньшей мере, одного специально подготовленного прокурора по вопросам киберпреступности в каждом из 11 крупных офисов. В Италии в соответствии с новым законодательством о киберпреступности было создано 29 прокурорских служб, которые обладают юрисдикцией по вопросам киберпреступности. В Португалии в Лиссабонской окружной службе судебного преследования имеется специализированный отдел по компьютерным преступлениям, где проводятся такие расследования.

В некоторых странах специальные прокуроры могут контролировать работу полицейских подразделений, занимающихся преступлениями в сфере высоких технологий. В большинстве стран службы судебного

преследования организованы по иерархическому принципу, когда старший прокурор может поручить дело специально подготовленному прокурору. Таким образом, можно выявить прокуроров, которые должны обладать знаниями на продвинутом уровне.

Что касается судей, то в некоторых странах дела, связанные с киберпреступностью, можно поручить специально подготовленному судье в суде, который рассматривает конкретные виды преступлений, например, дела, связанные с организованной преступностью. Примером (возможно, единственным в Европе) может служить Сербия, где специальный департамент окружного суда Белграда занимается делами, связанными с киберпреступностью. Однако, учитывая то, что в большинстве судебных систем преобладает принцип естественного права, необходимо избрать иной подход. В Нидерландах, пожалуй, в единственной стране в Европе, было создано пять центров со специально подготовленными судьями, которые оказывают содействие другим судьям. В Испании аналогичное предложение обсуждается в Генеральном судейском совете, согласно которому группа судей, специализирующихся на вопросах киберпреступности и электронных доказательствах, будет оказывать содействие и проводить консультации для других судей. В Бельгии не существует специализации, предусмотренной законом, но большинство судов могут попросить одного или более своих членов пройти специальных курс подготовки. Вместе с тем, тот факт, что эти дела передают специально подготовленным судьям, является лишь вопросом внутренней организации работы суда. Иногда компетенцию по рассмотрению таких дел по закону предоставляют специальным судам страны (Брюссель). Однако в большинстве случаев компетенция определяется по месту совершения преступления, где не всегда имеется специально подготовленный прокурор или судья. Во многих странах суды могут рассматривать преступления, связанные с киберпреступностью, гораздо чаще, чем в других странах, что требует и более высокого уровня специализации.

«Знания на продвинутом уровне» означают, что судьи и прокуроры должны иметь практические знания и уметь применять полученные знания по следующим вопросам:

– Компьютеры и сети:

Глоссарий компьютерной лексики и терминов в области киберпреступности;

Функционирование Интернета;

Протоколы и технология;

Роль поставщиков услуг.

– Киберпреступность:

Тенденции в области киберпреступности;

Типология: конкретные типы и методы совершения киберпреступлений (например, «фишинг» или Интернет-мошенничество в целях получения личных данных, бот-сети и другие вредоносные программы, детская порнография);

Практические примеры и имитационные модели.

– Законодательство о киберпреступности:

Национальное законодательство и прецедентное право;

Международное сотрудничество: международные и двусторонние договоры, каналы судебного сотрудничества и практические методы оперативного сотрудничества.

– Расследование и электронные доказательства:

Юрисдикция и территориальная компетенция;

Положения процессуального права и их практическое применение;

Методы поиска, изъятия и хранения электронных доказательств;

Характеристики компьютерного обеспечения для проведения криминалистической компьютерной экспертизы;

Выявление подозреваемых лиц;

Отслеживание потоков денежных средств преступного происхождения;

Меры и условия обеспечения безопасности;

Представление электронных доказательств в суде.

Пример: Подготовка по вопросам киберпреступности и электронным доказательствам – типичный модуль получения знаний на продвинутом уровне[1]

Задача курса. После окончания курса обучения судьи и прокуроры должны обладать и применять на практике знания на продвинутом уровне по следующим вопросам: функционирование компьютеров и сетей, понятие киберпреступности, законодательство о киберпреступности, юрисдикция, методы расследования и электронные доказательства, международное сотрудничество.

Занятие 1. Компьютеры и сети

– Глоссарий компьютерной лексики и терминов в области киберпреступности

– Функционирование ИКТ/инфраструктуры Интернета

Протоколы и технология

Как компьютеры обеспечивают коммуникации

Расследование IP и электронные доказательства – количество и названия компьютеров

[1] Основан на ответах на вопросы анкеты и на примере, предоставленном Нидерландами.

Роль поставщиков услуг

– Информация об Интернете

Сбор информации

Использование (скрытых) баз данных в Интернете

– Характеристики социальных групп

Методы коммуникаций

– Методы сохранения анонимности

– Определение/выявление местонахождения и данных о компьютерах, компаниях или лицах в Интернете

Занятие 2. Киберпреступность и риски для безопасности

– Тенденции в сфере киберпреступности

– Типология: конкретные типы и методы совершения киберпреступлений (например, «фишинг» или Интернет-мошенничество в целях получения личных данных, бот-сети и другие вредоносные программы, детская порнография)

– Как преступники использую информационные и коммуникационные технологии

– Правонарушители

– Последствия киберпреступлений

– Как повысить безопасность ИКТ

– Практические примеры и имитационные модели

Занятие 3. Законодательство о киберпреступности: материальное уголовное право

– Преступление против компьютерных данных и систем

– Компьютерное мошенничество и фальсификация

– Преступления, связанные с контентом (детская порнография, язык вражды)

– Преступления, связанные с правом на интеллектуальную собственность

– Судебные постановления/прецедентное право

Занятие 4. Расследование и электронные доказательства

– Электронные доказательства

Следы/отпечатки в компьютерах, Интернете, при цифровых коммуникациях

Меры по поиску, изъятию и хранению электронных доказательств

Характеристики программного обеспечения для криминалистической компьютерной экспертизы

Выявление подозреваемых лиц

Отслеживание потоков денежных средств преступного происхождения

Меры и условия обеспечения безопасности

Ведение/подготовка дела

Представление электронных доказательств в суде

– Организация и применение права в отношении киберпреступлений/электронных доказательств

– Рассмотрение дел

Занятие 5. Законодательство о киберпреступности: процессуальное право

– Оперативное хранение компьютерных данных

– Подготовка приказов

– Поиск и изъятие компьютерных данных

– Перехват трафика и контента данных

– Меры по обеспечению безопасности

– Взаимодействие с Интернет-провайдерами/частным сектором

– Рассмотрение дел

Занятие 6. Юрисдикция и территориальная компетенция

– Общие принципы

– Юрисдикция в сфере киберпреступности – проблемные аспекты

– Положения о юрисдикции в Конвенции о киберпреступности

– Рассмотрение дел

Занятие 7. Международное сотрудничество

– Конвенция о киберпреступности как базовый документ для развития международного сотрудничества

– Общие принципы

– Временные меры, роль круглосуточных контактных пунктов, сотрудничество с полицией

– Взаимная правовая помощь и роль компетентных органов

– Рассмотрение дел

Занятие 8. Оценка результатов и выводы

Логистика и материалы. Занятия можно проводить в онлайновом режиме или в аудитории. При проведении занятий аудитории необходимо следующее:

– Учебная аудитория с компьютером и проектором для презентаций

– Было бы полезно, если бы у слушателей был компьютер с доступом в Интернет (но это необязательное условие)

– Соответствующие выдержки из национального материального и процессуального законодательства

– Будапештская конвенция о киберпреступности, включая пояснительный доклад

– Папка с глоссарием терминов и другой исходной информацией

– Если лекции читаются на иностранном языке, необходимо обеспечить устный перевод и перевод всех материалов.

Судьям и прокурорам, как правило, не требуются такие технические навыки и знания, которые необходимы следователям, занимающимся расследованием преступлений в сфере высоких технологий и криминалистической компьютерной экспертизой. Тем не менее, возможно, было бы полезно напомнить о необходимости усилий, направленных на регулярное проведение программ подготовки для работников правоохранительных органов.

На средства, предоставленные Европейской комиссией (Программа Фальконе, 2002 г.), Ирландская служба полиции (Гарда Сиочана) при участии экспертов из 10 государств – членов ЕС возглавила проект, в рамках которого была разработана стандартизированная базовая программа по киберпреступности (1-ый уровень) для работников правоохранительных органов. С 2004 г. двухнедельный курс подготовки проводился во многих европейских и неевропейских странах. Курс был аккредитован в Университетском колледже Дублина в 2006 г. (*University College Dublin*).

В ходе реализации дальнейших проектов Ирландской службой полиции в партнерстве с Университетским колледжем Дублина были разработаны дополнительные промежуточные и продвинутые модули для аккредитации программы на получение степени магистра по криминалистической компьютерной экспертизе и расследованию для сотрудников правоохранительных органов во всем мире. Существующие промежуточные модули для сотрудников правоохранительных органов включают следующие компоненты:

– Расследования, связанные с Интернетом;

– Расследования, связанные с использованием компьютерных сетей;

– Криминалистическая экспертиза файловой системы новых технологий (*NTFS*);

– Криминалистическая экспертиза данных под операционной системой *Linux*;

– Криминалистическая экспертиза системы мобильной телефонной связи;

– Беспроводные локальные сети и передача голоса через Интернет (*LANS* и *VOIP*);

– Скриптинг на продвинутом уровне;

– Криминалистическая экспертиза онлайновых данных;

– Криминалистическая экспертиза данных под операционной системой *Microsoft Vista*.

Эти модули постоянно обновляются, а также разрабатываются дополнительные модули[1].

В июле 2007 г. Европол создал Группу по гармонизации подготовки в области киберпреступлений, главной целью которой является координирование усилий по проведению программ подготовки по расследованию преступлений в области высоких технологий в ЕС,

[1] К числу других примеров относятся программы борьбы с преступностью в области высоких технологий, разработанные Службой поддержки национальной полиции Великобритании (*UK National Policing Improvement Agency*).

чтобы разработать сертифицированную учебную программу для следователей правоохранительных органов Европы и распространить ее за пределами ЕС, чтобы помочь правоохранительным органам других стран, которые заинтересованы в этом. В число партнеров входят Европейская комиссия, Европейское бюро по борьбе с мошенничеством (*OLAF*), Агентство Евросоюза по координации национальных систем правосудия (*Eurojust*), Европейский колледж полиции (*CEPOL*), Интерпол, Совет Европы, ООН, Центр расследования киберпреступлений в Университетском колледже Дублина, Технологический университет в Труа, Кентерберийский университет в Крайстчерче, Болонский университет, а также представители промышленности.

4.3. Специализированные знания

Некоторые судьи и прокуроры могут получить специальные знания в рамках программ для аспирантов, с помощью самообразования, сетевого взаимодействия или на основе профессионального опыта. Эти знания не будут являться частью обычных программ подготовки. Судьи и прокуроры, обладающие такими специализированными знаниями, служат ценным источником информации для других и занимаются преподаванием.

5. Текущая подготовка по вопросам киберпреступности и электронным доказательствам

5.1 Начальная подготовка

«Начальная подготовка» означает подготовку слушателей после получения университетского юридического образования, чтобы они могли стать судьями и прокурорами. Во многих системах начальная подготовка проводится в юридических учебных заведениях в течение 1–3 лет; в некоторых странах такая начальная подготовка включает более или менее формализованные практические занятия на рабочем месте без специального учебного плана.

В большинстве стран вопросы о киберпреступности и электронных доказательствах не рассматривают в ходе начальной подготовки или изучают в крайне ограниченном объеме. <...>

Однако в некоторых странах вопросы киберпреступности и электронных доказательств являются неотъемлемой частью программ начальной подготовки. Например:

– В Нидерландах программа начальной подготовке включает однодневный базовый курс по киберпреступности, который преподается в Институте по подготовке прокуроров и судей (*SSR*) в Утрехте или

в Зютфене и включает учебные пособия и другую исходную информацию. Курс включает интерактивные семинары и рассмотрение дел. Кроме этого, помимо однодневного базового курса и тщательной подготовки в течение четырех дней, программа включает двухдневный мастер-класс.

– В Испанской школе судей проводится курс начальной подготовки по киберпреступности и электронным доказательствам для недавно назначенных судей, который включает вопросы процессуального и материального права. Он является частью обязательной программы подготовки по процессуальному праву и сбору доказательств. Вопросы киберпреступности и электронных доказательств освещаются на семинарах в течение четырех дней, которые включают аспекты национального законодательства, инструменты международного сотрудничества, демонстрацию программы для проведения криминалистической компьютерной экспертизы и методы расследования, изъятия электронных доказательств и рассмотрение конкретных дел. Кроме того, раз в год проводится специальный семинар по электронным доказательствам, а также еще один семинар по материальному праву (преступления, совершенные с помощью электронных средств). Эти семинары проводят специалисты в области права и ИТ. Кроме того, судьи имеют доступ к виртуальной библиотеке по электронной преступности. Целью этого курса начальной подготовки является предоставление базовых знаний.

– В «бывшей югославской Республике Македония» Академия по подготовке судей и прокуроров проводит курс начальной подготовки по киберпреступности и электронным доказательствам в рамках учебной программы по уголовному праву, ИТ и проведению обысков. Десять часов отводится на киберпреступность и электронные доказательства.

– В Португалии киберпреступность не является специальной и самостоятельной дисциплиной в учебном плане. Однако в разделе, посвященном уголовному расследованию, проводится специальный семинар (полтора часа учебного времени) по киберпреступности и электронным доказательствам. Во время занятий по уголовному праву и уголовно-процессуальному праву 9 часов отводится на компьютерные преступления и процессуальные аспекты получения электронных доказательств, и 9 часов посвящены ИКТ. Эти занятия проводят штатные преподаватели, судьи, прокуроры или адвокаты, обладающие опытом в этой области, сотрудники специализированных полицейских подразделений, эксперты в области ИТ или специалисты из частных компаний.

Имеющаяся информация позволяет сделать следующие выводы:

– Учитывая задачу по предоставлению всем судьям и прокурорам базовых знаний в области киберпреступности и электронных доказательств, предлагаемые программы подготовки носят весьма ограниченный характер.

– За крайне незначительным исключением, программы начальной подготовки включают лишь базовые знания, и проведение программ подготовки на продвинутом уровне не предусматривается.

– Стандартизированные учебные пособия для тиражирования знаний, как правило, отсутствуют.

5.2. Переподготовка

Программы переподготовки, т.е. дальнейшего профессионального обучения действующих судей и прокуроров, проводятся государственными юридическими учебными заведениями, а также могут проводиться рядом других организаций. Например:

– Во Франции Национальная школа подготовки судей проводит в школе пятидневный семинар на продвинутом уровне, а также предлагает двухдневную стажировку в бюро по борьбе с преступностью в сфере высоких технологий министерства внутренних дел (*OLCTIC*). Расходы (около 5000 евро за курс) покрываются за счет школы. В качестве преподавателей работают судьи, прокуроры, сотрудники полиции, эксперты в области ИТ или отобранные эксперты из промышленности.

– В Грузии Высшая школа судей является единственным учебным заведением, отвечающим за переподготовку судей. В ней проводятся двухдневный базовый курс по киберпреступности, который финансируется из государственного бюджета. В качестве преподавателей работают члены профессорско-преподавательского состава и судья Верховного и апелляционных судов. Подготовку прокуроров проводит учебное подразделение министерства юстиции, но курсы по киберпреступности и электронным доказательствам пока не были организованы.

– В Германии программы переподготовки судей и прокуроров проводит Академия по подготовке судей Германии, которая организует около 150 мероприятий в год. В 2009 г. два из этих учебных мероприятий посвящены киберпреступности, и каждое из них проводится в течение 4 дней. Как правило, занятия проводят прокуроры и судьи, обладающие опытом в области киберпреступности, а также сотрудники полиции, таможни, налоговых органов и т.п. Расходы на подготовку покрывают федеральные и местные органы государственного управ-

ления. На этих курсах слушатели получают базовые знания и знания на продвинутом уровне.

– В Нидерландах, несмотря на то, что программы переподготовки носят необязательный характер, каждый судья должен ежегодно проходить подготовку в течение определенного количества учебных часов. Каждый судья может решить, какой курс (курсы) ему выбрать. Институт по подготовке судей и прокуроров (*SSR*), а также несколько других учебных заведений и образовательных центров послевузовской подготовки проводят программы переподготовки по киберпреступности и электронным доказательствам на базовом и продвинутом уровнях. Ежегодно SSR предлагает три базовых курса, три курса углубленного обучения и один мастер-класс. В качестве преподавателей работают специалисты из национальной службы уголовного преследования, а также эксперты из частных компаний и промышленности. Кроме того, *SSR* также предлагает широкий перечень других курсов подготовки, охватывающих правовые и практические аспекты (всего около 400 курсов). Таким образом, подготовка по вопросам киберпреступности должна конкурировать со всеми этими курсами.

– В Польше Польская национальная школа судей и прокуроров проводит курсы подготовки на базовом и продвинутом уровнях в форме конференции, которая продолжается 4–5 дней. В 2009 г. было организовано два таких мероприятия («Методика преступлений, совершенных с использованием информационных систем», «Электронные доказательства во время слушания дела»).

– В Румынии Национальный институт судей проводит программу переподготовки, но только на базовом уровне. Например, с 2006 по 2009 гг. ежегодно проводилось по два двухдневных семинара, каждый из которых был рассчитан примерно на 25 судей/прокуроров. Они финансировались в основном из бюджета Национального института, частично за счет средств Европейской комиссии (PHARE) и частично за счет поддержки (в 2006 г.) компании eBay. В качестве преподавателей работали румынские судьи, специалисты в области ИТ, а также иностранные эксперты, финансирование которых осуществляли такие организации, как Совет Европы. Более того, киберпреступность является обязательным предметом децентрализованных программ подготовки на уровне отделов судебных расследования при апелляционных судах. Эти программы также координирует Национальный институт судей.

– В Испании Испанская школа судей при Генеральном совете судей проводит курсы переподготовки судей по киберпреступности и электронным доказательствам. Для прокуроров эти программы подготовки

предлагает Центр правовых исследований при министерстве юстиции. В обоих случаях программы подготовки организованы в сотрудничестве с *CYBEX*, частной компанией, специализирующейся на этих вопросах. Бюджет Школы судей на программы обучения по киберпреступности составляет около 42 000 евро. Также возможно финансовая поддержка со стороны частного сектора. Программы переподготовки проводятся на базовом уровне, продолжаются 3–4 дня и включают лекции и анализ практических дел. Для слушателей издаются учебные пособия, которые, как правило, получает каждый судья. В 2008 и 2009 гг. ежегодно проводилось по два таких семинара. Несмотря на то, что некоторые вопросы изучаются достаточно глубоко, регулярные учебные программы на продвинутом уровне пока не проводятся.

– В Португалии программы переподготовки по киберпреступности проводит Центр исследований судебной системы, который организовывает около 30 мероприятий в год. Два их них регулярно посвящены основным проблемам киберпреступности. Иногда проводятся другие семинары на смежные темы, например, авторское право в онлайновой сети или технология и суды. Занятия проводят судьи и прокуроры, юристы, сотрудники полиции и эксперты из государственного и частного секторов. Семинары пользуются популярностью и привлекают большое количество участников (в основном, прокуроров, но также адвокатов и судей уголовных судов).

– В Бельгии программа переподготовки до сих пор находится на этапе разработки, что связано с недавним созданием Института подготовки судей. Несомненно, задача заключается в том, чтобы организовать такой процесс обучения, в котором бы учитывались результаты и рекомендации ряда научно-исследовательских институтов и, в том числе, замечания Совета Европы. Институт может профинансировать участие бельгийских судей в программах подготовки за рубежом по их просьбе<...>

– В настоящее время в Хорватии не проводятся программы переподготовки по киберпреступности и/или электронным доказательствам. Этот вопрос обсуждался только благодаря программе *CARDS*, в которой участвует Хорватия.

– В «бывшей югославской Республике Македония» не существует программ переподготовки.

– Программы подготовки предлагает Академия европейского права *(ERA*). *ERA*, официально созданная по инициативе Европейского парламента в 1992 г., направляет свою деятельность на предоставление углубленных знаний и проведение анализа европейского права и права

Сообщества, организуя практические семинары и курсы для практикующих юристов. Академия также служит форумом для обмена опытом и мнениями о европейском праве и политике. *ERA* на регулярной основе организует открытые учебные мероприятия по киберпреступности, в которых участвуют слушатели из всех стран ЕС. В 2009–2010 гг. *ERA* также сотрудничает с Программой *TAIEX* (Техническое содействие в сфере информационного обмена), в рамках которой проводятся и будут проводиться циклы семинаров в Румынии, Болгарии, странах-кандидатах и странах потенциальных кандидатах на вступление в ЕС, чтобы ознакомить их с основными европейскими и международными инструментами борьбы с киберпреступностью.

Все семинары предназначены для использования в качестве площадок для дебатов и оценки того, как европейское законодательство в области киберпреступности применяется в разных государствах-членах и странах-кандидатах, а также перспектив для проведения эффективной общеевропейской кампании против незаконного использования Интернета. В настоящее время обсуждаются такие недавно принятые европейские правовые акты, как Конвенция Совета Европы о киберпреступности (2001 г.), Рамочное решение Совета 2005/222/*JHA* об атаках на информационные системы и Рамочное решение Совета 2004/68/*JHA* о борьбе против сексуальной эксплуатации детей и детской порнографии. Также рассматриваются вопросы дальнейшего сотрудничества с поставщиками услуг и веб-компаниями *Google, Microsoft и Yahoo!*.

На каждом семинаре используется программа, включающая комплексные методы обучения: вводные и более углубленные лекции, рассмотрение дел и другие виды интерактивного обучения. Особое внимание уделяется обсуждению в небольших рабочих группах. Курсы лекций и практические занятия проводят эксперты ЕС и национальные эксперты.

– В ряде стран учебные мероприятия финансируются частными компаниями. Например:

В Германии компания *eBay* финансирует учебный курс «Новые СМИ и уголовное право» для судей и прокуроров, который организован Немецкой академией подготовки судей. Курс ведет преподаватель, который предоставляет информацию о рынке компании *eBay*, связанной с ним уголовной деятельностью, используемых мерах противодействия и взаимодействии компании с правоохранительными органами. Компания *eBay* также участвовала в нескольких «одноразовых» курсах подготовки, которые были организованы Берлинским сенатом юстиции, в каждом из которых приняли участие около 100 прокуроров.

В Румынии компания *eBay* провела многочисленные учебные мероприятия для судей, прокуроров и сотрудников правоохранительных органов. В частности, компания *eBay* работала с Секретной службой США в Посольстве США, где проводился курс подготовки для 25 прокуроров из разных отделений *DIICOT* (Директорат по расследованию организованной преступности и терроризма), 15 судей и 20 сотрудников полиции в Сибиу. Кроме того, компания *eBay* принимала участие в организации дополнительных учебных мероприятий для судей в Таргу Жиу, а также для 60 судей из разных судов при апелляционном суде Крайовы.

Как отмечалось выше, практически во всех случаях внесение изменений или дополнений в учебные планы юридических учебных заведений требует проведения формальной оценки и процедур одобрения[1].

Несмотря на то, что, несомненно, многие инициативы направлены на удовлетворение необходимости в проведении адекватных курсов подготовки по киберпреступности для судей и прокуроров, со всей очевидностью ощущается отсутствие согласованности между описанными выше подходами.

Даже принимая во внимание национальные особенности законодательства и тот факт, что системы образования существенно отличаются друг от друга, проблемы киберпреступности носят международный характер и их решение требует минимального уровня координирования усилий и согласованности действий между странами. Одинаковое понимание проблем киберпреступности в разных странах может только улучшить согласованность судебных постановлений и предотвратить создание «надежных убежищ» для преступников, предоставив учебным заведениям экономически выгодные качественные и содержательные учебные программы.

Имеющаяся информация позволяет сделать следующие выводы:

– Большинство курсов переподготовки предоставляют знания на базовом уровне.

[1] В этой связи представляет интерес проект «Европейский сертификат по борьбе с киберпреступностью и использованию электронных доказательств (*European Certificate on the fight against cybercrime and the use of electronic evidence*), который осуществляет *CYBEX* при финансовой поддержки Европейской Комиссии (*JPEN*). Он включает четырехдневный стандартизированный базовый курс подготовки для судей, прокуроров и юристов. С начала 2009 г и по конец 2010 г. курс будет апробирован в 14 пилотных странах Европы и Латинской Америки. Его участники получат сертификат, свидетельствующий о том, что они получили базовые теоретические и практические, правовые и технические знания по вопросам, связанным с электронными доказательствами и киберпреступностью.

Совет Европы – в рамках Проекта по киберпреступности – также приступил к разработке учебногопособия для судей и прокуроров для использования во время двухдневного базового курса, посвященного законодательству о киберпреступности.

– Проводится крайне мало курсов, которые охватывают лишь очень незначительное количество судей и прокуроров.

– В большинстве случаев базовые курсы не стандартизированы. Таким образом, их тиражирование не представляется возможным, и они не позволяют судье или прокурору пройти системный курс обучения от базового уровня до продвинутого уровня. Судя по всему, исключением являются Нидерланды.

– Учебные пособия носят разрозненный и бессистемный характер.

– Учитывая то, что, в конечном счете, всем судьям и прокурорам необходимо получить, по меньшей мере, базовые знания в области киберпреступности и электронных доказательств, предлагаемых программ подготовки явно недостаточно, особенно принимая во внимание то, что нынешнее поколение практикующих судей и прокуроров скорее всего не получили никакой начальной подготовки и не изучали эти темы во время учебы в университете.

– Несмотря на незначительные исключения, программы подготовки судей и прокуроров на продвинутом уровне отсутствуют.

– Принимая во внимание международный характер киберпреступности, необходимо обеспечить минимальный уровень координирования и согласованности действий между разными странами.

6. Предлагаемый подход

6.1. Цель

Как было продемонстрировано в предыдущем разделе, в целом существующие программы подготовки и переподготовки не дают судьям и прокурорам такого уровня знаний, который необходим для рассмотрения дел, связанных с киберпреступностью и электронными доказательствами.

Таким образом, концепция подготовки судей и прокуроров должна быть направлена на решение следующих задач:

– Предоставить возможность учебным заведениям проводить программы начальной подготовки и переподготовки по вопросам киберпреступности, основанные на международных стандартах;

– Вооружить максимально возможное количество будущих и практикующих судей и прокуроров базовыми знаниями по вопросам киберпреступности и электронных доказательств;

– Предоставить программы подготовки на продвинутом уровне значительному количеству судей и прокуроров;

– Стимулировать дальнейшую специализацию и техническую подготовку судей и прокуроров;

– Содействовать расширению знаний с помощью сетевого взаимодействия между судьями и прокурорами;

– Облегчить доступ к разным учебным инициативам и сетям.

Для достижения этих целей следует принять следующие меры:

6.2. Институционализация начальной подготовки

– Странам, где начальная подготовка представляет собой практическое обучение на рабочем месте (прохождение практики или стажировки) без формально оформленного учебного плана, рекомендуется, чтобы, по меньшей мере, часть этого обучения (например, одна стажировка или аналогичный тренинг) была связана с киберпреступностью и электронными доказательствами.

– Странам, где начальная подготовка проводится в юридических учебных заведениях, необходимо принять следующие меры:

Их учебные планы должны включать, как минимум, один базовый модуль по киберпреступности и электронным доказательствам;

Эти проблемы следует дополнительно обсуждать при изучении обязательных модулей по материальному и процессуальному праву;

Необходимо предлагать факультативные модули для получения знаний о киберпреступности и электронных доказательствах на продвинутом уровне.

Следует стандартизировать специальные учебные модули таким образом, что бы их можно было тиражировать и предоставить возможность слушателям пройти курс обучения с базового уровня до продвинутого уровня. Тиражирование модулей означает, что их можно неоднократно использовать, по меньшей мере, в одной стране для разных слушателей, чтобы участники различных учебных мероприятий получили знания на одинаковом уровне. Это также означает, что обеспечивается стандартизация методов проведения подготовки. В целях обеспечения высокого качества подготовки после окончания каждого курса необходимо проводить оценку знаний.

6.3. Институционализация переподготовки

– Учебные заведения по переподготовке кадров должны предлагать, по меньшей мере, один базовый модуль по киберпреступности и электронным доказательствам, чтобы вооружить практикующих судей и прокуроров базовыми знаниями, если они не получили их во время прохождения курса начальной подготовки.

– Они должны также предлагать курсы подготовки на продвинутом уровне.

– И вновь: следует стандартизировать специальные учебные модули таким образом, чтобы их можно было тиражировать и предоставить возможность слушателям пройти курс обучения с базового уровня до продвинутого уровня. Для этого может возникнуть необходимость в максимально возможной гармонизации модулей программ переподготовки с модулями программ начальной подготовки. Необходимо также стандартизировать методы обучения и обеспечить контроль качества путем оценки знаний после окончания курсов.

– Для подготовки судей и следователей узкой специализации можно было бы способствовать проведению стажировок в подразделениях по борьбе с преступностью в сфере высоких технологий или организовать послевузовские курсы/программы[1].

6.4. Стандартизация и тиражирование курсов/модулей

– Следует разработать стандартизированные курсы или модули, которые можно было бы эффективно тиражировать в широких масштабах, чтобы предоставить возможность слушателям и практикующим судьям и прокурорам пройти курс обучения с базового уровня до продвинутого уровня.

– Необходимо провести оценку существующих базовых курсов[2], которые можно было бы включить в учебные планы программ начальной подготовки и переподготовки. Стандартный курс впоследствии можно было бы рекомендовать учебным заведениям, проводящим программы начальной подготовки и переподготовки.

– Аналогичной оценке можно было бы подвергнуть курсы подготовки на продвинутом уровне и затем рекомендовать учебным заведениям стандартные курсы на продвинутом уровне.

– И, наконец, необходимо провести подготовку преподавателей, чтобы они могли вести такие курсы, чтобы занятия проводили местные преподаватели на местных языках при ограниченном участии международных тренеров[3].

---

[1] Например, двухнедельный базовый курс, разработанный Ирландской службой полиции иУниверситетским колледжем Дублина (*UCD*), должен также представлять интерес для судей и прокуроров.

[2] Например, курс *ECCE*, разработанный и в настоящее время апробируемый *CYBEX*.

[3] Курс подготовки преподавателей был разработан *UCD* и ИНТЕРПОЛОМ, и его можно было бы использовать. Курс включает навыки преподавания, разработку курса и т.п. Этот курс НЕ предназначен исключительно для правоохранительных органов и может проводиться для всех.

6.5. Доступ к учебным пособиям и материалам для самообучения

– Необходимо разработать учебные пособия, отражающие общие международные стандарты и передовую практику. Они должны быть предоставлены учебным заведениям по конкурентным ценам для распространения на местах. Несомненно, несмотря на то, что высокий уровень стандартизации возможен при разработке программ подготовки для сотрудников правоохранительных органов, в которых особый акцент делается на технологии и криминалистической экспертизе, это в меньшей степени относится к подготовке судей и прокуроров, которых, в первую очередь, необходимо научить применять национальное законодательство. Тем не менее, разработка стандартизированных учебных пособий возможна таким образом, чтобы осталось достаточно места для того, чтобы включить в них национальные системы и законодательство.

– В некоторых странах учебные пособия для судей и прокуроров имеются в онлайновом режиме[1]. Другие страны должны последовать этой практике.

– Необходимо разрабатывать и предоставлять онлайновые курсы[2].

– Следует максимально облегчить доступ к учебным курсам (национальным и международным) с помощью упрощенных процедур одобрения.

6.6. Пилотные центры подготовки на базовом и продвинутом уровнях

– Следует создать ряд пилотных центров подготовки судей и прокуроров по вопросам киберпреступности и электронным доказательствам на базовом и продвинутом уровнях.

Эти центры могли бы:

Апробировать и осуществлять дальнейшую разработку стандартизированных курсов и материалов;

Распространять передовую практику;

Проводить исследования в области обучения;

---

[1] Примерами служат Нидерланды и библиотека электронных доказательств *CYBEX*. В рамках проекта «2 Центра», *UCD* будет разрабатывать онлайновые ресурсы для предоставления некоторых учебных пособий *AGIS/ISEC*.

[2] Например, в настоящее время *UCD* предлагает две программы *MS*, отдельные разделы которых полностью представлены в онлайновом режиме. В Португалии Центр подготовки судей намерен создать онлайновый курс «Суды и информационные и коммуникационные технологии», включающий модули по киберпреступности и электронным доказательствам<...>

Вести учет преподавателей;

Проводить подготовку преподавателей;

Предоставлять программы подготовки другим странам с аналогичными системами и языками.

Пилотные центры должны координировать свою работу друг с другом при поддержке Совета Европы.

– Судья и прокуроры, которые готовы стать специалистами, должны подумать об участии в

учебных программах в центрах повышения квалификации для правоохранительных

органов и промышленности[1].

6.7. Расширение знаний за счет сетевого взаимодействия

Несмотря на то, что программы начальной подготовки и переподготовки позволяют судьям и прокурорам закладывать основы отношений, обмениваться мнениями между коллегами и налаживать сетевое взаимодействие, важнейшую роль также играет взаимодействие с широким кругом других заинтересованных сторон.

Таким образом:

– Судья и прокуроры должны использовать существующие сети для судей[2] или прокуроров (например, *GPEN*)[3].

---

[1] Проект «2 Центра» (Центры повышения квалификации по вопросам киберпреступности сети аналитических исследований и образования) (2*Centre initiative (Cybercrime Centres of Excellence Network for Training Research and Education*) был запущен в марте 2009 г. (во время Конференции Совета Европы, «Октопус»). В рамках проекта 2*Centre* «изучаются существующие методы подготовки правоохранительных органов и промышленности по вопросам криминалистической экспертизы ИТ и расследования киберпреступлений. Проект посвящен рассмотрению деятельности сотрудников правоохранительных органов и соответствующего персонала в промышленности, направленной на получение знаний и навыков в области, в которой в настоящее время существует разнообразные уровни профессиональной подготовки, обучения в собственном учреждении, перекрестного обучения и обучения на рабочем месте». Университетский колледж Дублина стал первым центром повышения квалификации, в 2010 г. вторым центром станет Университет в городе Труа.

[2] Складывается впечатление, что международной сети судей, охватывающей проблемы киберпреступности и электронных доказательств, пока не существует. Примером инициативы на национальном уровне могут служить Нидерланды, где был создан внутренний ресурс Интранет типа «вики».

[3] Глобальная сеть для прокуроров, занимающихся электронными преступлениями (*GPEN*), была создана в 2008 г. и поддерживается Международной ассоциацией прокуроров (*IAP*). Сеть облегчает информационный обмен и сотрудничество между прокурорами по делам, связанным с электронными преступлениями или киберпреступностью, принимая во внимание Конвенцию о киберпреступности, и способствует разработке и проведению учебных программ, предоставлению прокурорам онлайновых ресурсов.

– Совет Европы должен обсудить создание международной сети по киберпреступности или сети судей, занимающихся рассмотрением дел об электронных преступлениях (аналогичной сети *GPEN* для прокуроров).

– Взаимодействие между европейскими институтами, проводящими программы подготовки по вопросам киберпреступности и электронным доказательствам, должно опираться на поддержку Совета Европы и Европейской сети по подготовке судей.

– Чтобы облегчить судьям и прокурорам доступ к этим и многим другим сетям, связанным с киберпреступностью, Совет Европы – на своем сайте *www.coe.int/cybercrime* – должен составить список инициатив и сетей и создать портал с указанием ссылок, краткой информацией и контактными данными различных сетей. Это также будет способствовать координированию работы сетей. В дальнейшем это облегчит доступ к существующим учебным материалам и инициативам.

6.8. Государственно-частное сотрудничество

Структурированное и регулируемое сотрудничество между правоохранительными органами и частным сектором (отраслью ИКТ, включая Интернет-провайдеров) жизненно важно для расследования киберпреступлений и получения электронных доказательств[1], и частный сектор передает правоохранительным органам свои опыт и знания и оказывает другую поддержку их инициативам в области обучения.

Поддержка частного сектора в подготовке судей и прокуроров была бы полезной, учитывая то, что частный сектор обладает соответствующим опытом в области знания предмета. В то же время, судьи и прокуроры должны оставаться независимыми и беспристрастными.

Таким образом:

– Юридические учебные заведения могут использовать опыт и знания частного сектора при разработке учебных программ, подготовке учебных пособий и проведении курсов обучения.

– Поддержка учебных заведений со стороны промышленности не должна сводиться к принятию потенциально выгодных решений

GPEN – это сеть для прокуроров, специализирующихся на электронных преступлениях, и каждый член *IAP* получает приглашение назначить, по меньшей мере, одного прокурора для регистрации в *GPEN* в качестве национального контактного лица. Работой сети руководит Правление развития *GPEN*, которое состоит из членов *IAP*.

[1] См. в качестве примера Руководящие принципы сотрудничества правоохранительных органов и Интернет-провайдеров, принятые на Конференции Совета Европы «Октопус» в апреле 2008 г.

в суде или стимулировать развитие бизнеса, а призвана обеспечивать судей и прокуроров адекватной информацией, позволяющей им принимать информированные решения.

– Частный сектор мог бы оказывать прозрачную поддержку международным или национальным организациям, научному сообществу, инициативам в области образования и другим третьим сторонам, которые в свою очередь поддерживают учебные заведения.

– Судьи и прокуроры должны иметь общее представление об Интернете и киберпреступности, но не менее важно предоставить им платформу для специализированной информации. Промышленность могла бы предоставить материалы для конкретных модулей (а не для полного курса), посвященных функционированию соответствующих платформ.

7. Оказание поддержки в реализации настоящей концепции

Реализация настоящей концепции, в первую очередь, является ответственностью юридических учебных заведений, но также нуждается в поддержке государственных и частных институтов и партнеров, в том числе международных организаций. Принимая во внимание значение для общества информационных и коммуникационных технологий, финансирование таких мер по проведению подготовки станет ценным вложением наряду с усилиями, которые следует приложить, чтобы предоставить учебным заведениям необходимые ресурсы.

Совет Европы и Европейская сеть по подготовке судей, а также другие организации должны способствовать реализации настоящей концепции во всей Европе и за ее пределами.

Европейская сеть по подготовке судей и Совет Европы могли бы в ближайшем будущем организовать совместную конференцию для обсуждения этой концепции.

Совет Европы и Европейская сеть по подготовке судей должны регулярно проводить оценку достигнутых результатов.

Реализация концепции на практике также должна опираться на поддержку донорских организаций. Заинтересованные доноры и организации могли бы стать партнерами в разработке проектов оказания содействия учебным заведениям и другим заинтересованным сторонам, которые готовы взять на себя ответственность за принятие мер, предусмотренных концепцией.

Для снижения риска возникновения конфликта интересов или дискредитации беспристрастности судей и прокуроров, доноры не должны

оказывать прямую поддержку, а могли бы предоставлять ресурсы через нейтральные третьи стороны, например международные организации, которые затем взаимодействовали бы с учебными заведениями.

8. Приложение

8.1 Лиссабонская сеть: связи с юридическими учебными заведениями

В Лиссабонской сети представлены 44 из 47 государств-членов Совета Европы. Членами Лиссабонской сети являются соответствующие национальные институты, отвечающие за начальную и дальнейшую подготовку судей и прокуроров. В зависимости от обстоятельств, членами сети могут быть Школы по подготовке судей, Центры юридической подготовки или подразделения по подготовке судей при министерствах юстиции.

<...>

8.2. Примеры базовых учебных курсов: структура и тематика

8.2.1. Пример Нидерландов

Базовая подготовка – 1 день

Программа:

1. Общая ориентация:

Что представляет собой киберпреступность?

Проявление киберпреступности

Законодательно-правовые рамки для правоприменения и судебного преследования

2. Правоприменение:

Цифровое правоприменение как повседневная практика

Методы правоприменения

3. Правоприменение (часть 2):

Интернет и правоприменение в соответствии с Актом о специальных привилегиях правоприменения

Выводы + оценка

8.2.2. Пример Германии (Академия по подготовке судей Германии)

Базовая подготовка: «Формы проявления и стратегия борьбы с киберпреступностью» – 4 дня

Программа:

День 1:

– Уголовный кодекс Германии

– Использование Уголовного кодекса Германии в контексте компьютерной и Интернет-преступности

– Проблемы повседневного опыта работы в прокуратуре и суде<...>

– Проблемы в повседневном опыте работы в прокуратуре и суде в Нидерландах

– Раскрытие и борьба с киберпреступностью в Европе

– Проблемы с провайдерами в Нидерландах и других европейских странах

– Конвенция Совета Европы о киберпреступности

– Важность и значение Конвенции о киберпреступности для Европы и остальных стран мира (Китай, США, Россия) <...>

День 2:

– Саботаж компьютерных систем

– Деятельность хакеров в Интернете

– Ловушки заказов в Интернете

–Шпионаж данных

– Компьютерное мошенничество с кредитными картами

– Атаки на банковские данные

– Фишинг-мошенничество и новые виды преступлений в Интернете

– Бот-сети

– Мошенничество в компании *eBay* или других платформ продаж<...>

– Превентивные поиски в Интернет случаев организованной преступности, терроризма, жестоких преступлений, отмывания денежных средств и т.п.

– Поиск в Интернете объявлений лиц с приступнообразным сознанием (школы и т.п.)

– Поиск в Интернете детской порнографии

– Международное сотрудничество в сфере поиска в Интернете

– Онлайновый поиск (проблемы, связанные с конституцией)<...>

День 3:

– Хранение и оценка данных в Германии и других странах

– Поиск данных в Интернет и отслеживание данных в сети

– Возможности криминалистической экспертизы ИТ и ограниченность анализа данных

– Системы размещения анонимных данных в Интернете

– Использование преступниками криптографии<...>

– Новые правовые проблемы, связанные с хранением и оценкой Интернет-данных

– Компетенция по применению всех правовых мер поиска

– Компетенция по получению доказательств для расследования и суда

– Новые факторы в сфере правоприменения<...>

День 4:

– Российская предпринимательская сеть

– Интеркейдж

– Защита от диверсий в отношении компьютеров или данных

– Позитивное «хакерство»

– Значение и фальсификации при использовании машин для голосования

– Политическое влияние новых законов

– Население, которое сидит в стеклянном доме<...>

8.2.3. Примеры Совета Европы

1. Практический семинар по киберпреступности для прокуроров, Белу-Оризонти,

Бразилия, 26 августа 2008 г. (организован Ministério Publico Estadual Minas Gerais

совместно с Советом Европы)

Базовая подготовка – 1 день

Программа:

1. Открытие семинара

– Вступительное слово

–Текущие законодательные реформы

2. Киберпреступность: новое явление

– Обзор существующих угроз

– Конкретные угрозы и дела, расследованные в Бразилии

3. Материальное право: каков характер правонарушений?

– Международные стандарты

– Типология, правовые концепции

– Конвенция о киберпреступности

– Положения бразильского законодательства

– Действующие положения

– Проведение правовых реформ

4. Расследования и международное сотрудничество

– Роль прокуроров в расследовании киберпреступлений

– Национальное процессуальное право

– Процессуальные меры и международное сотрудничество в рамках Конвенции о киберпреступности

5. Государственно-частное партнерство

– Примеры государственно-частного партнерства в Бразилии

– Правоприменение – сотрудничество Интернет-провайдера при расследовании киберпреступлений: руководящие принципы

– Обсуждение: сотрудничество между правоохранительными органами и Интернет-провайдерами: опыт Бразилии

2. Киберпреступность: курс подготовки для судей, Каир, Египет, 9–10 июня 2008 г.

(организован компанией Microsoft при содействии Совета Европы)

Настоящий курс проводился дважды для разных групп судей из коммерческих судов (они также отвечали за вопросы, связанные с электронными преступлениями)

Базовая подготовка – 1 день

Программы:

1. Открытие семинара

2. Киберпреступность: новое явление

– Обзор существующих угроз

– Конкретные угрозы

Мошенническое использование онлайновой идентификации и информации: примеры

Кредитные карты и другие виды мошенничества

3. Материальное право: каков характер правонарушений?

– Международные стандарты (эксперт Совета Европы)

Типология, правовые концепции

Конвенция о киберпреступности

Криминализация хищения персональных данных

– Положения национального законодательства

Действующие положения

Проведение правовых реформ

Часть 2. Доказательства в ходе судебного разбирательства дел, связанных с киберпреступностью

4. Расследование и уголовное преследование

– Процессуальные меры, предусмотренные Конвенцией о киберпреступности

– Роль полиции, прокуроров, судей, специализированных служб

– Национальное процессуальное право

5. Международное сотрудничество

– Конвенция о киберпреступности

– Положения национального законодательства и двусторонних договоров

– Круглосуточные контактные пункты
– Роль судей
6. Получение, сохранение, использование электронных доказательств
– Доказательства, находящиеся в компьютере обвиняемого: наличие цифровых файлов, использованных для киберпреступления
– Доказательства, идентифицирующие местонахождения сети: *IP* адреса
– Доказательства, полученные от Интернет-провайдеров
7. Судебное разбирательство и прецедентное право: примеры

8.3. Примеры курсов подготовки на продвинутом уровне: структура и тематика

8.3.1. Пример Нидерландов

Углубленная подготовка – 4 дня
Программа:
1-й и 2-й дни
Инфраструктура Интернета
– Представление о том, как работает Интернет
– Как связаны компьютеры?
– Что представляют собой *IP*-номера и компьютерные имена?
Информация об Интернете
– Как осуществлять сбор информации в Интернете
– Поиск (скрытых) баз данных в Интернете
Характеристики социальных сетей
– коммуникации
– анонимность
– определение местонахождения и идентификация компьютеров, компаний и
лиц в Интернете
Цифровые следы
– Что представляют собой «следы»?
– Какие следы остаются в компьютере?
– Какие следы остаются в Интернете?
– Какие следы можно обнаружить в цифровых коммуникациях?
Безопасность
– Риски, связанные с Интернетом
– Важность надежной цифровой безопасности
– Безопасное хранение информации
– Безопасность электронной почты

В течение этих двух дней каждый участник получает доступ к компьютеру, подсоединенному к Интернету, и получает практический опыт по обсуждаемым темам. Участникам сообщают имя определенного лица и просят собрать о нем как можно больше информации из открытых источников в Интернет. Их также просят отследить отправителей электронных писем (с помощью заголовков электронных писем) или найти следы цифровых коммуникаций.

3-й и 4-ый дни

Законодательно-правовая база

– Какой компетенцией обладают полиция и прокуроры при расследования дел,

связанных с киберпреступностью

– Рассмотрение дела группой по преступлениям в сфере высоких технологий

Организация расследования и судебного преследования киберпреступности в Нидерландах;

Перехват (это не будет включено в новый курс, поскольку является частью базовой программы);

Цифровые встречные иски

– Какие встречные иски известны

– Прецедентное право в отношении встречных исков

– Какие встречные иски можно ожидать в будущем и какой будет реакция на них

– Рассмотрение дел

Каждый участник получает учебные пособия, папку, которая включает все темы, обсуждаемые во время семинара, и которую можно использовать как справочное пособие, а также распечатки всех презентаций преподавателей и книгу Аржана Дасселаара *(Arjan Dasselaar) Handboek Digitale Criminaliteit*.

8.3.2. Предложение Нидерландов по проведению мастер класса

Разработка нового курса по киберпреступности

«Интенсивная программа подготовки по киберпреступности» (*Intensiveringsprogramma Cybercrime*), Национальный прокурор по киберпреступности и Институт по подготовке прокуроров и судей в Нидерландах (*SSR*) занимаются разработкой нового курса по киберпреступности, который охватывает широкий перечень тем: начиная с вопросов «перехвата» и кончая мастер-классами по киберпреступности в конкретных областях (бот-неты).

Пока работа над программой не завершена, но первый день будет посвящен основам перехвата (несанкционированное подключение

к проводной связи и Интернету), на второй день слушатели пройдут базовый курс по киберпреступности. Оба эти курса будут обязательными для всех прокуроров Нидерландов и станут частью их обязательного образования. Вторая часть курса предназначена исключительно для специалистов в области киберпреступности (будут введены строгие условия приема на эти курсы), включает курс углубленной подготовки (2–4 дня) и двухдневный мастер-класс (ежегодно). Эти курсы будут проводиться совместно с внешними партнерами, например *Fox-IT, Digital Intelligence Training* и *Hoffman Bedrijfsrecherche*.

Причиной разработки курса стало не разочарование в содержании проводимых программ подготовки, а стремление добиться того, чтобы части курса были более структурированы и лучше согласованы друг с другом, чтобы избежать дублирования в процессе преподавания.

Назначение прокуроров по вопросам киберпреступности в 11 самых крупных отделениях Прокурорской службы Нидерландов в рамках *Intensiveringsprogramma* также стало важным стимулом для разработки/пересмотра программ подготовки. Важным аспектом курса является принцип последовательного повышения уровня знаний; каждый участник должен сначала пройти два базовых курса, прежде чем его зачислят на курс углубленный подготовки и на прохождение мастер-классов.

Одной из возможных новых составляющих курса станет информационное графическое отображение работы и рисков, связанных с Интернетом. В настоящее время работа над графическим отображением находится на завершающих этапах и может также использоваться во время проведения пробных презентаций.

<...>

Последующие мероприятия

Для того чтобы прокуроры, которые занимаются киберпреступностью на повседневной основе, могли следить за последними достижениями в быстро развивающемся мире киберпреступности, в настоящее время проводятся две дополнительные программы по этой тематике.

Первая программа предусматривает создание Центра знаний и повышения квалификации при Национальной прокуратуре в Роттердаме. Этот центр будет отвечать на вопросы технического и юридического характера, следить за последними изменениями в прецедентном праве и распространять эту и другую необходимую информацию среди всех профессиональных сотрудников в области киберпреступности в полиции и в прокурорской службе (центр является совместным предприятием двух организаций).

Во-вторых, в качестве приложения к данному проекту идет создание «комнаты цифрового сотрудничества», которую можно сравнить с функционированием службы *Share Point*. В этой виртуальной комнате киберпрофессионалы смогут обсуждать вопросы, связанные с их работой, и заниматься поиском любой информации, необходимой для их деятельности.

<...>

Создание чувства неотложной необходимости: подготовка на управленческом уровне

Принимая во внимание относительно ограниченные возможности полиции Нидерландов, ей приходится делать выбор между тем, какие преступления следует или не следует расследовать (примечание: правовая система Нидерландов позволяет Прокурорской службе не расследовать и не вести судебного преследования в связи с преступлениями, что называется *opportuniteitsbeginsel*). Как правило, это выбор делается на уровне управленческих кадров.

По признанию полиции и Прокурорской службы на этом уровне отсутствуют знания, касающиеся последствий киберпреступлений и важности борьбы с киберпреступностью, что создает опасность того, что эти важные дела не будут рассмотрены, поскольку более важными будут признаны другие (обычные) преступления. В связи с этим, в настоящее время разрабатывается учебный курс для руководителей полиции и Прокурорской службы. <...>Этот учебный курс будет нацелен на создание чувства неотложной необходимости и в основном, будет направлен на ознакомление участников с реалиями киберпреступности в современном обществе. Он будет включать изучение тем не на уровне контента (как это происходит в процессе углубленного изучения предметов), а на стратегическом, управленческом уровне.

4.4. Организация по безопасности и сотрудничеству в Европе (ОБСЕ) *(Organization for Security and Co-operation in Europe, OSCE)*

СОВМЕСТНАЯ ДЕКЛАРАЦИЯ О СВОБОДЕ ВЫРАЖЕНИЯ МНЕНИЙ В ИНТЕРНЕТЕ

1 июня 2011 г.

Специальный докладчик Организации Объединенных Наций (ООН) по вопросу о поощрении и защите права на свободу мнений и их

свободное выражение, Представитель Организации по безопасности и сотрудничеству в Европе (ОБСЕ) по вопросам свободы средств массовой информации, Специальный докладчик по вопросам свободы выражения мнений Организации американских государств (ОАГ) и Специальный докладчик по вопросам свободы выражения мнений и свободного доступа к информации Африканской комиссии по правам человека и народов,

обсудив данные вопросы при содействии организации «*Артикль 19*», *Всемирной кампании за свободу выражения мнений* и *Центра за право и демократию*;

принимая во внимание и подтверждая наши совместные декларации от 26 ноября 1999 года, 30 ноября 2000 года, 20 ноября 2001 года, 10 декабря 2002 года, 18 декабря 2003 года, 6 декабря 2004 года, 21 декабря 2005 года, 19 декабря 2006 года, 12 декабря 2007 года, 10 декабря 2008 года, 15 мая 2009 года и 3 февраля 2010 года;

вновь подчеркивая фундаментальное значение свободы выражения мнений, – включая принципы независимости и многообразия, – как отдельного права, так и в виде важнейшего инструмента защиты всех других прав, а также основополагающего элемента демократии и средства достижения целей развития;

подчеркивая преобразующую роль Интернета в плане предоставления права голоса миллиардам людей повсюду в мире и существенного расширения их возможности получать информацию, а также укрепления плюрализма и обеспечения отчетности;

признавая огромные возможности Интернета в содействии осуществлению других прав и активизации общественности, а также в упрощении доступа к товарам и услугам;

приветствуя значительный рост доступа к Интернету почти во всех странах и регионах мира, отмечая при этом, что миллиарды людей по-прежнему лишены такого доступа или пользуются второсортными формами доступа;

отмечая, что некоторые правительства предприняли попытки ввести или приняли меры с конкретной целью значительно ограничить свободу выражения мнений в Интернете вопреки нормам международного права;

признавая, что осуществление права на свободу выражения мнений может быть подвергнуто определенным ограничениям, которые предусмотрены законодательством и необходимы, например, в целях предотвращения преступлений и защиты основополагающих прав других лиц, включая детей, но подчеркивая при этом, что любые подобные

ограничения должны быть сбалансированными и соответствовать нормам и принципам международного права в части права на свободу выражения мнений;

выражая обеспокоенность тем, что даже предпринимаемые с наилучшими намерениями многие усилия правительств в вышеупомянутых целях не учитывают особенности Интернета, что в результате приводит к чрезмерному ограничению свободы выражения мнений;

отмечая механизмы подхода, предусматривающего участие многих заинтересованных сторон, принятого в рамках Форума Организации Объединенных Наций по вопросам управления пользованием Интернетом;

будучи осведомленными о широком круге субъектов, действующих в качестве промежуточных звеньев в обеспечении работы Интернета: провайдеров таких услуг, как доступ и обеспечение межсистемной связи Интернета, передача, обработка и направление интернет-трафика, хостинг и доступ к публикуемым пользователями материалам, поиск и цитирование материалов в Интернете, финансовые операции и функционирование социальных сетей; а также о попытках некоторых государств переложить ответственность за вредоносный или противозаконный контент на этих субъектов;

принимают 1 июня 2011 года нижеследующую Декларацию о свободе выражения мнений и Интернете:

• **Общие принципы**

• Принципы свободы выражения мнений распространяются на Интернет так же, как и на все прочие средства коммуникации. Ограничения свободы выражения мнений в Интернете приемлемы только, если они соответствуют установленным международным нормам, в том числе предусмотрены законодательством и необходимы для защиты интересов, признанных в рамках международного права («тройной тест»).

• При определении пропорциональности ограничения свободы выражения мнений в Интернете результаты воздействия такого ограничения на способность Интернета обеспечивать позитивную свободу выражения мнений должны сопоставляться с его преимуществами в плане защиты других интересов.

• Подходы к регулированию, разработанные для других средств коммуникации, таких как телефония и теле- и радиовещание, не могут быть автоматически перенесены на Интернет; такие подходы должны быть специально для него разработаны.

• Необходимо уделять большее внимание выработке альтернативных, индивидуальных подходов, адаптированных к уникальным характеристикам Интернета, как ответных мер в связи с противоза-

конным контентом, признавая при этом, что никакие специальные ограничения не должны вводиться в отношении контента материалов, размещаемых в Интернете.

• Саморегулирование может служить эффективным инструментом реагирования на вредоносные высказывания и должно получать поддержку.

• Необходимо поддерживать деятельность по повышению осведомленности и просветительские кампании в целях содействия участию каждого человека в автономном, самостоятельном и ответственном пользовании Интернетом («интернет-грамотность»).

• **Ответственность субъектов, действующих в качестве промежуточных звеньев**

• Ни одно лицо, которое просто предоставляет технические интернет-услуги, такие как обеспечение доступа или поиск, передача или кэширование информации, не должно нести ответственность за созданный другими лицами контент, который был распространен при помощи этих услуг, если это лицо не вносило изменения в данный контент и не отказывалось выполнить судебное решение об удалении данного контента в случаях, когда оно имеет возможность это сделать («принцип простой передачи»).

• Необходимо рассмотреть возможность полной защиты прочих субъектов, выполняющих функции промежуточных звеньев, в том числе упомянутых в преамбуле, от ответственности за произведенный другими лицами контент на условиях, описанных в пункте 2 *a*). По меньшей мере, эти «промежуточные звенья» не обязаны осуществлять мониторинг произведенного пользователями контента, и по отношению к ним не должны применятся правила внесудебного удаления контента, которые не обеспечивают необходимую защиту свободы выражения мнений (как и многие применяющиеся в настоящее время правила предупреждения и удаления).

• **Фильтрация и блокирование**

• Принудительное блокирование целиком веб-сайтов, IP-адресов, портов, сетевых протоколов или отдельных разновидностей интернет-ресурсов (например, социальных сетей) представляет собой крайнюю меру, аналогичную запрещению газет или вещания, и может быть оправдано лишь при соответствии таких действий международным нормам, например в случаях, когда необходимо защитить детей от сексуального насилия.

• Вводимые государством или коммерческим поставщиком услуг системы фильтрации интернет-контента, которые не подконтрольны конеч-

ным пользователям, являются формой предварительной цензуры и не могут быть оправданы, будучи ограничением свободы выражения мнений.

• Продукция, позволяющая конечным пользователям фильтровать содержимое Интернета, должна сопровождаться доступной для конечных пользователей информацией о специфике работы таких фильтров и возможных трудностях, способных привести к чрезмерной фильтрации.

• **Уголовная и гражданская ответственность**

• В отношении судебных дел, касающихся интернет-контента, должна применяться юрисдикция того государства, к которому данные судебные дела имеют прямое и существенное отношение, потому что обычно именно в этом государстве, имеющем прямое отношение к делу, находится автор публикации и загружена сама публикация, которая непосредственно касается данного государства. Частные стороны могут только подавать судебные иски в определенной юрисдикции, в которой они могут заявить, что понесли существенный ущерб (правило, направленное против «клеветнического туризма»).

• В нормах ответственности, включая защиту в гражданских делах, должна учитываться заинтересованность общества в целом в защите как свободы выражения мнений, так и форума, где оно имеет место (то есть необходимо сохранить аспект «публичной площадки» в Интернете).

• Что касается публикаций в Интернете, которые появляются в одном и том же месте в неизменной по существу форме, то срок исковой давности для возбуждения соответствующих судебных дел должен начинаться от даты первоначальной публикации, и в отношении этой публикации может быть рассмотрено только одно исковое заявление, которое в необходимых случаях позволяло бы одновременно взыскивать компенсацию за убытки, понесенные во всех юрисдикциях (правило «одной публикации»).

• **Сетевой нейтралитет**

• При распределении трафика и данных в Интернете не должно быть какой-либо дискриминации на основании класса устройства, контента, авторства, происхождения и/или назначения публикаций, услуг или приложений.

• Поставщики интернет-услуг должны сохранять прозрачность в отношении используемых ими форм управления трафиком или информацией и сообщать о них в доступной форме всем заинтересованным сторонам.

• **Доступ к Интернету**

• Осуществление права на свободу выражения мнений обязывает государства содействовать обеспечению всеобщего доступа к Интернету.

Доступ к Интернету также необходим в целях обеспечения соблюдения других прав, таких как право на образование, здравоохранение и труд, свободу собрания и ассоциации, а также права на свободное участие в выборах.

• Ограничение доступа к Интернету или какой-либо его части для всего населения или для определенных его сегментов (отключение Интернета) не может быть оправдано ни при каких обстоятельствах, даже если это происходит в связи с необходимостью сохранения общественного порядка или в интересах национальной безопасности. То же относится к замедлению операций в Интернете в целом или в каких-либо его частях.

• Отказ физическим лицам в праве на доступ к Интернету в качестве наказания представляет собой крайнюю меру, которая может быть оправдана только в случае отсутствия более мягких форм наказания или в случае принятия судом соответствующего решения, с учетом воздействия этой меры на осуществление прав человека.

• Другие меры, ограничивающие доступ к Интернету, например введение обязательной регистрации или других требований к поставщикам услуг, не являются законными, за исключением тех случаев, когда эти меры соответствуют международному праву в части мер по ограничению свободы выражения мнений.

• Государства имеют позитивные обязательства содействовать обеспечению всеобщего доступа к Интернету. Как минимум они должны

• Создать законодательные механизмы, включающие схемы ценообразования, всеобщие требования к техническому обслуживанию и лицензионные соглашения, которые способствовали бы более широкому доступу к Интернету, распространяющемуся даже на бедные и отдаленные сельские районы.

• Оказывать прямую поддержку в целях содействия доступу к Интернету, включая создание центров ИКТ на базе местных сообществ и других пунктов коллективного доступа.

• Способствовать повышению осведомленности населения как о пользовании Интернетом, так и о выгодах, которые он способен обеспечить, в особенности среди бедных, детей, пожилых, а также населения отдаленных сельских районов.

• Принять специальные меры в целях обеспечения равного доступа к Интернету инвалидам и лицам, находящимся в неблагоприятных условиях.

• В целях осуществления вышеуказанных рекомендаций государства должны принять подробные и многолетние планы действий по содействию доступу к Интернету, включающие четкие и конкретные цели,

а также нормы в отношении прозрачности, отчетности перед общественностью, а также системы мониторинга.

Франк Ла Рю
Специальный докладчик
Организации Объединенных Наций (ООН)
по вопросу о поощрении и защите права
на свободу мнений и их свободное выражение

Дунья Миятович
Представитель Организации по безопасности
и сотрудничеству в Европе (ОБСЕ) по вопросам
свободы средств массовой информации

Каталина Ботеро Марино
Специальный докладчик по вопросам
свободы выражения мнений
Организации американских государств (ОАГ)

Фейт Панси Тлакула
Специальный докладчик по вопросам
свободы выражения мнений и свободного доступа
к информации Африканской комиссии
по правам человека и народов

4.5. Организация экономического сотрудничества и развития (ОЭСР)
(Organisation for Economic Co-operation and Development, OECD)

РЕКОМЕНДАЦИЯ СОВЕТА ОЭСР О ПРИНЦИПАХ ФОРМИРОВАНИЯ ИНТЕРНЕТ-ПОЛИТИКИ

13 декабря 2011 г.

Совет,

принимая во внимание статью 5 (*b*) Конвенции о создании Организации экономического сотрудничества и развития 14 декабря 1960 года;

принимая во внимание правило 18 (*b*) Правил процедур;

учитывая *Декларацию относительно будущего интернет-экономики («Сеульская декларация») от 18 июня 2008 г.*, которой признается, что интернет представляет собой открытую, децентрализованную платформу для общения, сотрудничества, инноваций, творчества, повышения производительности и экономического роста;

учитывая *Рекомендацию Совета управляющих, касающуюся Руководящих принципов защиты частной жизни и трансграничных потоков личных данных, Рекомендацию Совета, касающуюся Руководящих принципов безопасности информационных систем и сетей – На пути к культуре безопасности, Рекомендацию Совета о развитии широкополосных сетей, Рекомендацию Совета о защите критически важных информационных инфраструктур*;

признавая, что на заседании высокого уровня ОЭСР – *Интернет-экономика: Генерирование инноваций и роста*, – состоявшемся в июне 2011 года, представители стран – членов ОЭСР, Египта, Консультативного комитета ОЭСР по бизнесу и промышленности Консультативного комитета ОЭСР по технологиям интернета согласилась принять *Коммюнике о принципах формирования интернет-политики (Коммюнике)*;

признавая, что данное Коммюнике, основываясь на Сеульской декларации, подчеркивает, что сила и динамизм Интернета зависит от легкости доступа к интернету через высокоскоростные сети, открытости и доверия пользователей, что интернет позволяет людям отдавать свои голоса в пользу приверженности демократии и что формирование любой политики, связанной с этим процессом, должно способствовать открытости и основываться на уважении прав человека и верховенстве закона;

по предложению Комитета по информационной, компьютерной и коммуникационной политике:

I. **Рекомендует**, чтобы при формировании или пересмотре своей политики в сфере интернет-экономики члены ОЭСР в сотрудничестве со всеми заинтересованными сторонами принимали во внимание следующие принципы, согласованные на высоком уровне в том контексте, как они интерпретируются в *Коммюнике*:

1. Поддерживать и защищать глобальный свободный обмен информацией;

2. Поддерживать открытый, распределенный и взаимосвязанный характер интернета;

3. Способствовать инвестициям и конкуренции в сфере высокоскоростных сетей и услуг;

4. Поддерживать и способствовать трансграничному предоставлению услуг;

5. Поощрять сотрудничество всех заинтересованных сторон в процессе разработки политики;

6. Способствовать естественному формированию норм и правил поведения;

7. Совершенствовать возможности предоставления общедоступных, достоверных данных в процесс разработки политики;

8. Обеспечить транспарентность (прозрачность) процессов, достоверность процессов и отчетность;

9. Усилить согласованность и эффективность защиты частной жизни на глобальном уровне;

10. Максимально расширять полномочия частных лиц;

11. Содействовать творчеству и инновациям;

12. Ограничивать ответственность интернет-посредников;

13. Поощрять сотрудничество по обеспечению безопасности интернета;

14. Предоставить необходимый приоритет деятельности правоохранительных органов.

II. **Напоминает**, что *Коммюнике о принципах формирования интернет-политики*, которое прилагается в целях информации, дает возможность и способствует тому, чтобы государства-члены и заинтересованные стороны применяли их для эффективных и согласованных подходов в формировании своей политики как на национальном, так и на международном уровне;

III. **Призывает**

Членов ОЭСР к тому, чтобы:

• Довести данную Рекомендацию до сведения своих правительств, всех заинтересованных сторон, включая бизнес-сообщество, гражданское общество, техническое и интернет-сообщество, а также до сведения иных международных форумов; и

• Учитывать, координировать и сотрудничать на национальном и международном уровне в рамках мультистейхолдеского процесса, в целях эффективного применения данной Рекомендации;

• Тем, кто не является членом ОЭСР, придерживаться этой Рекомендации и сотрудничать со странами – членами ОЭСР в ее применении;

IV. Поручает Комитету по информационной, компьютерной и коммуникационной политике:

• содействовать распространению данной Рекомендации;

• оказывать содействие как странам – членам ОЭСР, так и нечленам ОЭСР в применении данной Рекомендации в рамках мультистейкхолдерского процесса.

Приложение

КОММЮНИКЕ О ПРИНЦИПАХ ФОРМИРОВАНИЯ ИНТЕРНЕТ-ПОЛИТИКИ

(принято на заседании высокого уровня ОЭСР по интернет-экономике: Генерирование инноваций и роста, состоявшемся 28–29 июня 2011 года)

Сеульская декларация относительно будущего интернет-экономики, принятая на совещании на уровне министров ОЭСР – *Будущее интернет-экономики* – в 2008 году, признала, что интернет представляет собой открытую, децентрализованную платформу для общения, сотрудничества, инноваций, творчества, повышения производительности и экономического роста. Опираясь на Сеульскую декларацию, на заседании высокого уровня ОЭСР – *Интернет-экономика: Генерирование инноваций и роста*, состоявшемся в июне 2011 года, было подчеркнуто, что сила и динамизм интернета зависит от легкости доступа к интернету через высокоскоростные сети, открытости и доверия пользователей. В контексте данного заседания высокого уровня мы, представители стран – членов ОЭСР, Египта, Консультативного комитета ОЭСР по бизнесу и промышленности и Консультативного комитета ОЭСР по технологиям интернета, согласились принять следующие основополагающие принципы формирования интернет-политики в качестве важного шага для того, чтобы интернет оставался открытым и динамичным.

Мы признаем, что интернет позволяет людям отдавать свои голоса в пользу приверженности демократии и что формирование любой политики, связанной с этим процессом, должно способствовать открытости и основываться уважении прав человека и верховенстве закона;

Мы признаем важный вклад заинтересованных сторон, в том числе бизнес-сообщества, гражданского общества, технического интернет-сообщества, академических институтов, в поступательное развитие интернета и совершенствование общества с использованием возможностей интернета.

Мы обращаем особое внимание на то, что расширение повсеместного доступа к использованию сетей широкополосного интернета, которые могут стать доступными в конкурентной среде и по доступным ценам, будет способствовать развитию инноваций и стимулировать рост интернет-экономики и экономики в целом.

Мы подчеркиваем, что в определенных случаях общественная поддержка и инвестиции могут быть необходимы для наибольшей

практической доступности таких сетей в наших странах, в частности для сельских местностей и отдаленных районов, и что вмешательство государства должно содействовать рыночной конкуренции и стимулировать инвестиции частных лиц.

Мы акцентируем важность создания спроса и значительную роль, которую правительства могут играть в этом отношении путем стимулирования использования сетей широкополосного доступа к интернету в таких областях, как наука, образование, здравоохранение, транспорт и интеллектуальные электрические сети, а также поощрение использования интернета для решения проблем старения населения.

Мы признаем, что новые и развивающиеся технологии и протоколы, дающие возможность расширения потенциала и инноваций, такие как *IPv*6, семантические веб-технологии и облачные вычисления (*cloud computing*), выступают в качестве общего двигателя экономического и социального развития. В контексте недавних природных катаклизмов мы признаем, что устойчивые сети способны играть ключевую роль в обеспечении обмена информацией и содействии быстрому распределению помощи.

Интернет вырос и чрезвычайно быстро распространяется по всему миру и продолжает приносить значительные выгоды экономике и обществу. Участие частных лиц в сфере инноваций и согласованное взаимодействие заинтересованных сторон в экономике интернета через развертывание высокоскоростных сетей широкополосного доступа к интернету также может помочь в расширении возможностей доступа к легальному контенту наряду с поддержкой свободного распространения информации и знаний, свободы выражения мнений, свободы ассоциаций и собраний, защиты индивидуальных свобод как важнейших компонентов демократического общества и культурного разнообразия.

Принципы формирования интернет-политики в настоящем Коммюнике разработаны с тем, чтобы помочь сохранить фундаментальную открытость интернета, чтобы одновременно отвечать определенным целям государственной политики, таким, как защита частной жизни, безопасности, детей в онлайн-среде, интеллектуальной собственности, а также укрепление доверия в интернете. Эффективная защита прав интеллектуальной собственности играет жизненно важную роль в стимулировании инновации и содействует развитию интернет-экономики. Принципы формирования интернет-политики необходимы для того, чтобы принимать во внимание уникальные социальные, технические и экономические аспекты интернет-среды. Очевидно, что открытый

и доступный характер интернета нуждается в поддержке для получения выгод от свободы выражения мнений и поддержке легитимного обмена информацией, знаниями и мнениями между пользователями, включая исследования и разработки, которые содействуют широкой инновационной деятельности в наших экономиках.

Признавая зависимость нашей экономики от интернета, глобальный характер интернета и различия в подходах, применяемых для стимулирования интернет-экономики, включая управленческие стратегии в сфере инноваций, в проведении собраний различных групп заинтересованных сторон для формирования согласованной интернет-политики, мы, правительства, заинтересованные стороны частного сектора, гражданского общества, договорились о следующих принципах формирования интернет-политики:

• **Поддерживать и защищать глобальный свободный обмен информацией:**

Интернет-экономика, как в равной степени и возможность людей обучаться, обмениваться информацией и знаниями, возможность высказать свое мнение, создание и формирование ассоциаций и объединений, зависит от глобального свободного обмена информацией. Для обеспечения свободного онлайнового обмена информацией важно работать вместе для того, чтобы достигнуть лучшей глобальной совместимости, несмотря на существующие различия в законодательных актах и нормативном регулировании. Обеспечение свободного обмена информацией является также существенным для правительств в направлении их деятельности, связанной с обеспечением лучшей защиты персональных данных, защиты детей в онлайновой среде, защиты прав потребителей, интеллектуальной собственности, и для решения вопросов кибербезопасности. В целях содействия свободному обмену информацией правительства должны также уважать фундаментальные права человека.

• **Поддерживать открытый, распределенный и взаимосвязанный характер интернета:**

В качестве децентрализованной сети сетей интернет достиг глобального взаимодействия без какого-либо международного режима регулирования. Создание такого формального регулирующего порядка несет в себе риск подрыва роста интернета. Открытость интернета для новых устройств, приложений и услуг играет важную роль в его успешном стимулировании инновационной деятельности, творчества и в экономическом росте. Такая открытость является следствием постоянно развивающегося взаимодействия и независимости различных технических

компонентов интернета, позволяя осуществлять сотрудничество и содействовать инновациям, при этом давая возможность техническим компонентам интернета функционировать независимо друг от друга. Такая независимость позволяет изменять политику и регулирование некоторых компонентов без необходимости внесения изменений в другие или влиять на инновации и сотрудничество. Открытость интернета также проистекает из принятых на глобальном уровне, консенсуально установленных технических стандартов, которые поддерживают мировые товарные рынки и коммуникации. Распределение ролей, открытость и компетентность глобальных многосторонних, мультистейкхолдерских инструментов, которые устанавливают стандарты для разного уровня компонентов интернета, должны быть признаны и их вклад должен быть использован для различных технических элементов государственной политики. Сохранение технологической нейтральности и надлежащего качества всех интернет-услуг также важно для того, чтобы обеспечить открытую и динамичную интернет-среду. Предоставление открытого доступа к услугам интернета является критически важным для интернет-экономики.

• **Содействовать инвестициям и конкуренции в сфере высокоскоростных сетей и услуг:**

Высокоскоростные сети и услуги имеют существенное значение для дальнейшего экономического роста, создания рабочих мест, повышения конкурентоспособности и для людей в целях улучшения условий их жизни. Общественно-государственная политика должна поощрять здоровую конкуренции в сфере предоставления услуг высокоскоростного широкополосного доступа к интернету, которые пользователи должны получать по доступным ценам, и стимулировать инвестиции для наибольшего географического охвата широкополосным доступом к интернету.

Общественно-государственная политика должна также содействовать оптимальному уровню инвестиций путем создания спроса на высокоскоростные широкополосные сети и услуги, в особенности в тех сферах, в которых правительства играют ключевую роль, таких, как образование, здравоохранение, распределении энергии и транспорт.

Общественно-государственная политика должна способствовать укреплению разнообразия контента, платформ, приложений, онлайн-сервисов и других средств коммуникаций пользователей, которые будут создавать спрос на сети и услуги, а равно дадут возможность пользователям в полной мере воспользоваться преимуществами таких сетей и услуг и получить доступ к разнообразному контенту на недискриминацион-

ных условиях, включая возможность выбора культурного и языкового контента.

• **Стимулировать и обеспечивать трансграничное предоставление услуг:**

Поставщики услуг должны иметь возможность предоставлять услуги через интернет в трансграничном масштабе и на технологически нейтральной основе таким образом, чтобы способствовать совместимости услуг и технологий в соответствующих случаях. Пользователи должны иметь возможность доступа и создания правомерного контента и запуска приложений по своему выбору. Для обеспечения минимизации затрат и рентабельности прочие барьеры в отношении местоположения, доступа и использования трансграничных объектов и функций должны быть сведены к минимуму, при условии, что соответствующая защита данных и меры безопасности осуществляются теми способами, которые отвечают требованиям, предусмотренным в Руководящих принципах ОЭСР, и отражают необходимый баланс между всеми фундаментальными правами, свободами и принципами.

• **Поощрять совместные действия заинтересованных сторон в процессах разработки политики:**

Комплексный характер интернета, его глобальный охват и постоянная эволюция требуют своевременной, универсальной и инновационностимулирующей политики. Из-за быстро меняющейся технологической, экономической и социальной среды, в рамках которой внезапно появляются новые политические вызовы, мультистекхолдерский процесс демонстрирует обеспечение гибкости и универсальности, которые требуются в условиях существующих глобальные вызовов в сфере интернет-политики. Этот мультистейкхолдерский процесс должен включать все заинтересованные стороны и осуществляться в условиях гласности. В частности, постоянная поддержка необходима для мультистейкхолдерской среды, которая является фундаментом процесса управления интернетом и администрирования важнейших ресурсов интернета (к примеру, таких, как ресурс присвоения имен и номеров), и эти различные заинтересованные стороны должны продолжать в полной мере играть свою роль в рамках этой мультистейкхолдерской модели. Правительства должны также работать в мультистейкхолдерской среде для достижения международных целей государственной политики, а также укрепления международного взаимодействия в управлении интернетом.

• **Способствовать естественному формированию норм и правил поведения:**

Правительства могут достичь определенных политических целей с помощью гибких адаптивных мер, поощряя, содействуя и поддержи-

вая развитие кодексов поведения, которые поддерживаются эффективным механизмом формирования и предоставления отчетности. Такие кодексы поведения могли бы разрабатываться участниками мультистейкхолерского процесса на добровольной основе и в случае необходимости могли бы применяться соответствующими органами государственной власти. Такие кодексы поведения следует поощрять и содействовать добровольным совместным усилиям частного сектора, направленным на уважение свободы выражения мнений, ассоциаций и собраний в режиме он-лайн и на борьбу с незаконной деятельностью, включая мошенничество, использование вредоносной, недобросовестной и вводящей в заблуждение практики, размещаемой в интернете. Такие совместные усилия должны быть сбалансированными и соответствовать действующей нормативно-правовой базе, и там, где такие совместные усилия не могут предприниматься, иные, альтернативные варианты политики, соотносимые с этими принципами, должны рассматриваться после консультаций с соответствующими заинтересованными сторонами.

• **Совершенствовать возможности предоставления общедоступных, достоверных данных в процесс формирования политики:**

Публично доступные данные могут повысить качество участия всех заинтересованных сторон в формировании интернет-политики, так же как и в принятии окончательных политических решений правительств. Сбор, проверка и распространение объективных данных для того, чтобы информировать о решениях в области интернет-политики, должны быть усилены и использоваться для того, чтобы расширить совместные исследовательские возможности правительств, компетентных органов и заинтересованных сторон. Международно-сопоставимые показатели помогут определить текущее экономическое развитие и оценки пропорциональности и эффективности любых политических решений, созданных в рамках мультистейкхолдеркого процесса. Сбор данных должен осуществляться таким образом, чтобы избежать административной нагрузки, и анализ данных должен быть осуществлен тщательно для принятия верных политических решений.

• **Обеспечить транспарентность (прозрачность) процессов, достоверность процессов и отчетность:**

В целях создания общественного доверия к интернет-среде следует поощрять способы формирования политики и независимой политики, обеспечивающие прозрачность процессов, достоверность процессов и отчетности. Транспарентность (прозрачность) гарантирует, что пользователи интернета имеют своевременную, доступную и полезную информацию, касающуюся их прав и интересов. Достоверность

процессов обеспечивает предсказуемые процедуры принятия решений, лежащие в основе определения понятий, установления и защиты прав человека. Отчетность достигается за счет проведения политики, которая в соответствующих случаях налагает ответственность на стороны за их действия в интернете.

• **Усилить согласованность и эффективность защиты частной жизни на глобальном уровне:**

Надежная защита частной жизни имеет ключевое значение для обеспечения того, чтобы интернет реализовал свой социальный и экономический потенциал. Существующие вызовы в отношении проблем частной жизни, вероятно, обострятся, поскольку и экономика и общество в большей степени связаны с расширением инновационного использования личной информации, которая намного легче собирается, хранится и анализируется. Поскольку физические лица все больше взаимодействуют между собой с помощью интернета в общественной и частной жизни, они должны иметь возможность лучше понимать то, как их личные данные могут быть использованы, иметь возможность осуществлять больший контроль над тем, как они используются, и не сомневаться в том, что с этими данными будут обращаться должным образом. Правила защиты частной жизни должны основываться на общепризнанных принципах, таких, как Руководство ОЭСР о защите частной жизни, и правительства должны работать для того, чтобы достичь глобального взаимодействия путем расширения взаимного признания правовых норм, которые обеспечивают достижение тех же целей. Осуществление трансграничного взаимодействия будет и дальше защищать неприкосновенность частной жизни и содействовать инновациям. Правила защиты частной жизни должны также учитывать фундаментальные права других лиц общества, включая право на свободу слова, свободу печати и открытого и гласного правления.

• **Максимально расширять полномочия частных лиц:**

Интернет открывает возможности для лиц осуществлять контроль над информацией, которую они получают, так же как и контроль персональных данных, которые сообщаются о них. Для максимизации таких возможностей правительства, частный сектор, техническое интернет-сообщество и гражданское общество должны работать вместе, с тем чтобы обеспечить возможности надлежащего и эффективного индивидуального контроля за получением и раскрытием персональных данных, и такая совместная работа должна включать инициативы по обучению пользователей и цифровую грамотность.

• **Содействовать творчеству и инновациям:**

Многочисленные факторы свидетельствуют о том экстраординарном источнике творчества и инноваций, которые основаны на интернете, включая защиту прав интеллектуальной собственности в отношении творческой деятельности, а низкие барьеры для входа в интернет обеспечивают возможности творчества и развития новых технологий, продуктов и услуг. Сеульская Декларация ОЭСР о будущем интернет-экономики высветила некоторые из таких факторов, включая открытую интернет-среду, которая способствует свободному потоку информации, исследованиям, инновациям, предпринимательству, широкому доступу к общественной информации и контенту, стимулированию фундаментальных и прикладных исследований в интернете, управлению знаниями и инновациями в сетях, организации коллективной работы с участием университетов, правительственных и общественных исследований. Низкие барьеры для входа, поддерживающие открытый характер платформ в интернет-среде, имели ключевое значение для онлайн-творчества и инноваций. Принципы, политика и практика должны продолжать поощрять и развивать интернет-среду, которая благоприятствует начинаниям творческих и инновационных технологий, бизнесу, другим усилиям, которые уважают признанные законные права без необходимости получения разрешения или обязанности взаимодействовать с традиционными провайдерами услуг связи. Защита интеллектуальной собственности является фундаментальным инструментом продвижения инноваций и творчества в интернете. Новые и взаимодополняющие подходы, сбалансированные для обеспечения эффективной защиты интеллектуальной собственности, должны также поощряться в случае необходимости, а также они должны обеспечивать защиту законной конкуренции и фундаментальных принципов, таких, как свобода слова, доступ к законному контенту и интернет-услугам и технологиям, достоверность процессов защиты частной жизни. Разумная интернет-политика должна включать нормы ответственности, которые позволят частному сектору на добровольной основе взаимодействовать в целях защиты интеллектуальной собственности. Адекватные меры включают в себя законные действия по устранению и пресечению нарушений и полноту соблюдения прав пользователей, прав заинтересованных сторон и достоверность процессов. В русле мультистейкхолдерского процесса, предусмотренного настоящим документом, все стороны должны играть свою определенную роль, в том числе физические лица, провайдеры, интернет-посредники и органы юстиции.

• **Ограничить ответственность интернет-посредников:**

Соответствующие ограничения ответственности интернет-посредников существуют и продолжают играть основополагающую роль, в частности в отношении контента третьих лиц. Интернет-посредники, как и другие заинтересованные стороны, могут и действительно играют важную роль в устранении и пресечении незаконной деятельности, мошенничества и вводящей в заблуждение и недобросовестной практики, осуществляемой через их сети системы, а также в продвижении экономического роста. Ограничения играют важную роль в содействии инновациям и свободному распространению информации, а также в создании стимулов для взаимодействия заинтересованных сторон. В этом контексте правительства могут принять решение созвать заинтересованные стороны в открытый, мультистейкхолдерский процесс для определения соответствующих обстоятельств, в которых интернет-посредники могли бы предпринять действия по обучению пользователей, оказанию помощи правообладателям в реализации их прав или пресечению нелегального контента, при этом свести к минимуму нагрузку на посредников и создать условия правовой определенности для них в отношении достоверности процессов и в целом для использования принципов, обозначенных в этом документе. В решении этих текущих задач социальные и экономические издержки и выгоды, включая влияние на доступ к интернету, использование, безопасность и развитие вариантов политики, следует оценивать как часть процесса их разработки, их совмещения со всеми фундаментальными правами и свободами, а также их соразмерности, принимая во внимание важность проблем, поставленных на карту.

• **Поощрять сотрудничество по обеспечению безопасности интернета:**

Политика в отношении решения проблем безопасности и снижения степени уязвимости имеет важное значение для сохранения жизнеспособности интернета. Следует поощрять признанные в международном масштабе и создаваемые с учетом потребностей рынка стандарты безопасности и лучшие практики, обеспечивающие онлайновую безопасность. При этом следует поощрять крупные достижения в научно-исследовательских и опытно-конструкторских работах (*R&D on novel security systems capable of dealing with the high complexity of ICT networks, R&D*) по новым системам безопасности, способным справиться с высокой сложностью сетей ИКТ, информационных систем и приложений. Политика, направленная на повышение безопасности в сети, не должна нарушать базовые условия, которые позволяют интернету функционировать в качестве глобальной открытой платформы

для инноваций, экономического роста и социального прогресса, и такая политика не должна использоваться в качестве предлога для протекционизма. Политика должна быть также нацелена на повышение индивидуальных и коллективных усилий для самозащиты и укрепления доверия и надежности. Согласованность и потенциальные последствия политики и иные экономические и социальные аспекты интернета следует тщательно оценить в рамках мультистейкхолдерского процесса, до того, как такая политика будет принята и применена.

• Предоставлять соответствующие приоритеты для действий правоохранительных органов:

Поощрение инвестиций и инноваций торговых площадок интернета требует четко определенных юридических прав, надежных и достоверных процессов для защиты этих прав, включая права пользователей, в соответствии с требованиями правительств исполнить право, подлежащее применению. Важно в этой связи, чтобы правительства, бизнес и гражданское общество работали вместе для укрепления уважения к закону и защиты фундаментальных прав. Должны существовать соответствующие государственные правоприменительные средства и осуществляться взаимодействие с бизнесом, с тем чтобы обеспечить осуществление деятельности, связанной с интернетом, в соответствии с законом. Действующее законодательство и регулятивные нормы могут пересматриваться для того, чтобы обеспечить эффективность их применения в соответствии с фундаментальными правами. Наконец, следует улучшить взаимодействие в сфере трансграничных расследований и правоприменительных действий.

4.6. Содружество Независимых Государств (СНГ)

МОДЕЛЬНЫЙ ЗАКОН ОБ ОСНОВАХ РЕГУЛИРОВАНИЯ ИНТЕРНЕТА

(Принят в Санкт-Петербурге 16 мая 2011 г. Постановлением 36-9 на 36-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ)

Глава I. Общие положения

• **Сфера регулирования отношений настоящим Законом**

• Настоящий Закон устанавливает принципы и определяет основные направления регулирования отношений, связанных с использова-

нием Интернета, устанавливает порядок государственной поддержки развития Интернета, определяет отношения между участниками процесса регулирования Интернета и их функции при осуществлении регулирования, устанавливает правила определения места и времени совершения юридически значимых действий при использовании Интернета.

• Действие настоящего Закона не распространяется на отношения, связанные с обеспечением свободы доступа к информации, информационной безопасности и охраны интеллектуальной собственности, если иное прямо не установлено в настоящем Законе.

• Основные понятия, используемые в настоящем Законе

Для целей настоящего Закона используются следующие основные понятия:

Интернет – глобальная информационно-телекоммуникационная сеть, связывающая информационные системы и сети электросвязи различных стран посредством глобального адресного пространства, основанная на использовании комплексов интернет-протоколов (*Internet Protocol, IP*) и протокола передачи данных (*Transmission Control Protocol, TCP*) и предоставляющая возможность реализации различных форм коммуникации, в том числе размещения информации для неограниченного круга лиц;

управление Интернетом – разработка и применение правительствами, государственными предприятиями и учреждениями, предприятиями частного сектора и организациями гражданского общества согласованных принципов, правовых норм, организационных правил и технических процедур принятия решений, регулирующих развитие Интернета и его использование;

оператор услуг Интернета – лицо, осуществляющее деятельность по обеспечению пользователей доступом в Интернет и (или) иными услугами, оказываемыми с использованием интернет-технологий;

уполномоченный орган (в области Интернета) – орган государственной власти, осуществляющий функции по выработке государственной политики и нормативно-правовому регулированию в сфере развития и использования Интернета;

национальный сегмент Интернета – включает в себя домены, признанные в установленном национальным законодательством порядке национальными доменами государства, интернет-ресурсы, расположенные в иных доменах или не относящиеся к каким-либо доменам, хостинг которым предоставляется на территории государства, а также

сети связи национальных операторов связи, предоставляющих услуги по доступу в Интернет;

доменное имя (домен) – символьное обозначение, зарегистрированное для сетевой адресации, в которой используется система доменных имен *DNS*;

национальный домен первого уровня – домен, имя которого представлено кодом страны, утвержденным Международной организацией по стандартизации (*ISO* 3166), или иной домен;

национальный домен второго уровня – субдомен домена первого уровня, имя которого включает в себя имя домена первого уровня и собственное имя;

национальный регистратор – организация, осуществляющая регистрацию электронных адресов национальных доменов и ведение справочника указанных адресов.

• Субъекты отношений, регулируемых настоящим Законом

Субъектами отношений, регулируемых настоящим Законом, являются:

– государство в лице его органов власти, уполномоченных на осуществление регулирования Интернета;

– пользователи Интернета – юридические и физические лица, которым предоставляются услуги Интернета;

– операторы услуг Интернета;

– саморегулируемые организации, участвующие в процессе регулирования Интернета.

• Соотношение настоящего Закона и международных договоров

Если международным договором, участником которого является государство, предусмотрены иные правила, чем установленные настоящим Законом, применяются положения международного договора.

Глава II. Принципы регулирования

• Основные принципы регулирования отношений, связанных с использованием Интернета

Регулирование отношений, связанных с использованием Интернета, осуществляется с соблюдением следующих основных принципов:

– обеспечение прав и свобод граждан, включая право на использование Интернета и доступ к размещенной в нем информации;

– учет особенностей построения и развития Интернета, включая установленные на международном уровне и действующие на момент

принятия настоящего Закона применимые организационные правила и технические процедуры;

– ограничение сферы регулирования Интернета только теми предметными областями, в отношении которых отсутствуют либо не могут быть применены в силу требований действующего законодательства нормы и правила, установленные на международном уровне либо принятые саморегулируемыми организациями пользователей и операторов услуг Интернета;

– нераспространение регулирования на отношения, связанные с развитием Интернета и не затрагивающие установленные законодательством права и интересы личности, общества и государства.

• **Подготовка нормативных правовых актов, направленных на регулирование правоотношений, связанных с использованием Интернета**

• Подготовка нормативных правовых актов, направленных на регулирование правоотношений, связанных с использованием Интернета, осуществляется при участии представителей саморегулируемых организаций пользователей и операторов услуг Интернета в качестве экспертов (специалистов).

• Нормативные правовые акты, затрагивающие нормы и правила, которые регулируют технологические и организационные аспекты развития Интернета на международном уровне, подлежат обязательному согласованию с международными организациями, принявшими указанные нормы и правила.

• **Государственное регулирование и поддержка развития Интернета**

• Государство поощряет и поддерживает развитие Интернета.

• Органы государственной власти, органы местного самоуправления принимают меры, обеспечивающие:

– равноправный, недискриминационный доступ пользователей к Интернету;

– недопущение необоснованных ограничений деятельности операторов услуг Интернета и осуществляемого посредством Интернета обмена информацией;

– содействие развитию рынка услуг, оказываемых с использованием интернет-технологий, недопущение монополизации и недобросовестной конкуренции.

• Государство в лице уполномоченного органа государственной власти и саморегулируемые организации пользователей и операторов услуг Интернета совместно участвуют в разработке проектов между-

народных норм, регулирующих технологические и организационные аспекты развития Интернета.

• Бюджетные ассигнования, связанные с государственной поддержкой развития Интернета, предусматриваются законодательством о бюджете на соответствующий период и направляются органам исполнительной власти и иным организациям, участвующим в развитии Интернета.

Глава III. Основные направления регулирования

• **Компетенция участников регулирования отношений, связанных с использованием Интернета**

• Участниками процесса регулирования Интернета являются государство, операторы услуг Интернета, саморегулируемые организации.

• Государство в лице уполномоченных органов в процессе регулирования Интернета осуществляет:

– разработку, координацию и реализацию государственной политики на национальном, региональном и международном уровнях;

– создание благоприятных условий для развития, распространения и широкого применения Интернета и интернет-технологий;

– разработку, согласование и принятие законов, иных нормативных правовых актов, регулирующих отношения, связанные с использованием Интернета;

– надзор за соблюдением законодательства, регулирующего отношения, связанные с использованием Интернета;

– содействие распространению передового опыта в области регулирования отношений, связанных с использованием Интернета;

– борьбу с правонарушениями, совершаемыми с использованием Интернета.

• Операторы услуг Интернета в процессе регулирования Интернета осуществляют:

– разработку предложений, принципов и инструментария для заинтересованных сторон по вопросам регулирования отношений, связанных с использованием Интернета;

– участие в разработке государственной политики, проектов нормативных правовых актов в сфере использования Интернета;

– участие в разработке стандартов, применяемых при развитии Интернета.

• Саморегулируемые организации в процессе регулирования Интернета осуществляют:

– общественный контроль за мерами, предлагаемыми и применяемыми государством;

– общественную экспертизу разрабатываемых и (или) принимаемых законов и иных нормативных правовых актов;

– участие в разработке стандартов, применяемых при развитии Интернета;

– участие в организации функционирования системы национальных доменных имен;

– контроль качества услуг, оказываемых операторами услуг Интернета;

– содействие решению задачи обеспечения равноправного доступа граждан к Интернету.

• **Международное сотрудничество в области регулирования Интернета**

• Международное сотрудничество в области регулирования Интернета осуществляется на основе соблюдения общепризнанных принципов и норм международного права, международных договоров, а также устоявшихся в международной практике обычаев и деловых обыкновений.

• Уполномоченный орган в пределах своих полномочий представляет и защищает интересы государства в области Интернета, взаимодействует с уполномоченными органами иностранных государств, межправительственными и международными неправительственными организациями, а также координирует вопросы международного сотрудничества в области Интернета, осуществляемого государством, его гражданами и организациями, обеспечивает выполнение обязательств государства, вытекающих из международных договоров в области Интернета.

• Национальный регистратор принимает такие правила регистрации доменных имен второго уровня в национальном сегменте Интернета, которые позволяли бы аннулировать регистрации доменных имен, нарушающих национальное законодательство или публичный порядок других государств либо используемых администратором домена для осуществления деятельности, запрещенной национальным законодательством.

• Иностранные организации или иностранные граждане, осуществляющие деятельность в области использования Интернета на территории государства, пользуются правовым режимом, установленным для собственных граждан, если иное не установлено национальным законодательством.

• Компетентные судебные и правоохранительные органы по вопросам оказания правовой помощи по преступлениям в сфере компьютерной информации взаимодействуют с компетентными органами иностранных государств в соответствии с международными договорами или на основе принципа взаимности путем направления и исполнения запросов.

Расходы, связанные с исполнением указанных запросов, возмещаются в порядке, предусмотренном соответствующими международными договорами.

• Взаимодействие и разрешение споров государств – участников СНГ по вопросам регулирования Интернета осуществляется через Координационный совет государств – участников СНГ по информатизации при Региональном содружестве в области связи, созданный решением Совета глав правительств СНГ.

• Регулирование и государственная поддержка развития и эксплуатации инфраструктуры Интернета

• Государство осуществляет стимулирование развития и использования инфраструктуры Интернета, в том числе путем применения налоговых льгот и преференций.

• При принятии решений о государственной поддержке инфраструктурных проектов развития Интернета приоритет должен отдаваться передовым технологическим решениям, обеспечивающим более широкое использование Интернета гражданами по доступным для них ценам.

• Государство создает условия для равного доступа к инфраструктуре Интернета для всех пользователей на недискриминационной основе.

• Государство осуществляет целевую деятельность по распространению использования интернет-технологий во взаимодействии между государством, предприятиями частного сектора и гражданами, путем оказания государственных услуг с использованием указанных технологий.

• Определение места и времени совершения юридически значимых действий

• Юридически значимые действия, осуществленные с использованием Интернета, признаются совершенными на территории государства, если действие, породившее юридические последствия, было совершено лицом во время его нахождения на территории этого государства.

• Временем совершения юридически значимых действий признается время совершения первого действия, породившего юридические последствия.

• **Коллизионные вопросы**

В случае если при разрешении споров, связанных с использованием Интернета, возникает коллизия иностранного и национального законодательства, то действует норма национального законодательства государства, на территории которого в соответствии со статьей 11 настоящего Закона считается совершенным юридически значимое действие.

• **Противодействие использованию Интернета в противоправных целях**

Государство принимает законодательные и иные меры в целях противодействия использованию Интернета в противоправных целях. В указанных целях государство устанавливает обязанность операторов услуг Интернета хранить информацию о пользователях и об оказанных им услугах не менее 12 месяцев и предоставлять данные сведения по запросу судебных и (или) правоохранительных органов.

МОДЕЛЬНЫЙ ИНФОРМАЦИОННЫЙ КОДЕКС ДЛЯ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

(Принят в Санкт-Петербурге 23 ноября 2012 г. Постановлением 38-6 на 38-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ)

Часть первая

Раздел I
Общие положения

Глава 1. Основы информационного законодательства

Статья 1. Сфера действия и основные цели информационного законодательства

1. Информационным законодательством регулируются информационные и информационно-инфраструктурные отношения.

Субъектами информационных и информационно-инфраструктурных отношений, которые регулируются информационным законодательс-

твом, являются физические лица, юридические лица, органы государственной власти, органы местного самоуправления и судебные органы.

2. Основными целями информационного законодательства являются:

создание правовых основ для построения информационного общества;

обеспечение и защита конституционных прав и свобод человека в информационной сфере, прав юридических лиц;

обеспечение информационной безопасности человека, общества и государства;

содействие развитию системы информационных ресурсов, созданию развитой информационной инфраструктуры, повышению эффективности предпринимательской деятельности в информационной сфере;

создание правовых условий для эффективной конкуренции на рынке информационных услуг и работ;

создание правовых условий для эффективного информационного обеспечения физических и юридических лиц, органов государственной власти и органов местного самоуправления;

обеспечение правовой поддержки и защиты национального производителя информационных продуктов и информационных технологий;

гармонизация с международным законодательством в информационной сфере.

Статья 2. Основные понятия, используемые в информационном законодательстве

В информационном законодательстве используются следующие основные понятия:

адресный спам – массовая рассылка или публикация однотипных сообщений без предварительного согласия получателя;

документ – сведения, представленные на любом материальном носителе в установленных законодательством форме и виде и с обязательными реквизитами, которые позволяют их идентифицировать;

защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, а также несанкционированных воздействий на нее;

иностранные информационные ресурсы – информационные ресурсы, которые находятся в ведении уполномоченных органов иностранных государств, доступные для субъектов информационных и информационно-инфраструктурных отношений;

информационно-инфраструктурные отношения – общественные отношения, возникающие в процессе создания, распространения,

использования, хранения и уничтожения (утилизации) информации, а также в процессе деятельности субъектов информационной инфраструктуры, предоставления информационных услуг и выполнения работ в информационной сфере, использования информационных технологий и ресурсов и обеспечения информационной безопасности;

информационные отношения – общественные отношения, возникающие в процессе создания, распространения, использования, хранения и уничтожения (утилизации) информации;

информационные ресурсы – совокупность информации, включая документы, независимо от содержания, времени и места создания;

информационные ресурсы органов власти – информационные ресурсы, находящиеся в ведении органов государственной власти и органов местного самоуправления, доступные для субъектов информационных и информационно-инфраструктурных отношений;

информационные услуги и работы – деятельность по обеспечению оборота информации, направленная на удовлетворение информационных потребностей субъектов информационных отношений, осуществляемая как на договорной, так и на недоговорной основе;

информационный продукт – любая обособленная информация, представленная в конкретно организованной форме и конкретном виде, независимо от содержания, времени и места создания, по поводу которой возникают или могут возникнуть правовые отношения;

информация – сведения или данные, порядок использования которых независимо от способа их представления, хранения или организации подлежит правовому регулированию в соответствии с настоящим Кодексом и национальным законодательством;

информация о деятельности органов государственной власти, органов местного самоуправления и судебных органов – информация, созданная или подготовленная в пределах своих полномочий органами государственной власти, органами местного самоуправления, организациями, подведомственными органам государственной власти и (или) органам местного самоуправления, судебным органам, и относящаяся к их деятельности;

массовая информация – предназначенная для неопределенного круга лиц печатная, электронная (цифровая, в том числе аудио- и аудиовизуальная) информация;

национальные информационные ресурсы – информационные ресурсы, находящиеся под юрисдикцией государства, доступные для субъектов информационных и информационно-инфраструктурных отношений;

обладатель информации – физическое или юридическое лицо, орган государственной власти, орган местного самоуправления или судебный

орган, которые своими силами создали информацию либо приобрели на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

поисковый спам – сайты и страницы в Интернете, созданные с целью манипуляции результатами поиска и выдающие лицу, осуществляющему поиск информации, некорректные, не соответствующие действительности результаты;

правовой режим информации – установленный в соответствии с законодательством порядок создания, распространения, использования, хранения и уничтожения (утилизации) информации, а также порядок отнесения информации к категории информации с ограниченным доступом;

правовой режим конфиденциальности информации – правовой режим доступа к конфиденциальной информации, а также регламентация ее использования, способов и средств обеспечения ее защиты;

правовой режим секретности информации – правовой режим доступа к секретной информации, а также регламентация ее использования, способов и средств обеспечения ее защиты;

распространение (передача) информации – деятельность, связанная с предоставлением информации неопределенному либо определенному кругу лиц;

секретная информация – информация, которая содержит сведения, составляющие государственную или другую предусмотренную законом тайну;

статистическая информация (данные) – любая информация, которая в количественном и качественном измерении характеризует массовые явления и процессы, имеющие место в экономической, социальной и других сферах общественной жизни;

статистические данные – информация, полученная в результате обработки первичных данных на основе статистической методологии и представленная в формализованном виде.

Статья 3. Основные принципы информационного законодательства

Информационное законодательство базируется на следующих основных принципах:

обеспечение свободы получения и распространения информации для всех субъектов информационных отношений и информационно-инфраструктурных отношений;

обеспечение доступности, достоверности, полноты и своевременности информации;

установление баланса прав и законных интересов человека, общества и государства в информационной деятельности;

ограничение доступа к информации исключительно на основании закона;

обеспечение минимизации негативного информационного воздействия и негативных последствий функционирования информационных технологий;

недопущение несанкционированного распространения, использования и уничтожения информации;

предоставление возможности получения государственных и (или) муниципальных услуг в электронном виде.

Статья 4. Нормативные правовые акты информационного законодательства

Информационное законодательство основывается на конституции и состоит из информационного кодекса и принятых в соответствии с ним законов.

Нормы информационного законодательства, содержащиеся в других законах, должны соответствовать информационному кодексу.

В соответствии с национальным законодательством уполномоченные органы вправе принимать подзаконные акты по вопросам, относящимся к сфере информационного законодательства.

Глава 2. Гарантии и защита прав и интересов в информационной сфере

Статья 5. Основные права и свободы в информационной сфере

Каждый имеет право свободно искать, получать, использовать, создавать, распространять и хранить информацию любыми законными способами и средствами.

Статья 6. Ограничение прав и свобод в информационной сфере

Осуществление прав и свобод в информационной сфере может быть ограничено только законом в интересах защиты основ конституционного строя, обеспечения национальной безопасности, защиты территориальной целостности и общественного порядка с целью предотвращения беспорядков, преступлений, разжигания социальной, расовой, межнациональной, межэтнической и религиозной вражды, для защиты здоровья и морали населения, репутации или прав других лиц, для недопущения несанкционированного доступа, распространения, использования и уничтожения информации

с ограниченным доступом или для поддержки авторитета и беспристрастия правосудия.

Не допускаются сбор, хранение, использование и распространение конфиденциальной информации, информации о частной жизни человека без его согласия, кроме случаев, установленных национальным законодательством.

Статья 7. Гарантии прав и интересов в информационной сфере

Обеспечение информационных прав и свобод человека в информационной сфере, обеспечение информационной безопасности является одной из важнейших функций государства.

Обеспечение права каждого человека на свободу поиска, получения, использования, создания, распространения и хранения информации любыми законными способами и средствами возлагается на уполномоченные в соответствии с национальным законодательством органы.

Статья 8. Защита прав и интересов в информационной сфере

Каждый имеет право на защиту своих прав и интересов в информационной сфере.

Органы государственной власти, органы местного самоуправления, судебные органы обязаны принимать все необходимые меры в целях обеспечения защиты прав и интересов в информационной сфере.

Каждый субъект информационных и информационно-инфраструктурных отношений, чьи права и интересы нарушены, индивидуально или совместно с другими, имеет право направить жалобу или другие соответствующие обращения в судебные органы, в органы государственной власти и органы местного самоуправления.

Решение по жалобе или другим соответствующим обращениям должно предусматривать мероприятия по исключению нарушения прав и интересов субъектов информационных и информационно-инфраструктурных отношений, в частности возможную компенсацию нанесенного ущерба, а также меры по выполнению этого решения.

Глава 3. Функции государства и его органов в информационной сфере

Статья 9. Участие органов государственной власти и органов местного самоуправления в информационных и информационно-инфраструктурных отношениях

Непосредственное участие органов государственной власти и органов местного самоуправления в информационных и информационно-инф-

раструктурных отношениях может осуществляться только на основании, в пределах полномочий и способом, которые определены конституцией, информационным кодексом и принятыми в соответствии с ним законами.

Статья 10. Основные направления участия органов государственной власти и органов местного самоуправления в информационных и информационно-инфраструктурных отношениях

Основными направлениями участия органов государственной власти и органов местного самоуправления в информационных и информационно-инфраструктурных отношениях являются:

обеспечение условий для эффективной реализации и защиты конституционных прав и свобод человека в информационной сфере;

создание политических, экономических, правовых и других основ построения информационного общества;

всемерное и всестороннее развитие национальной информационной инфраструктуры;

развитие системы информационных ресурсов, сохранения информационного продукта, в том числе культурных и духовных ценностей;

обеспечение экономических и правовых условий для всемерной поддержки и защиты национального производителя информационного продукта и информационных технологий;

обеспечение государственной поддержки развития общественно важных направлений в информационной сфере, в том числе: средств массовой информации, современных компьютерных информационных технологий, программных средств, а также содействие широкому внедрению и применению информационных технологий в государственном управлении, экономике, обороне, здравоохранении, образовании, экологии и других областях;

содействие добросовестной конкуренции, недопущение монополизации на рынке социально важных информационных услуг и работ;

создание условий для своевременного, качественного и эффективного информационного обеспечения физических и юридических лиц, органов государственной власти и органов местного самоуправления;

развитие системы непрерывного образования населения и специалистов в информационной сфере;

создание условий для развития системы электронного документооборота, применения электронного документа и электронной подписи;

формирование и осуществление единой научно-технической политики в сфере информатизации с учетом мирового уровня развития информационных технологий;

равноправная интеграция государства в глобальное информационное пространство, соблюдение международных договоров и соглашений в информационной сфере.

Раздел II
Основные положения

Глава 1. Основные положения об информационной инфраструктуре

Статья 11. Национальная информационная инфраструктура

Основным условием обеспечения информационных прав и свобод человека в информационной сфере является всемерное развитие национальной информационной инфраструктуры, состоящей из совокупности систем:

производства информации;

распространения информации;

производства средств производства информации и информационных технологий;

накопления и хранения информации;

предоставления информационных услуг;

сервисного обслуживания;

подготовки кадров;

обеспечения информационной безопасности;

иных систем.

Статья 12. Назначение информационной инфраструктуры

Информационная инфраструктура предназначена для обеспечения оборота информации путем предоставления информационных услуг и проведения работ.

Информационные услуги предоставляются и работы проводятся на конкурентных условиях.

Раздел III
Информационные отношения. Оборот информации

Глава 1. Общие положения

Статья 13. Оборот информации

Оборот информации происходит в процессе ее создания, распространения, использования, хранения и уничтожения (утилизации).

Информация может находиться в гражданском, административном или другом обороте.

Оборот информации, в котором принимают участие субъекты информационных и информационно-инфраструктурных отношений, регулируется информационным кодексом и принятыми в соответствии с ним законами.

Глава 2. Создание информации

Статья 14. Право на создание информации

Каждое физическое или юридическое лицо имеет право на создание любой информации любыми законными способами и средствами в любом виде и на любых материальных носителях в соответствии с национальным законодательством.

Статья 15. Массовая информация

Деятельность средств массовой информации регулируется национальным законодательством.

Статья 16. Статистическая информация

Статистическая информация подразделяется на государственную статистическую информацию, которая собирается и создается в интересах управления государством, и локальную статистическую информацию, которая собирается и создается в интересах отдельных субъектов в разных сферах общественной жизни.

Общественные отношения по сбору, созданию, распространению, использованию, хранению и уничтожению государственной статистической информации регулируются национальным законодательством.

Общественные отношения по сбору, созданию, распространению, использованию, хранению и уничтожению локальной статистической информации регулируются информационным кодексом и соответствующими договорами, заключенными между физическими и (или) юридическими лицами, которые проводят статистические исследования, и физическими и (или) юридическими лицами, которые их заказывают.

Статья 17. Создание статистической информации

Статистическая информация существует в виде первичных данных и статистических данных, а также аналитических материалов, которые готовятся на основании этих данных.

Первичные данные собираются в процессе проведения статистических наблюдений путем их регистрации в соответствии со специальной программой, разработанной на основе статистической методологии.

Статистическая методология, которая используется при статистических исследованиях и при обработке первичных данных, должна быть объявлена.

Органы государственной власти и органы местного самоуправления, предприятия, учреждения и организации, независимо от форм собственности, обязаны предоставлять первичные данные для создания государственной статистической информации в порядке, установленном национальным законодательством.

Первичные данные для создания локальной статистической информации предоставляются на добровольной основе.

Создание статистической информации, при которой происходит сбор персональных данных, проводится в соответствии с национальным законодательством о защите персональных данных.

Субъекты статистических наблюдений имеют право знать о целях исследований, правилах и условиях использования статистической информации.

Статья 18. Информация о деятельности органов государственной власти, органов местного самоуправления и судебных органов

Информация о деятельности органов государственной власти, органов местного самоуправления и судебных органов предоставляется любому лицу в соответствии с национальным законодательством.

Порядок предоставления информации о деятельности органов государственной власти, органов местного самоуправления и судебных органов в электронном виде определяется информационным кодексом или иным национальным законом.

Глава 3. Распространение информации

Статья 19. Право на распространение информации

Каждое физическое или юридическое лицо имеет право на свободное распространение любой информации любыми законными способами и средствами в любом виде и на любых материальных носителях.

При распространении информации должны быть обеспечены ее своевременная доставка потребителю и целостность, а также выполнение требований национального законодательства в сфере интеллектуальной собственности.

Статья 20. Распространение печатной и (или) электронной информации

Информация в целях распространения может представляться в печатном и (или) электронном виде.

Субъектами процесса распространения печатной и (или) электронной информации являются юридические и физические лица, в том числе издатели, производители и распространители.

Распространители печатной и (или) электронной продукции самостоятельно планируют и осуществляют свою деятельность, которую имеют право осуществлять только после государственной регистрации.

Распространители в соответствии с нормами, установленными национальным законодательством, или договорными обязательствами обязаны своевременно распространять печатную и (или) электронную продукцию.

Особенности распространения печатной и (или) электронной информации регулируются национальным законом.

Статья 21. Распространение аудиовизуальной информации

Субъектами процесса распространения аудиовизуальной информации являются операторы и провайдеры телекоммуникаций, а также субъекты, осуществляющие прокат и распространение аудиовизуальной информации.

Общественные отношения, связанные с распространением аудиовизуальной информации, регулируются национальным законом.

Статья 22. Распространение недостоверной информации

В случае распространения недостоверных сведений о любом лице оно имеет право на опровержение такой информации, а также на ее извлечение из информационного продукта.

Опровержение недостоверной информации осуществляется тем же способом, которым она была распространена. Ответственность за опубликование опровержения недостоверной информации несут ее распространители.

Порядок опубликования опровержения и извлечения недостоверной информации определяется национальным законодательством.

Статья 23. Запрещение на распространение информации

Запрещается несанкционированное распространение информации с ограниченным доступом.

Запрещается распространение информации, которая содержит пропаганду нарушения территориальной целостности и суверенитета государства, войны, социального, расового, национального, этнического, религиозного превосходства, жестокости и насилия, порнографию.

Глава 4. Использование информации

Статья 24. Использование информации

Все физические и юридические лица, органы государственной власти, органы местного самоуправления, судебные органы имеют право на использование информации, полученной или созданной ими законным способом.

Глава 5. Хранение информации

Статья 25. Право на хранение информации

Все физические и юридические лица, органы государственной власти, органы местного самоуправления, судебные органы имеют право на хранение информации, полученной или созданной ими законным способом.

Информация о физическом лице сохраняется в соответствии с национальным законодательством о защите персональных данных.

Информация, имеющая важное значение для человека, общества и государства ввиду своей исторической, культурной, научной, образовательной, информационной ценности, подлежит сохранению в соответствии с национальным законодательством.

Хранение информации, имеющей важное значение для человека, общества и государства, осуществляется в назначенной для этого системе учреждений (библиотеки, архивы, музеи и т.п.), а также в отдельных библиотечных, архивных и музейных фондах и собраниях разной формы собственности.

Всем физическим и юридическим лицам, органам государственной власти, органам местного самоуправления гарантируется свободный доступ в фонды библиотек, архивов, музеев государственной формы собственности с соблюдением требований национального законодательства о защите информации с ограниченным доступом.

Организация хранения информации в библиотеках, архивах, музеях, порядок формирования и использования их фондов определяются национальным законодательством.

Статья 26. Хранение аудиовизуальной и (или) электронной массовой информации

Редакции аудиовизуальных и (или) электронных средств массовой информации обязаны на протяжении года хранить копии всей массовой информации, которая ими распространялась.

Копии массовой информации сохраняются на носителях, которые обеспечивают ее воссоздание в том виде, в котором она распространялась.

Статья 27. Хранение контрольных экземпляров печатных и электронных изданий

Контрольные экземпляры всех печатных и электронных изданий в обязательном порядке подлежат сохранению в соответствии с национальным законодательством.

Ответственность за предоставление контрольных экземпляров печатных и электронных изданий для их последующего хранения несут редакции средств массовой информации и издатели.

Учреждения и организации, предназначенные для хранения контрольных экземпляров всех печатных и электронных изданий, определяются законодательством.

Глава 6. Уничтожение (утилизация) информации

Статья 28. Уничтожение (утилизация) информации

Информация, имеющая важное значение для человека, общества и государства ввиду своей исторической, культурной, научной, образовательной, информационной ценности, может быть уничтожена только в соответствии с порядком, устанавливаемым национальным законодательством.

Персональные данные, собранные не в соответствии с требованиями законодательства, должны быть уничтожены в установленном законодательством порядке.

Персональные данные, собранные правоохранительными органами в соответствии с требованиями законодательства, но не содержащие информации об осуществлении запрещенных законом действий, должны быть уничтожены в установленном законодательством порядке.

Раздел IV
Правовой режим информации

Глава 1. Общие положения

Статья 29. Правовой режим информации

По правовому режиму информация делится на открытую информацию и информацию с ограниченным доступом.

Виды информации и порядок определения конкретного перечня сведений, которые могут быть отнесены к информации с ограниченным доступом, определяются национальным законодательством.

Виды информации и порядок определения конкретного перечня сведений, которые обязательно должны быть публично объявлены, определяются национальным законодательством.

Ограничения в использовании информации устанавливаются национальным законодательством.

Контроль за обеспечением установленного правового режима информации осуществляется органами государственной власти, органами местного самоуправления, общественными организациями, юридическими лицами в пределах полномочий, установленных национальным законодательством.

Органы государственной власти в пределах полномочий, установленных национальным законодательством, обеспечивают защиту нарушенных прав и интересов субъектов информационных отношений в части обеспечения правового режима информации.

Глава 2. Открытая информация

Статья 30. Доступ к открытой информации

Никто не может быть ограничен в доступе, использовании, распространении и хранении открытой информации, за исключением случаев, которые определяются национальным законодательством.

Доступ к открытой информации, которая хранится в фондах библиотек, архивов, музеев государственной формы собственности, с целью обеспечения ее сохранения может осуществляться по регистрационному (заявочному) принципу.

Статья 31. Обязательность публикации информации

Обязательной публикации подлежат все нормативные правовые акты, если иное не предусмотрено национальным законодательством.

Статья 32. Право на получение информации, подлежащей обязательной публикации

Каждый имеет право обратиться в любой орган государственной власти или местного самоуправления с запросом о предоставлении сведений, перечень которых установлен национальным законодательством.

Орган государственной власти или орган местного самоуправления обязан в установленный национальным законодательством срок предоставить заявителю запрашиваемую информацию.

В случае если орган государственной власти или орган местного самоуправления не имеет в своем распоряжении запрашиваемой информации, он в установленный национальным законодательством

срок передает запрос тому органу государственной власти или местного самоуправления, который владеет данной информацией, сообщая об этом заявителю.

Статья 33. Ограничение на обязательность публикации

Обязательность публикации информации не распространяется на случаи, когда такая публикация может негативно повлиять на:

конфиденциальность деятельности органов государственной власти или органов местного самоуправления, если такая конфиденциальность предусмотрена национальным законодательством;

международные отношения, национальную безопасность;

осуществление правосудия, прав человека на справедливое судебное разбирательство или возможность государственных органов проводить расследование криминального или административного характера;

конфиденциальность коммерческой информации, если такая конфиденциальность охраняется национальным законодательством с целью защиты законных экономических интересов, за исключением информации о вредных для окружающей среды выбросах;

конфиденциальность персональных данных и (или) архивов, которые касаются человека, если он не дал согласия на публикацию такой информации в соответствии с требованиями национального законодательства.

Глава 3. Информация с ограниченным доступом

Статья 34. Распространение и (или) использование информации с ограниченным доступом

Информация с ограниченным доступом по правовому режиму делится на конфиденциальную и секретную.

Информация с ограниченным доступом по решению суда может быть распространена и (или) использована без согласия ее владельца, если эта информация является общественно значимой и право общественности на получение этой информации преобладает над правом ее владельца на ее защиту.

Статья 35. Конфиденциальная информация

Обладатели информации имеют право самостоятельно устанавливать правовой режим конфиденциальности, если это не противоречит требованиям национального законодательства.

Юридические лица в соответствии с требованиями национального законодательства обеспечивают осуществление правового режима

конфиденциальности информации, в том числе при проведении работ или предоставлении услуг за средства государственного бюджета.

Юридические лица в соответствии с договорными обязательствами обеспечивают осуществление правового режима конфиденциальности информации относительно информации, полученной от физических или юридических лиц и определенной ими как конфиденциальная информация.

Перечень видов сведений, которые могут быть отнесены органами государственной власти и органами местного самоуправления к конфиденциальной информации, устанавливается национальным законодательством.

Органы государственной власти и органы местного самоуправления обеспечивают правовой режим конфиденциальности информации в соответствии с порядком, установленным национальным законодательством.

Перечень сведений, которые не могут быть отнесены органами государственной власти и органами местного самоуправления, физическими и юридическими лицами к конфиденциальной информации, устанавливается национальным законодательством.

Статья 36. Секретная информация

Правовой режим секретности информации определяется национальным законодательством.

Перечень видов сведений, которые не могут быть отнесены к секретной информации, устанавливается национальным законодательством.

Часть вторая

Раздел V
требования к обороту информации

Глава 1. Общие положения

Статья 37. Общие требования к обороту информации

Оборот информации производится в соответствии с информационным кодексом и принятыми в соответствии с ним законами.

Субъекты информационных и информационно-инфраструктурных отношений обязаны соблюдать требования к обороту информации в случаях, установленных информационным кодексом и принятыми в соответствии с ним законами.

Оборот информации с ограниченным доступом, информации, причиняющей вред здоровью и (или) развитию, ограничивается в соответствии с информационным кодексом и принятыми в соответствии с ним законами.

Статья 38. Сотрудничество органов государственной власти и (или) органов местного самоуправления с общественными объединениями в целях противодействия обороту в Интернете информации, не соответствующей требованиям национального законодательства (противоправной информации)

Органы государственной власти и (или) органы местного самоуправления вправе в соответствии с национальным законодательством сотрудничать с общественными объединениями, деятельность которых направлена на обнаружение в Интернете информации, не соответствующей требованиям национального законодательства (противоправной информации).

Указанное сотрудничество осуществляется в соответствии с соглашениями, заключаемыми органами государственной власти и (или) органами местного самоуправления с данными общественными объединениями.

В соответствии с указанными соглашениями общественные объединения, обнаружив противоправную информацию, направляют сведения об адресе сайта в Интернете, на котором данная информация размещена, в орган государственной власти и (или) орган местного самоуправления для принятия мер реагирования согласно их компетенции.

Глава 2. Защита информации

Статья 39. Защита информации

Субъекты информационных и информационно-инфраструктурных отношений в случаях, установленных национальным законодательством, обязаны обеспечить:

предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к ней;

своевременное обнаружение фактов несанкционированного доступа к информации;

предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянный контроль за обеспечением уровня защищенности информации.

Глава 3. Требования к обороту информации в целях противодействия распространению спама

Статья 40. Запрет на распространение адресного и (или) поискового спама

Запрещается распространение адресного и (или) поискового спама.

Статья 41. Требования к электронным сообщениям в целях противодействия распространению адресного спама

Любое электронное сообщение должно содержать информацию о лице, которое является отправителем данного сообщения.

В электронном сообщении должны содержаться сведения о том, каким образом его получатель может связаться с отправителем данного сообщения.

Заголовок электронного сообщения должен соответствовать содержанию текста сообщения.

Электронное сообщение должно содержать уведомление о способе, в соответствии с которым получатель сообщения может отказаться от получения последующих сообщений от лица, являющегося отправителем первоначального сообщения, вне зависимости от их содержания.

Статья 42. Требования к рекламе в целях противодействия распространению адресного и (или) поискового спама

Реклама, распространяемая посредством электронных сообщений, должна содержать:

адрес электронной почты рекламодателя и рекламораспространителя;

слово «реклама» в заголовке электронного сообщения;

указание на доказательства наличия предварительного согласия адресата на получение рекламы;

уведомление о способе отказа от получения рекламы в будущем.

Реклама товаров и услуг посредством адресного и (или) поискового спама, а также содействие в организации подобного рода деятельности не допускаются.

Статья 43. Обязанности операторов связи по предупреждению и противодействию распространению адресного и (или) поискового спама

Операторы связи, осуществляющие прием, обработку, хранение, передачу или доставку электронных сообщений, обязаны в случае получения обращения от любого лица, указывающего на распространение адресного и (или) поискового спама, проверив данную информацию, при выявлении признаков правонарушения направить сообщение в уполномоченный в соответствии с национальным законодательством орган.

Статья 44. Запрет на составление списков адресов электронной почты

Не допускается составление списков адресов электронной почты, относящихся к конкретным лицам, их последующее распространение, а также использование таких адресов в целях распространения адресного и (или) поискового спама.

Глава 4. Противодействие обороту информации, причиняющей вред здоровью и (или) развитию

Статья 45. Информация, причиняющая вред здоровью и (или) развитию

Информацией, причиняющей вред здоровью и (или) развитию, являются любые сведения, распространение которых запрещено либо ограничено среди лиц определенных возрастных или иных категорий в соответствии с национальным законодательством.

Статья 46. Классификация информации

Производители и (или) распространители информации обязаны классифицировать ее по возрастным или иным категориям в соответствии с критериями, установленными национальным законодательством, в целях последующего размещения знака информационной продукции в соответствии со статьей 49 настоящего Кодекса.

В целях соответствия произведенной производителями и (или) распространяемой распространителями информации указанным критериям данные лица, а также любое лицо вправе обратиться для проведения экспертизы в уполномоченный в соответствии с национальным законодательством орган.

Срок, порядок проведения экспертизы, а также порядок возмещения расходов, связанных с проведением экспертизы, устанавливаются национальным законодательством.

Статья 47. Последствия экспертизы информации

Уполномоченный в соответствии с национальным законодательством орган после получения экспертного заключения принимает решение о соответствии либо несоответствии информации установленным требованиям.

Статья 48. Требования к обороту информации, причиняющей вред здоровью и (или) развитию

Оборот информации, содержащей сведения, причиняющие вред здоровью и (или) развитию, не допускается, за исключением случаев, установленных национальным законодательством.

Оборот информации, распространение которой ограничено, допускается при обозначении знаком информационной продукции в соответствии с классификацией данной информации.

Статья 49. Размещение знака при обороте информации, распространение которой ограничено

Производитель, распространитель информации размещают знак информационной продукции при обороте информации, распространение которой ограничено в порядке и в соответствии с условиями, установленными национальным законодательством.

Раздел VI
Предоставление государственных и (или) муниципальных услуг в электронном виде

Глава 1. Общие положения

Статья 50. Общие требования к предоставлению государственных и (или) муниципальных услуг, в том числе информационных, в электронном виде

Государственные и (или) муниципальные услуги, в том числе информационные, предоставляются в электронном виде любому обратившемуся лицу в случае, если возможность предоставления конкретной услуги не запрещена национальным законодательством.

Указанные услуги оказываются через специальный сайт в Интернете.

В соответствии с национальным законодательством должен быть определен перечень государственных и муниципальных услуг, в том числе информационных, открытый для всеобщего доступа.

В соответствии с национальным законодательством должен быть определен перечень государственных и муниципальных услуг, предоставление которых осуществляется без взимания платы.

Глава 2. Требования к специальному сайту в интернете для предоставления государственных и (или) муниципальных услуг

Статья 51. Специальный сайт в Интернете для предоставления государственных и (или) муниципальных услуг

Специальный сайт в Интернете создается в соответствии с национальным законодательством по решению уполномоченного органа.

Специальный сайт в Интернете должен обеспечивать:

предоставление государственных и (или) муниципальных услуг, а также содержать перечень указанных услуг;

возможность заполнения в электронной форме документов, необходимых для получения государственной и (или) муниципальной услуги;

возможность подачи в электронной форме документов для получения государственной и (или) муниципальной услуги;

возможность получения в электронной форме информации о ходе исполнения государственной и (или) муниципальной услуги;

возможность получения результата государственной и муниципальной услуги в электронной форме, если такая возможность не противоречит сути данной услуги;

возможность внесения платы за предоставление государственной и (или) муниципальной услуги в электронной форме.

Статья 52. Требование к обеспечению безопасности

При предоставлении государственной и (или) муниципальной услуги в электронной форме лицо, уполномоченное в соответствии с национальным законодательством, обязано обеспечить неразглашение персональных данных физических лиц, обратившихся за соответствующей услугой.

Глава 3. Предоставление информации о деятельности органов государственной власти и (или) органов местного самоуправления в электронном виде

Статья 53. Требование к предоставлению информации о деятельности органов государственной власти и (или) органов местного самоуправления в электронном виде

Органы государственной власти и (или) органы местного самоуправления обязаны предоставить информацию в электронном виде о своей деятельности любому лицу в случае, если указанная информация по своему правовому режиму не отнесена к информации с ограниченным доступом.

Статья 54. Форма предоставления информации о деятельности органов государственной власти и (или) органов местного самоуправления

Информация в электронном виде о деятельности органов государственной власти и (или) органов местного самоуправления предоставляется в следующих двух формах:

размещение информации о деятельности органов государственной власти и (или) органов местного самоуправления в Интернете;

предоставление информации о деятельности органов государственной власти и (или) органов местного самоуправления в электронном виде обратившемуся лицу.

Статья 55. Порядок размещения информации о деятельности органов государственной власти и (или) органов местного самоуправления в Интернете

Органы государственной власти и (или) органы местного самоуправления для размещения информации о своей деятельности обязаны создавать в Интернете свои официальные сайты, на которых размещают данную информацию.

Органы государственной власти и (или) органы местного самоуправления в соответствии с национальным законодательством назначают должностных лиц, которые обязаны следить за достоверностью и актуальностью информации, размещаемой на указанных сайтах.

Статья 56. Содержание информации о деятельности органов государственной власти и (или) органов местного самоуправления, размещаемой в Интернете

Информация о деятельности органов государственной власти и (или) органов местного самоуправления, размещаемая в Интернете, должна содержать следующие сведения:

общие сведения об органе государственной власти и (или) органе местного самоуправления, перечень которых устанавливается национальным законодательством;

сведения о нормативных правовых актах, регламентирующих деятельность органа государственной власти и (или) органа местного самоуправления, а также принятых органом государственной власти и (или) органом местного самоуправления;

перечень государственных и (или) муниципальных услуг, предоставляемых органом государственной власти и (или) органом местного самоуправления;

статистическую информацию о деятельности органа государственной власти и (или) органа местного самоуправления;

информацию о работе органа государственной власти и (или) органа местного самоуправления с обращениями физических и юридических лиц;

график приема должностными лицами органа государственной власти и (или) органа местного самоуправления.

Статья 57. Предоставление информации о деятельности органов государственной власти и (или) органов местного самоуправления в электронном виде

Информация о деятельности органов государственной власти и (или) органов местного самоуправления предоставляется по запросу любого лица, направленному либо по адресу электронной почты соответствующего органа, указанному на его официальном сайте, либо посредством специального сайта, предназначенного для предоставления государственных и (или) муниципальных услуг.

В случае если информация о деятельности органа государственной власти и (или) органа местного самоуправления уже размещена в Интернете, в ответе на запрос может быть указана только ссылка на соответствующий сайт в Интернете.

Глава 4. Предоставление информации о деятельности судебных органов в электронном виде

Статья 58. Требование к предоставлению информации о деятельности судебных органов в электронном виде

Информация о деятельности судебных органов в электронном виде предоставляется в соответствии с главой 3 настоящего раздела с учетом особенностей, предусмотренных настоящей главой.

Статья 59. Содержание информации о деятельности судебных органов, размещаемой в Интернете

Информация о деятельности судебных органов, размещаемая в Интернете, должна содержать следующие сведения:

общие сведения о судебном органе, перечень которых устанавливается национальным законодательством;

информацию о порядке судопроизводства и рассмотрения дел в суде;

тексты судебных актов (постановлений);

данные судебной статистики;
информацию о работе судебного органа;
график приема должностными лицами судебного органа.

Статья 60. Особенности размещения судебных актов (постановлений) в Интернете

При размещении в Интернете текстов судебных актов (постановлений) из указанных актов (постановлений) исключаются персональные данные, кроме фамилий и инициалов судей (судьи) и прокурора.

Вместо исключенных персональных данных используются обозначения, не позволяющие идентифицировать участников процесса.

В Интернете не подлежат размещению судебные акты (постановления) по делам, связанным с государственной или иной охраняемой законом тайной, безопасностью государства, по делам об усыновлении (удочерении) ребенка, другим делам, затрагивающим права и законные интересы несовершеннолетних, по делам о преступлениях против половой неприкосновенности и половой свободы личности.

Раздел VII
Платежи в электронной форме

Глава 1. Общие положения

Статья 61. Основы осуществления платежей в электронной форме

Физические и юридические лица (плательщики и получатели) вправе осуществлять платежи и расчеты в электронной форме без открытия банковских счетов в кредитных организациях.

Денежные средства для осуществления платежей и расчетов в электронной форме предварительно должны быть предоставлены плательщиком оператору, осуществляющему их перевод получателю.

Оператор вправе привлекать агента для приема денежных средств от физических и юридических лиц либо для передачи операторам распоряжений физических и юридических лиц по осуществлению платежей и расчетов.

Глава 2. Осуществление платежей в электронной форме

Статья 62. Условия деятельности оператора

Оператор, которым является кредитная организация, имеющая право на осуществление деятельности в соответствии с национальным

законодательством, несет ответственность за сохранность денежных средств при осуществлении платежей в электронной форме.

Оператор и агент в порядке, установленном национальным законодательством, вправе взимать плату за осуществление платежей в электронной форме.

Статья 63. Порядок осуществления платежей в электронной форме

Платеж в электронной форме осуществляется на основании распоряжения плательщика в пользу получателя посредством специальных разделов на сайтах в Интернете операторов либо привлеченных ими агентов.

Платеж в электронной форме может осуществляться между плательщиком и получателем, являющимися клиентами одного оператора или различных операторов.

Статья 64. Виды платежей в электронной форме

Электронные платежи могут осуществляться физическими лицами в следующих видах:

без проведения идентификации физического лица;

с проведением идентификации физического лица.

В случае если платеж в электронной форме осуществляется без проведения идентификации физического лица, национальным законодательством может быть установлен предельный размер платежа, осуществляемого в электронной форме.

Статья 65. Обеспечение банковской тайны и защиты персональных данных оператором и агентом

Оператор и агент обязаны гарантировать банковскую тайну, а также защиту персональных данных в порядке, установленном национальным законодательством.

Раздел VIII
Ответственность за нарушение положений информационного кодекса

Статья 66. Ответственность за нарушение положений информационного кодекса

Нарушение положений информационного кодекса влечет за собой дисциплинарную, гражданско-правовую, административную, уголовную ответственность в соответствии с национальным законодательством.

4.7. Шанхайская организация сотрудничества (ШОС)

СОГЛАШЕНИЕ МЕЖДУ ПРАВИТЕЛЬСТВАМИ ГОСУДАРСТВ – ЧЛЕНОВ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА О СОТРУДНИЧЕСТВЕ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(Екатеринбург, 16 июня 2009 г.)

Правительства государств – членов Шанхайской организации сотрудничества, далее именуемые «Стороны»,

отмечая значительный прогресс в развитии и внедрении новейших информационно-коммуникационных технологий и средств, формирующих глобальное информационное пространство,

выражая озабоченность угрозами, связанными с возможностями использования таких технологий и средств в целях, не совместимых с задачами обеспечения международной безопасности и стабильности, как в гражданской, так и в военной сферах,

придавая важное значение международной информационной безопасности как одному из ключевых элементов системы международной безопасности,

будучи убежденными в том, что дальнейшее углубление доверия и развитие взаимодействия Сторон в вопросах обеспечения международной информационной безопасности являются настоятельной необходимостью и отвечают их интересам,

принимая во внимание важную роль информационной безопасности в обеспечении прав и основных свобод человека и гражданина,

учитывая Резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»,

стремясь ограничить угрозы международной информационной безопасности, обеспечить интересы информационной безопасности Сторон и создать международную информационную среду, для которой характерны мир, сотрудничество и гармония,

желая создать правовые и организационные основы сотрудничества Сторон в области обеспечения международной информационной безопасности,

согласились о нижеследующем:

Статья 1. Основные понятия

Для целей взаимодействия Сторон в ходе выполнения настоящего Соглашения используются основные понятия, перечень которых приведен в Приложении 1 («Перечень основных понятий в области международной информационной безопасности»), являющемся неотъемлемой частью настоящего Соглашения.

Приложение 1 может по мере необходимости дополняться, уточняться и обновляться по согласованию Сторон.

Статья 2. Основные угрозы в области обеспечения международной информационной безопасности

Реализуя сотрудничество в соответствии с настоящим Соглашением, Стороны исходят из наличия следующих основных угроз в области обеспечения международной информационной безопасности:

1) разработка и применение информационного оружия, подготовка и ведение информационной войны;

2) информационный терроризм;

3) информационная преступность;

4) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств;

5) распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств;

6) угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

Согласованное понимание Сторонами существа перечисленных в настоящей статье основных угроз приведено в Приложении 2 (Перечень основных видов угроз в области международной информационной безопасности, их источников и признаков), являющемся неотъемлемой частью настоящего Соглашения.

Приложение 2 может по мере необходимости дополняться, уточняться и обновляться по согласованию Сторон.

Статья 3. Основные направления сотрудничества

С учетом угроз, указанных в статье 2 настоящего Соглашения, Стороны, их уполномоченные представители, а также компетентные органы государств Сторон, которые определяются в соответствии со статьей 5 настоящего Соглашения, осуществляют сотрудничество

в области обеспечения международной информационной безопасности по следующим основным направлениям:

1) определение, согласование и осуществление необходимых совместных мер в области обеспечения международной информационной безопасности;

2) создание системы мониторинга и совместного реагирования на возникающие в этой области угрозы;

3) выработка совместных мер по развитию норм международного права в области ограничения распространения и применения информационного оружия, создающего угрозы обороноспособности, национальной и общественной безопасности;

4) противодействие угрозам использования информационно-коммуникационных технологий в террористических целях;

5) противодействие информационной преступности;

6) проведение необходимых для целей настоящего Соглашения экспертиз, исследований и оценок в области обеспечения информационной безопасности;

7) содействие обеспечению безопасного, стабильного функционирования и интернационализации управления глобальной сетью Интернет;

8) обеспечение информационной безопасности критически важных структур государств Сторон;

9) разработка и осуществление совместных мер доверия, способствующих обеспечению международной информационной безопасности;

10) разработка и осуществление согласованной политики и организационно-технических процедур по реализации возможностей использования электронной цифровой подписи и защиты информации при трансграничном информационном обмене;

11) обмен информацией о законодательстве государств Сторон по вопросам обеспечения информационной безопасности;

12) совершенствование международно-правовой базы и практических механизмов сотрудничества Сторон в обеспечении международной информационной безопасности;

13) создание условий для взаимодействия компетентных органов государств Сторон в целях реализации настоящего Соглашения;

14) взаимодействие в рамках международных организаций и форумов по проблемам обеспечения международной информационной безопасности;

15) обмен опытом, подготовка специалистов, проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов Сторон в области информационной безопасности;

16) обмен информацией по вопросам, связанным с осуществлением сотрудничества по перечисленным в настоящей статье основным направлениям.

Стороны или компетентные органы государств Сторон могут по взаимной договоренности определять другие направления сотрудничества.

Статья 4. Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество и свою деятельность в международном информационном пространстве в рамках настоящего Соглашения таким образом, чтобы такая деятельность способствовала социальному и экономическому развитию и была совместимой с задачами поддержания международной безопасности и стабильности, соответствовала общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека, а также принципам регионального сотрудничества и невмешательства в информационные ресурсы государств Сторон.

2. Деятельность Сторон в рамках настоящего Соглашения должна быть совместимой с правом каждой Стороны искать, получать и распространять информацию с учетом того, что такое право может быть ограничено законодательством в целях защиты интересов национальной и общественной безопасности.

3. Каждая Сторона имеет равное право на защиту информационных ресурсов и критически важных структур своего государства от неправомерного использования и несанкционированного вмешательства, в том числе от информационных атак на них.

Каждая Сторона не проводит по отношению к другой Стороне подобных действий и оказывает содействие другим Сторонам в реализации вышеуказанного права.

Статья 5. Основные формы и механизмы сотрудничества

1. В течение шестидесяти дней с даты вступления настоящего Соглашения в силу Стороны обменяются через депозитария данными о компетентных органах государств Сторон, ответственных за реализацию настоящего Соглашения, и каналах прямого обмена информацией по конкретным направлениям сотрудничества.

2. С целью рассмотрения хода выполнения настоящего Соглашения, обмена информацией, анализа и совместной оценки возникающих угроз информационной безопасности, а также определения, согласования

и координации совместных мер реагирования на такие угрозы Стороны проводят на регулярной основе консультации уполномоченных представителей Сторон и компетентных органов государств Сторон (далее – консультации).

Очередные консультации проводятся по согласованию Сторон, как правило, один раз в полугодие в Секретариате Шанхайской организации сотрудничества или на территории государства одной из Сторон по ее приглашению.

Любая из Сторон может инициировать проведение внеочередных консультаций, предлагая время и место, а также повестку дня для последующего согласования со всеми Сторонами и Секретариатом Шанхайской организации сотрудничества.

3. Практическое взаимодействие по конкретным направлениям сотрудничества, предусмотренным настоящим Соглашением, Стороны могут осуществлять по линии компетентных органов государств Сторон, ответственных за реализацию Соглашения.

4. В целях создания правовых и организационных основ сотрудничества по конкретным направлениям компетентные органы государств Сторон могут заключать соответствующие договоры межведомственного характера.

Статья 6. Защита информации

1. Настоящее Соглашение не налагает на Стороны обязательств по предоставлению информации в рамках сотрудничества в соответствии с настоящим Соглашением и не является основанием для передачи информации в рамках этого сотрудничества, если раскрытие такой информации может нанести ущерб национальным интересам.

2. В рамках сотрудничества в соответствии с настоящим Соглашением Стороны не осуществляют обмен информацией, которая согласно законодательству государства любой из Сторон относится к государственной тайне и (или) государственным секретам. Порядок передачи и обращения с подобной информацией, которая в конкретных случаях может считаться необходимой для целей исполнения настоящего Соглашения, регулируется на основании и на условиях соответствующих договоров между Сторонами.

3. Стороны обеспечивают надлежащую защиту передаваемой или создаваемой в ходе сотрудничества в рамках настоящего Соглашения информации, не относящейся в соответствии с законодательством государства любой из Сторон к государственной тайне и (или) государственным секретам, доступ к которой и распространение которой

ограничены в соответствии с законодательством и (или) соответствующими нормативно-правовыми актами государства любой из Сторон.

Защита такой информации осуществляется в соответствии с законодательством и (или) соответствующими нормативно-правовыми актами государства получающей Стороны. Такая информация не раскрывается и не передается без письменного согласия Стороны, являющейся источником этой информации.

Такая информация должным образом обозначается в соответствии с законодательством и (или) соответствующими нормативно-правовыми актами государств Сторон.

Статья 7. Финансирование

1. Стороны самостоятельно несут расходы по участию их представителей и экспертов в соответствующих мероприятиях по исполнению настоящего Соглашения.

2. В отношении прочих расходов, связанных с исполнением настоящего Соглашения, Стороны в каждом отдельном случае могут согласовывать иной порядок финансирования в соответствии с законодательством государств Сторон.

Статья 8. Отношение к другим международным договорам

Настоящее Соглашение не затрагивает прав и обязательств каждой из Сторон по другим международным договорам, участником которых является ее государство.

Статья 9. Разрешение споров

Стороны решают спорные вопросы, которые могут возникнуть в связи с толкованием или применением положений настоящего Соглашения, путем консультаций и переговоров.

Статья 10. Рабочие языки

Рабочими языками при осуществлении сотрудничества в рамках настоящего Соглашения являются русский и китайский языки.

Статья 11. Депозитарий

Депозитарием настоящего Соглашения является Секретариат Шанхайской организации сотрудничества.

Подлинный экземпляр настоящего Соглашения хранится у депозитария, который в течение пятнадцати дней с даты его подписания направит Сторонам его заверенные копии.

Статья 12. Заключительные положения

1. Настоящее Соглашение заключается на неопределенный срок и вступает в силу на тридцатый день с даты получения депозитарием четвертого уведомления в письменной форме о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу. Для Стороны, выполнившей внутригосударственные процедуры позднее, настоящее Соглашение вступает в силу на тридцатый день с даты получения депозитарием соответствующего уведомления.

2. Стороны могут вносить изменения в настоящее Соглашение, которые по взаимному согласию Сторон оформляются отдельным протоколом.

3. Настоящее Соглашение не направлено против каких-либо государств и организаций и после его вступления в силу открыто для присоединения любого государства, разделяющего цели и принципы настоящего Соглашения, путем передачи депозитарию документа о присоединении. Для присоединяющегося государства настоящее Соглашение вступает в силу по истечении тридцати дней с даты получения депозитарием последнего уведомления о согласии на такое присоединение подписавших его и присоединившихся к нему государств.

4. Каждая из Сторон может выйти из настоящего Соглашения, направив депозитарию в письменной форме уведомление об этом не менее чем за девяносто дней до предполагаемой даты выхода. Депозитарий извещает о таком намерении другие Стороны в течение тридцати дней с даты получения такого уведомления.

5. В случае прекращения действия настоящего Соглашения Стороны принимают меры для полного выполнения обязательств по защите информации, а также ранее согласованных совместных работ, проектов и иных мероприятий, осуществляемых в рамках Соглашения и не завершенных к моменту прекращения действия Соглашения.

Совершено в г. Екатеринбурге 16 июня 2009 года в одном подлинном экземпляре на русском и китайском языках, причем оба текста имеют одинаковую силу.

Приложение 1
к Соглашению между правительствами
государств –членов Шанхайской организации сотрудничества
о сотрудничестве в области обеспечения
международной информационной безопасности

ПЕРЕЧЕНЬ ОСНОВНЫХ ПОНЯТИЙ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

«Информационная безопасность» – состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве;

«информационная война» – противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны;

«информационная инфраструктура» – совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации;

«информационное оружие» – информационные технологии, средства и методы, применяемые в целях ведения информационной войны;

«информационная преступность» – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях;

«информационное пространство» – сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;

«информационные ресурсы» – информационная инфраструктура, а также собственно информация и ее потоки;

«информационный терроризм» – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях;

«критически важные структуры» – объекты, системы и институты государства, воздействие на которые может иметь последствия, прямо затрагивающие национальную безопасность, включая безопасность личности, общества и государства;

«международная информационная безопасность» – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве;

«неправомерное использование информационных ресурсов» – использование информационных ресурсов без соответствующих прав или с нарушением установленных правил, законодательства государств Сторон либо норм международного права;

«несанкционированное вмешательство в информационные ресурсы» – неправомерное воздействие на процессы формирования, создания, обработки, преобразования, передачи, использования, хранения информации;

«угроза информационной безопасности» – факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве.

Приложение 2
к Соглашению между правительствами
государств –членов Шанхайской организации сотрудничества
о сотрудничестве в области обеспечения международной
информационной безопасности

ПЕРЕЧЕНЬ ОСНОВНЫХ ВИДОВ УГРОЗ В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ИХ ИСТОЧНИКОВ И ПРИЗНАКОВ

1. Разработка и применение информационного оружия, подготовка и ведение информационной войны.

Источником этой угрозы являются создание и развитие информационного оружия, представляющего непосредственную угрозу для критически важных структур государств, что может привести к новой гонке вооружений и представляет главную угрозу в области международной информационной безопасности.

Ее признаками являются применение информационного оружия в целях подготовки и ведения информационной войны, а также воз-

действия на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться перед лицом агрессора и не может воспользоваться законным правом самозащиты; нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах; деструктивное воздействие на критически важные структуры.

2. Информационный терроризм.

Источником этой угрозы являются террористические организации и лица, причастные к террористической деятельности, осуществляющие противоправные действия посредством или в отношении информационных ресурсов.

Ее признаками являются использование информационных сетей террористическими организациями для осуществления террористической деятельности и привлечения в свои ряды новых сторонников; деструктивное воздействие на информационные ресурсы, приводящее к нарушению общественного порядка; контролирование или блокирование каналов передачи массовой информации; использование сети Интернет или других информационных сетей для пропаганды терроризма, создания атмосферы страха и паники в обществе, а также иные негативные воздействия на информационные ресурсы.

3. Информационная преступность.

Источником этой угрозы являются лица или организации, осуществляющие неправомерное использование информационных ресурсов или несанкционированное вмешательство в такие ресурсы в преступных целях.

Ее признаками являются проникновение в информационные системы для нарушения целостности, доступности и конфиденциальности информации; умышленное изготовление и распространение компьютерных вирусов и других вредоносных программ; осуществление *DOS*-атак (отказ в обслуживании) и иных негативных воздействий; причинение ущерба информационным ресурсам; нарушение законных прав и свобод граждан в информационной сфере, в том числе права интеллектуальной собственности и неприкосновенности частной жизни; использование информационных ресурсов и методов для совершения таких преступлений, как мошенничество, хищение, вымогательство, контрабанда, незаконная торговля наркотиками, распространение детской порнографии и т.д.

4. Использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других стран.

Источником этой угрозы является неравномерность в развитии информационных технологий в различных государствах и существующая тенденция к увеличению «цифрового разрыва» между развитыми и развивающимися странами. Некоторые государства, имеющие преимущества в развитии информационных технологий, умышленно ограничивают развитие прочих стран и получение доступа к информационным технологиям, что приводит к возникновению серьезной опасности для государств с недостаточными информационными возможностями.

Ее признаками являются монополизация производства программного обеспечения и оборудования информационных инфраструктур, ограничение участия государств в международном информационно-технологическом сотрудничестве, препятствующее их развитию и увеличивающее зависимость этих стран от более развитых государств; встраивание скрытых возможностей и функций в программное обеспечение и оборудование, поставляемые в другие страны, для контроля и влияния на информационные ресурсы и (или) критически важные структуры этих стран; контроль и монополизация рынка информационных технологий и продуктов в ущерб интересам и безопасности государств.

5. Распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Источником этой угрозы являются государства, организации, группа лиц или частные лица, использующие информационную инфраструктуру для распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Ее признаками являются появление и тиражирование в электронных (радио и телевидение) и прочих средствах массовой информации, в сети Интернет и других сетях информационного обмена информации:

искажающей представление о политической системе, общественном строе, внешней и внутренней политике, важных политических и общественных процессах в государстве, духовных, нравственных и культурных ценностях его населения;

пропагандирующей идеи терроризма, сепаратизма и экстремизма;

разжигающей межнациональную, межрасовую и межконфессиональную вражду.

6. Угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

Источниками этих угроз являются стихийные бедствия и другие опасные природные явления, а также катастрофы техногенного характера, возникающие внезапно или в результате длительного процесса, способные оказать масштабное разрушительное воздействие на информационные ресурсы государства.

Их признаками являются нарушение функционирования объектов информационной инфраструктуры и, как следствие, дестабилизация критически важных структур, государственных систем управления и принятия решений, результаты которой прямо затрагивают безопасность государства и общества.

4.8. Европейский Союз (ЕС)

СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ ЕВРОПЕЙСКОГО СОЮЗА: ОТКРЫТОЕ, БЕЗОПАСНОЕ И ЗАЩИЩЕННОЕ КИБЕРПРОСТРАНСТВО[1]

(Брюссель, 7 февраля 2013 г.)

1. Введение

1.1. Контекст

Интернет и киберпространство в более широком смысле оказали огромное влияние на все части общества в течение двух последних десятилетий. Наша повседневная жизнь, основные права, социальное взаимодействие и экономики зависят от бесперебойной работы информационных технологий и технологий связи. Открытое и свободное киберпространство способствует вовлеченности в политическую и общественную жизнь во всем мире, устраняет барьеры между странами, сообществами и гражданами, позволяет взаимодействовать и обмениваться информацией и идеями в мировом масштабе, обеспе-

[1] Стратегия кибербезопасности Европейского союза была представлена Совместным информационным оокладом Европейскому Парламенту, Совету Европы, Европейскому экономическому и социальному комитету и Комитету регионов. – URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (неофициальный перевод О.В. Демидова и М.Б. Касеновой).

чивает площадку для свободы выражения и реализации основных прав, а также наделяет людей правами в своих поисках демократического и более справедливого общества, что наиболее отчетливо проявилось во время «Арабской весны».

Для того, чтобы киберпространство оставалось открытым и свободным, те же самые нормы, принципы и ценности, которые ЕС поддерживает за пределами Сети, должны также применяться в Сети. Основные права, демократия и верховенство закона нуждаются в защите в киберпространстве. Наша свобода и процветание все больше зависят от надежного и инновационного Интернета, расцвет которого продолжится, если инновации частного сектора и гражданское общество будут стимулировать его рост. Тем не менее свобода в Сети требует также безопасности и защищенности. Киберпространство следует защищать от происшествий, вредоносной деятельности и злоупотреблений, и правительства играют значимую роль в обеспечении свободного и безопасного киберпространства. У правительств имеются несколько задач: защищать доступ и открытость, уважать и защищать основные права в Сети, а также поддерживать надежность и способность к взаимодействию сети «Интернет». Тем не менее частный сектор является владельцем и управляет значительными частями киберпространства, в связи с чем любая инициатива, нацеленная на успех в данной области, должна признавать его ведущую роль.

Информационно-коммуникационные технологии стали основой нашего экономического роста и являются критичным ресурсом, от которого зависят все отрасли экономики. В настоящее время они поддерживают сложные системы, которые поддерживают работоспособность ключевых секторов экономики, таких как финансы, здравоохранение, энергетика и транспорт, в то время как многие бизнес-модели строятся на непрерывной доступности Интернета и бесперебойном функционировании информационных систем.

Создав Единый цифровой рынок, Европа смогла увеличить свой ВВП на почти 500 миллиардов € в год[1]; что составляет в среднем 1000 € на человека. Гражданам требуется доверие и надежность для развития новых сетевых технологий, включая электронные платежи, облачную обработку данных или межмашинную коммуникацию[2]. К сожалению, исследование «Евробарометр» (*Eurobarometer*), проведенное в 2012 году[3], показало, что практически треть европейцев не уверены

[1] URL: http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

[2] Например, установки с внедренными датчиками для связи с системой орошения, когда наступает время наполнить из водой.

[3] Специальное исследование «Евробарометр 390 по кибербезопасности», 2012 г.

в своей способности пользоваться Интернетом для банковских операций или для покупок. Подавляющее большинство также сообщило, что избегает раскрывать личную информацию в Сети по соображениям безопасности. Более одного из десяти пользователей Интернета в масштабе ЕС уже стали жертвами сетевого мошенничества.

Последние годы показали, что, несмотря на огромные выгоды, которые несет с собой цифровой мир, он также является уязвимым. Происшествия в сфере кибербезопасности[1], независимо от того, являются они преднамеренными или случайными, растут с тревожащей скоростью и могут нарушить предоставление важных услуг, которые мы принимаем как данность, таких как услуги водоснабжения, здравоохранения, энергоснабжения или мобильной связи. Угрозы могут иметь разное происхождение, в том числе уголовные, политически мотивированные или организуемые государством атаки, а также стихийные бедствия и непреднамеренные ошибки.

Экономика ЕС уже страдает от киберпреступлений[2] против частного сектора и физических лиц. Киберпреступники используют все более изощренные методы проникновения в информационные системы, осуществляя кражу критически важных данные или требуя выкуп у компаний. Рост экономического шпионажа и действий, организуемых государствами в киберпространстве, представляет собой новую категорию угроз для правительств и компаний ЕС.

Правительства в странах, не входящих в ЕС, также могут злоупотреблять киберпространством в целях наблюдения и контроля своих собственных граждан. ЕС может противостоять такой ситуации, способствуя свободе в Сети и обеспечивая уважение основных прав в Сети.

Все данные факторы показывают, почему правительства во всем мире начали разрабатывать стратегии кибербезопасности и рассматри-

[1] Под кибербезопасностью обычно понимаются меры защиты и действия, которые можно осуществить для защиты киберпространства как в гражданской, так и в военной области от угроз, которые связаны с его взаимозависимыми сетями и информационной инфраструктурой или могут нанести им урон. Кибербезопасность стремится защитить доступность и целостность сетей и инфраструктуры, а также конфиденциальность содержащейся в них информации.

[2] Под киберпреступностью обычно понимается широкий спектр различных преступных деяний, в которых компьютеры и информационные сети задействованы в качестве основного орудия или в качестве основной цели. Киберпреступность включает в себя традиционные преступления (напр., мошенничество, подделки и хищение персональных данных), преступления, связанные с контентом (напр., распространение детской порнографии в сети или подстрекательство к расовой ненависти), и преступления, относящиеся только к компьютерам и информационным системам (напр., атаки на информационные системы, отказ в предоставлении услуги и вредоносные программные средства).

вать киберпространство в качестве международной проблемы, приобретающей все бóльшую важность. Для ЕС пришло время активизировать свою работу в данной сфере. В данном предложении для Стратегии кибербезопасности, внесенном Комиссией и Верховным представителем Союза по иностранным делам и политике безопасности (Верховным представителем) изложено видение ЕС в данной области, уточнены роли и обязанности и определены требуемые действия, основанные на мощной и эффективной защите и содействии правам граждан для того, чтобы сетевая среда ЕС стала самой безопасной в мире.

1.2. Принципы кибербезопасности

Безграничный и многослойный Интернет стал одним из самых мощных инструментов общемирового прогресса без государственного надзора и регулирования. В то время как частный сектор должен и далее играть ведущую роль в развитии и повседневном управлении Интернетом, необходимость наличия требований к прозрачности, подотчетности и безопасности становится все более заметной. В данной стратегии уточняются принципы, которыми должна руководствоваться политика кибербезопасности в ЕС и в международном плане.

Базовые ценности ЕС распространяются на цифровой мир в той же степени, что и на физический мир

В киберпространстве действуют те же самые законы и нормы, которые распространяются также на другие сферы нашей повседневной жизни.

Защита основных прав, свободы самовыражения, персональных данных и частной жизни

Кибербезопасность может быть надежной и эффективной только в том случае, когда она основывается на основных правах и свободах, закрепленных в Хартии Европейского Союза по правам человека, и на базовых ценностях ЕС. Соответственно права частных лиц невозможно защитить при отсутствии надежных сетей и систем. Любое совместное использование информации в целях кибербезопасности, если речь идет о личных данных, должно соответствовать законодательству ЕС по защите данных и полностью учитывать права частных лиц в данной области.

Доступ для всех

Ограниченный доступ к Интернету или его отсутствие и «цифровая неграмотность» представляют собой неблагоприятное состояние для граждан, учитывая то, насколько компьютерный мир способствует

деятельности в рамках общества. Каждый должен иметь возможность доступа к Интернету и к неограниченному потоку информации. Целостность и безопасность интернета должны гарантироваться для обеспечения безопасного доступа для всех.

Демократичное и эффективное руководство заинтересованных лиц

Цифровой мир не контролируется одним лицом. В настоящее время существует несколько заинтересованных лиц, большинство из которых являются коммерческими и негосударственными организациями, принимающими участие в ежедневном управлении ресурсами, протоколами и стандартами Интернета, а также занимающимися развитием интернета в будущем. ЕС подтверждает важность всех заинтересованных лиц в существующей модели управления Интернетом и поддерживает данный подход к руководству со стороны заинтересованных лиц[1].

Общая ответственность за обеспечение безопасности

Растущая зависимость от информационно-коммуникационных технологий во всех сферах человеческой жизни ведет к уязвимостям, которые нуждаются в надлежащем определении, тщательном анализе, устранении или уменьшении. Всем соответствующим субъектам, органам государственной власти, частному сектору или отдельным гражданам необходимо признать данную общую ответственность, предпринять действия для самозащиты и при необходимости обеспечить скоординированный ответ для укрепления кибербезопасности.

2. Стратегические приоритеты и действия

ЕС следует защищать сетевую среду, обеспечивая максимально возможную свободу и безопасность к пользе всех. В данной Стратегии предлагаются конкретные действия, которые могут повысить эффективность деятельности ЕС в целом, одновременно подтверждая, что решение проблем безопасности в киберпространстве является в первую очередь задачей Стран-участниц. Указанные действия являются как краткосрочными, так и долгосрочными, включают в себя разнообразные политические инструменты[2], и связаны с разными типами субъектов, будь то учреждения ЕС, Страны-участницы или промышленность.

[1] См. также *COM*(2009) 277, Информационный доклад Комиссии Европейскому Парламенту и Совету «Управление Интернетом: следующие шаги».

[2] Действия, относящиеся к коллективному доступу к информации, если речь идет о персональных данных, должны соответствовать закону о защите данных ЕС.

Видение ЕС, представленное в настоящей Стратегии, воплощено в пяти стратегических приоритетах, которые обращены к подчеркнутым выше проблемам:

- Достижение киберустойчивости
- Радикальное уменьшение киберпреступности
- Разработка политики и потенциала кибероборонны, связанных с Общей политикой безопасности и обороны (ОПБО)
- Развитие промышленных и технологических ресурсов кибербезопасности
- Выработка последовательной политики международного киберпространства для Европейского Союза и продвижение базовых ценностей ЕС

2.1. Достижение киберустойчивости

Как органы государственной власти, так и частный сектор должны развивать потенциал и эффективно сотрудничать для развития киберустойчивости в ЕС. Основанные на положительных результатах, достигнутых посредством мероприятий, осуществленных до настоящего времени[1], дальнейшие действия ЕС могут помочь, в частности, борьбе с киберрисками и угрозами, имеющими трансграничный масштаб, и способствовать скоординированному реагированию в чрезвычайных ситуациях. Это станет надежным подспорьем хорошему функционированию внутреннего рынка и укрепит внутреннюю безопасность ЕС.

Европа останется уязвимой в отсутствие существенных усилий по наращиванию государственного и частного потенциала, ресурсов и процессов для предупреждения, обнаружения и устранения происшествий в сфере кибербезопасности. По этой причине Комиссия разработала политику сетевой и информационной безопасности (СИБ)[2]. **Европейское агентство по сетевой и информационной безопасности (*ENISA*)** было создано в 2004 году[3]. Совет и Парламент

[1] См. ссылки в настоящем Информационном докладе, а также в Рабочем документе персонала Комиссии «Оценка влиянии», приложенном к предложению Комиссии для Директивы по сетевой и информационной безопасности, в частности разделы 4.1.4, 5.2, Приложение 2, Приложение 6, Приложение 8.

[2] В 2001 году Комиссия приняла информационный доклад «Сетевая и информационная безопасность: Предложение для подхода к Европейской политике» (*COM*(2001)298); в 2006 году она приняла Стратегию для безопасного информационного общества (*COM*(2006)251). Начиная с 2009 года Комиссия также приняла План действий и Информационный доклад по защите критичной информационной инфраструктуры (ЗКИИ) (*COM*(2009)149, одобренный Резолюцией Совета 2009/C 321/01; и *COM*(2011)163, одобренное Заключениями Совета 10299/11).

[3] Регламент (ЕС) № 460/2004

проводят согласование нового Регламента для укрепления *ENISA* и обновления мандата Агентства[1]. В дополнение к этому Рамочная директива по электронным коммуникациям[2] требует от провайдеров электронных коммуникаций соответствующим образом управлять рисками для своих сетей и информировать о значительных нарушениях безопасности. Законодательство о защите данных ЕС также[3] требует от контролеров данных обеспечивать выполнение требований и мер по защите данных, в том числе мер, относящихся к безопасности, и в сфере услуг электронных коммуникаций открытого доступа. Контролеры данных должны уведомлять компетентные национальные органы о происшествиях, связанных с нарушениями в отношении персональных данных.

Несмотря на прогресс, основанный на добровольно принятых обязательствах, в масштабе ЕС по-прежнему существуют разрывы, в частности, в национальных возможностях, координации в случае распространения происшествий через границы и в участию и готовности частного сектора. Настоящая Стратегия сопровождается предложением для **законодательных органов**, в частности:

• Определить минимальные общие требования к СИБ на национальном уровне, которые будут обязывать Страны-участницы: назначить компетентные национальные органы для СИБ; создать хорошо функционирующие группы быстрого реагирования на нарушения компьютерной безопасности; а также принять национальную стратегию СИБ и национальный план сотрудничества в сфере СИБ. Развитие потенциала и координация также относятся к учреждениям ЕС: Группа быстрого реагирования на нарушения компьютерной безопасности, отвечающая за безопасность ИТ-систем учреждений, агентств и органов ЕС («*CERT-EC*») была создана на постоянной основе в 2012 г.

• Создать согласованные механизмы предотвращения, выявления, устранения и реагирования, позволяющие национальным компетентным органам СИБ осуществлять совместное использование информации и содействие друг другу. Компетентным национальным органам СИБ будет поручено обеспечить соответствующее сотрудничество в масштабе ЕС, в частности, на основе плана сотрудничества Союза в области СИБ, разработанного для реагирования на кибер-

[1] *COM*(2010)521. Действия, предложенные в данной Стратегии, не влекут за собой внесение изменений в существующий или будущий мандат *ENISA*.

[2] Статьи 13*a* и 13*b* Директивы 2002/21/ЕС.

[3] Статья 17 Директивы 95/46/ЕС; статья 4 Директивы 2002/58/ЕС.

происшествия трансграничного масштаба. Данное сотрудничество будет также строиться на основе прогресса, достигнутого в контексте «Европейского форума для стран-участниц (*EFMS*)»[1], в ходе которого состоялись продуктивные обсуждения и обмен мнениями по государственной политике СИБ, и который можно интегрировать с уже действующим механизмом сотрудничества.

• Повысить подготовленность и вовлеченность частного сектора. Поскольку значительное большинство сетевых и информационных систем принадлежат и эксплуатируются частными лицами, повышение вовлеченности частного сектора в укрепление кибербезопасности является решающим. Частному сектору следует разработать собственный потенциал киберустойчивости на техническом уровне и осуществить обмен передовой практикой среди отраслей. Инструменты, разработанные промышленностью для реагирования на инциденты, выявления причин и проведения судебных экспертиз, также должны принести пользу государственному сектору.

Тем не менее у частных субъектов по-прежнему отсутствуют эффективные стимулы для представления надежных данных о существовании или влиянии происшествий в области СИБ, принятия культуры риск-менеджмента или инвестирования в решения по безопасности. Предлагаемый законопроект соответственно нацелен на обеспечение того, чтобы субъекты ряда ключевых направлений (а именно энергетика, транспорт, банковское дело, фондовые биржи и инструменты реализации ключевых служб Интернета, а также государственные администрации) оценивали риски кибербезопасности, которые им угрожают, обеспечивали надежность и устойчивость сетей и информационных систем с помощью соответствующего риск-менеджмента, а также предоставляли выявленную информацию в национальные компетентные органы СИБ. Принятие культуры кибербезопасности может улучшить возможности для бизнеса и повысить конкурентоспособность в частном секторе, что может превратить кибербезопасность в коммерческий аргумент.

Указанные субъекты должны будут информировать компетентные национальные органы СИБ о происшествиях со значительным влиянием на непрерывность ключевых услуг и поставки товаров, зависящих от сетевых и информационных систем.

[1] Европейский форум для стран-участниц был запущен посредством *COM*(2009) 149 в качестве платформы, способствующей обсуждению практики надлежащей политики безопасности и устойчивости Критичной информационной инфраструктуры среди органов государственной власти Стран-участниц.

Компетентные национальные органы СИБ должны сотрудничать и обмениваться информацией с другими регулирующими органами, в частности, с органами защиты персональных данных. Компетентные органы НИС должны в свою очередь информировать правоохранительные органы о происшествиях с предполагаемым серьезным криминальным характером. Компетентные национальные органы также должны регулярно публиковать на специально выделенном сайте несекретную информацию о текущих заблаговременных предупреждениях о происшествиях и рисках и о согласованном реагировании. Правовые обязательства не должны подменять собой или препятствовать развитию неформального и добровольного сотрудничества, в том числе между государственным и частным секторами, для повышения уровней безопасности, обмена информацией и передовой практикой. В частности, Европейское государственно-частное партнерство для устойчивости (*EP3R*[1]) является надежной и законной платформой на уровне ЕС, которую следует развивать дальше.

Программа объединения европейских инфраструктур *Connecting Europe Facility* (*CEF*)[2] будет оказывать финансовую поддержку ключевой инфраструктуре, связывая потенциал СИБ Стран-участниц и облегчая сотрудничество в масштабе ЕС.

В заключение, учения по реагированию на киберпроисшествия на уровне ЕС являются значимыми для стимулирования сотрудничества между Странами-участницами и частным сектором. Первое учение с участием Стран-участниц было проведено в 2010 г. («Кибер Европа 2010»). Второе учение, в котором также принимал участие частный сектор, состоялось в октябре 2012 г. («Кибер Европа 2012»). Командно-штабное учение ЕС и США проводилось в ноябре 2011 г. («Кибер Атлантик 2011»). Последующие учения планируются в ближайшем будущем, в том числе с участием международных партнеров.

[1] Европейское государственно-частное партнерство для устойчивости начало свое работу посредством документа *COM*(2009) 149. Данная платформа инициировала работу и способствует сотрудничеству между государственным и частным секторами в определении ключевых активов, ресурсов, функций и базовых требований к устойчивости, а также потребностей сотрудничества и механизмов реагирования на крупномасштабные нарушения, влияющие на электронные коммуникации.

[2] https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. Бюджетная строка CEF 09.03.02 – Телекоммуникационные сети (для содействия взаимосвязи и операционной совместимости публичных национальных услуг в сети, а также доступа к таким сетям).

Комиссия:
• Будет продолжать свою работу, осуществляемую Совместным исследовательским центром в тесном сотрудничестве с органами власти, владельцами и операторами критичной инфраструктуры Стран-участниц, по определению уязвимостей СИБ для критичной европейской инфраструктуры, и поощряя разработку устойчивых систем. • Запустит в начале 2013 г. пилотный проект, финансируемый ЕС[1], по **борьбе с бот-сетями и вредоносными программными средствами**, для обеспечения рамочной основы координации и сотрудничества между странами – участницами ЕС, организациями частного сектора, такими как Провайдеры услуг Интернета, и международными партнерами.
Комиссия поручает *ENISA*:
• Оказывать содействие Странам-участницам в развитии мощного **национального потенциала киберустойчивости**, в частности путем накопления экспертного опыта безопасности и устойчивости промышленных систем управления, транспортной и энергетической инфраструктуры. • Изучить в 2013 году целесообразность создания Группы (групп) реагирования на происшествия, связанные с компьютерной безопасностью, для Промышленных систем управления (*ICS-CSIRT*) для ЕС. • Продолжить поддерживать Страны-участницы и учреждения ЕС в проведении регулярных общеевропейских учений по реагированию на киберпроисшествия, которые будут также представлять собой операционную основу участия ЕС в международных учениях по реагированию на киберпроисшествия.
Комиссия предлагает Европейскому парламенту и Совету:
• Быстро принять предложение в отношении **Директивы об общем высоком уровне сетевой и информационной безопасности (СИБ)** в масштабе Союза, учитывающей национальные функциональные возможности и готовность, сотрудничество на уровне ЕС, реализацию практики риск-менеджмента и совместное использование информации о СИБ.
Комиссия поручает промышленности:
• Принять на себя лидерство в **инвестировании** в киберзащиту высокого уровня и разработать передовую практику и обмен информацией на уровне отрасли и с государственными органами с целью

[1] CIP-ICT PSP-2012-6, 325188. Общий бюджет составляет 15 млн евро, в том числе финансирование ЕС в размере 7,7 млн Евро.

обеспечения надежной и эффективной защиты активов и частных лиц, в частности, посредством государственно-частных партнерств, таких как *EP3R* и «Доверие в цифровой жизни» (*TDL*)[2].

Повышение осведомленности

Обеспечение кибербезопасности является общей ответственностью. Конечные пользователи играют очень значимую роль в обеспечении безопасности сетей и информационных систем: им необходимо знать о рисках, с которыми они сталкиваются в Сети, и иметь право предпринимать простые шаги для защиты от них.

Несколько инициатив было разработано в последние годы, и их следует продолжать. В частности, агентство *ENISA* принимало участие в повышении осведомленности путем публикации отчетов, организации экспертных семинаров, и развития государственно-частного партнерства. Европол, Евроюст и национальные органы защиты данных также ведут активную деятельность для повышения осведомленности. В октябре 2012 г. агентство *ENISA* совместно с рядом Стран-участниц провело первый «Месячник европейской кибербезопасности». Повышение осведомленности является одним из направлений, в котором активно действует Рабочая группа ЕС и США по кибербезопасности и киберпреступлениям[2], а также является важным в контексте «Программы повышения безопасности Интернета»[3] (где основное внимание уделяется безопасности детей в Сети).

Комиссия поручает ENISA:

• Предложить в 2013 году «дорожную карту» для «Прав на сетевую и информационную безопасность» в качестве добровольной программы сертификации для продвижения расширенных навыков и компетенции профессионалов в сфере ИТ (например, администраторов интернет-сайтов).

[1] http://www.trustindigitallife.eu/

[2] Данной Рабочей группе, созданной на Саммите ЕС – США в ноябре 2010 г. (*MEMO*/10/597), поручено решение задач, связанных с выработкой совместных подходов по широкому спектру проблем кибербезопасности и киберпреступности.

[3] Программа повышения безопасности Интернета финансирует сеть НГО, активно действующих в сфере охраны детей в Сети, сеть правоохранительных органов, которые обмениваются информацией и передовой практикой, касающихся использования Интернета в преступных целях для распространения материалов сексуальной эксплуатации детей, а также сеть исследователей, собирающих информацию об использовании, рисках и последствиях применения сетевых технологий для жизней детей.

Комиссия:
• Организует при поддержке *ENISA* **чемпионат** по кибербезопасности в 2014 г., в ходе которого студенты университетов будут соревноваться, предлагая решения по СИБ.
Комиссия предлагает Странам-участницам[1]:
• Ежегодно организовывать **месячник кибербезопасности** при поддержке *ENISA* и с участием частного сектора, начиная с 2013 г., с целью повысить осведомленность среди конечных пользователей. Синхронизированный месячник кибербезопасности ЕС – США будет организовываться, начиная с 2014 г. • **Активизировать государственную деятельность по образованию и обучению СИБ** путем введения: обучения СИБ в школах к 2014 г.; обучения СИБ, разработке защищенного программного обеспечения и защите персональных данных для студентов по направлению «Вычислительная техника»; а также базового обучения СИБ для сотрудников, работающих в органах государственного управления.
Комиссия предлагает промышленности:
• Повышать **осведомленность** о кибербезопасности **на всех уровнях**, как в практике деловых отношений, так и при взаимодействии с клиентами. В частности, промышленности следует продумать пути повышения ответственности главных должностных лиц и советов директоров за обеспечение кибербезопасности.

2.2. Радикальное уменьшение киберпреступности

Чем больше мы живем в цифровом мире, тем больше возникает возможностей, используемых киберпреступниками. Киберпреступность является одной из наиболее быстро растущих форм преступности, жертвами которой ежедневно становятся более миллиона людей во всем мире. Киберпреступники и киберпреступные сети становятся все более изощренными, и мы нуждаемся в соответствующих оперативных средствах и функциональных возможностях, чтобы справляться с ними. Киберпреступления отличаются большой выгодой и малым риском, и преступники часто использует анонимность доменов интернет-сайтов. Киберпреступность не знает границ – глобальный охват Интернета означает, что правоохранительные органы должны использовать согласованный и совместный трансграничный подход для реагирования на такую растущую угрозу.

[1] Также при участии соответствующих национальных органов, включая компетентные органы по СИБ и органы защиты данных.

Мощное и эффективное законодательство

ЕС и Страны-участницы нуждаются в мощном и эффективном законодательстве для борьбы с киберпреступностью. Конвенция Совета Европы по киберпреступности, также известная как «Будапештская конвенция», является обязывающим международным договором, который обеспечивает эффективную рамочную основу для принятия национального законодательства.

ЕС уже принял законодательные акты о киберпреступности, в том числе Директиву по борьбе с сексуальной эксплуатацией детей в Сети и детской порнографией[1]. ЕС также планирует согласовать в ближайшем будущем Директиву по атакам на информационные системы, в частности, путем использования бот-сетей.

Комиссия:
• Будет обеспечивать быстрое транспонирование и реализацию директив, относящихся к киберпреступности. • Призывает те Страны-участницы, которые еще не ратифицировали **Будапештскую конвенцию Совета Европы по киберпреступности**, ратифицировать и реализовать ее положения в возможно короткий срок.

Усиленный оперативный потенциал для борьбы с киберпреступностью

Развитие методов киберпреступности быстро ускорилось: правоохранительные органы не могут бороться с киберпреступностью, используя устаревшие оперативные средства. В настоящее время не все Страны-участницы ЕС обладают оперативными возможностями, которые необходимы им для эффективного реагирования на киберпреступления. Все Страны-участницы нуждаются в эффективных национальных подразделениях по борьбе с киберпреступностью.

Комиссия:
• Будет поддерживать Страны-участницы через финансируемые ею программы[4] для **выявления недостатков и укрепления их способности** проводить расследования и бороться с киберпреступностью. В дополнение к этому Комиссия будет поддерживать организации,

[1] Директива 2011/93/ЕС, заменившая Рамочное решение Совета 2004/68/*JHA*.

[2] В 2013 г. в рамках Программы профилактики и борьбы с преступностью (*ISEC*). После 2013 г. через Фонд внутренней безопасности (новый инструмент в рамках Долгосрочной финансовой рамочной основы (*MFF*)).

которые связывают исследовательские/учебные заведения, субъектов правоохранительной деятельности и частный сектор, аналогично текущей работе, осуществляемой финансируемыми Комиссией центрами передового опыта по борьбе с киберпреступностью, уже созданными в ряде Стран-участниц.

• Совместно со Странами-участницами будет координировать работу по выявлению передовой практики и наилучших имеющихся технологий по борьбе с киберпреступностью, в том числе при поддержке Совместного исследовательского центра (например, в области разработки и использования инструментов судебной экспертизы или анализа угроз).

• Будет тесно взаимодействовать с недавно начавшим работу **Европейским центром по борьбе с киберпреступностью (*EC*3), Европолом и Евроюстом** для согласования таких политических подходов с передовой практикой оперативной деятельности.

Улучшение координации на уровне ЕС

ЕС может дополнить работу Стран-участниц, содействуя скоординированному и совместному подходу, объединяя правоохранительные органы, органы юстиции, заинтересованные государственные и частные организации ЕС и за пределами ЕС.

Комиссия:

• Будет поддерживать недавно начавший работу **Европейский центр по борьбе с киберпреступностью (*EC*3)** в качестве европейского координационного центра по борьбе с киберпреступностью. *EC*3 будет обеспечивать анализ и оперативную информацию, поддерживать расследования, обеспечивать судебную экспертизу высокого уровня, содействовать сотрудничеству, создавать каналы для обмена информацией между компетентными органами в Странах-участницах, частным сектором и другими заинтересованными сторонами, а также постепенно станет выразителем мнения правоохранительного сообщества[1].

• Будет поддерживать меры по усилению ответственности регистраторов доменных имен и обеспечению точности информации о владельцах интернет-сайтов, в частности на основе Правоохранительных рекомендация для Корпорации Интернета по распределению имен

[1] 28 марта 2012 г. Европейская комиссия приняла информационный доклад «Борьба с преступностью в цифровую эпоху: создание Европейского центра борьбы с киберпреступностью».

и адресов (*ICANN*), в соответствии с законодательством ЕС, включая правила по защите данных.
• Будет развивать существующее законодательство с целью продолжить усиление мер ЕС по борьбе с сексуальной эксплуатацией детей в Сети. Комиссия приняла Европейскую стратегию по хорошему Интернету для детей[1] и совместно со странами, входящими и не входящими в ЕС, стала инициатором **Глобального альянса против сексуальной эксплуатации детей в Сети**[2]. Альянс является инструментом для дальнейших действий Стран-участниц, поддерживаемых Комиссией и *ЕС*3.
Комиссия поручает Европолу (*ЕС*3):
• Первоначально сконцентрировать свою аналитическую и оперативную поддержку на расследованиях киберпреступлений в Странах-участницах, помочь ликвидировать и разрушить киберпреступные сети, в первую очередь в сфере сексуальной эксплуатации детей, мошенничеств с платежами, бот-сетей и вторжений.
• Регулярно готовить стратегические и оперативные отчеты о тенденциях и возникающих угрозах для определения приоритетов и целей следственных мероприятий, проводимых подразделениями по борьбе с киберпреступностью в Странах-участницах.
Комиссия поручает Европейскому полицейскому колледжу (*CEPOL*) совместно с Европолом:
• Координировать разработку и планирование учебных курсов с целью вооружить правоохранительные органы знаниями и экспертным опытом для эффективной борьбы с киберпреступностью.
Комиссия поручает Евроюсту:
• Определить основные препятствия на пути сотрудничества органов юстиции по расследованию киберпреступлений и координации между Странами-участницами и третьими странами, поддерживать расследование и преследование киберпреступлений как на оперативном, так и на стратегическом уровне, а также учебные мероприятия в данной сфере.
Комиссия поручает Евроюсту и Европолу (*ЕС*3):
• Тесно сотрудничать, в том числе путем обмена информацией, с целью повышения собственной эффективности в борьбе с киберпреступностью, в соответствии со своими мандатами и компетенцией.

[1] *COM*(2012 г.) 196 окончательный вариант.

[2] Заключения Совета по Глобальному альянсу против сексуальной эксплуатации детей в сети (Совместное заявление ЕС и США от 7 и 8 июня 2012 г. и Декларация о создании Глобального альянса против сексуальной эксплуатации детей в сети (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm)).

2.3. Разработка политики и потенциала кибероборонны, связанных с Общей политикой безопасности и обороны (ОПБО)

Мероприятия по кибербезопасности в ЕС также связаны с аспектом кибероборонны. Развитие потенциала кибероборонны следует сконцентрировать на выявлении, реагировании и восстановлении после изощренных киберугроз для повышения устойчивости систем связи и информации, обеспечивающих интересы Стран-участниц в сфере обороны и национальной безопасности.

Учитывая, что угрозы носят комплексный характер, следует усилить синергию между гражданским и военным подходами к защите критичных киберактивов. Указанные мероприятия следует поддерживать исследованиями и разработками, а также более тесным сотрудничеством между правительствами, частным сектором и учебными заведениями в ЕС. Во избежание дублирования ЕС изучит возможности того, как ЕС и НАТО смогут дополнить усилия друг друга по повышению устойчивости критичной государственной, военной и другой информационной инфраструктуры, от которой зависят члены обеих организаций.

Верховный представитель сосредоточится на следующих ключевых мероприятиях и предлагает Странам-участницам и Европейскому оборонному агентству вести совместную работу по следующим направлениям:

- Оценка оперативных требований ЕС к кибероборонне и содействие развитию функциональных возможностей и технологий кибероборонны ЕС для учета всех аспектов развития потенциала, включая принципы, руководство, организацию, персонал, обучение, технологию, инфраструктуру, логистику и способность к взаимодействию;
- Разработка рамочной основы политики кибероборонны ЕС для защиты сетей в рамках миссий и операций ОПБО, в том числе динамичное управление рисками, улучшение анализа угроз и совместное использование информации. Расширение возможностей для обучения и проведения учений по кибербезопасности для военнослужащих в европейском и многонациональном контексте, включая интегрирование элементов кибероборонны в существующие программы учений;
- Содействие диалогу и координации между гражданскими и военными субъектами в ЕС, обращая особое внимание на обмен передовой практикой, обмен информацией и ранее предупреждение, реагирование на происшествия, оценку рисков, повышение осведомленности и определение кибербезопасности в качестве приоритета;

• Обеспечение диалога с международными партнерами, в том числе НАТО, другими международными организациями и международнысм центрами передового опыта, обеспечение эффективного оборонного потенциала, определение направлений для сотрудничества и избежание дублирования усилий.

2.4. Развитие промышленных и технологических ресурсов для кибербезопасности

Европа обладает превосходными возможностями для научно-исследовательских и опытно-конструкторских работ, но многие общемировые лидеры, предоставляющие инновационные продукты и услуги информационно-коммуникационных технологий (ИКТ), находятся за пределами ЕС. Существует риск, что Европа не только станет в чрезмерной степени зависимой от ИКТ, производимых за ее пределами, но также и от решений по безопасности, разработанных вне ее границ. Ключевым моментом является обеспечение того, чтобы те аппаратные и программные компоненты, производимые в ЕС и третьих странах, которые используются в критичных услугах и инфраструктуре и все чаще применяются в мобильных устройствах, являлись надежными, защищенными и гарантировали защиту персональных данных.

Развитие единого рынка для продуктов кибербезопасности

Высокий уровень безопасности можно обеспечить только в случае, если все участники производственно-сбытовой цепочки (напр., изготовители оборудования, разработчики программного обеспечения, провайдеры услуг для информационного общества) придают первостепенное значение безопасности. Представляется[1], тем не менее, что многие игроки по-прежнему рассматривают безопасность как нечто не намного большее, чем дополнительное бремя, и спрос на решения по безопасности является ограниченным. Соответствующие требования к эффективности кибербезопасности следует реализовать в масштабе всей производственно-сбытовой цепочки продукции ИКТ, используемой в Европе. Частному сектору требуются стимулы для обеспечения высокого уровня кибербезопасности; например, маркировка, указывающая на соответствующую эффективность кибербезопасности, позволит компаниям с высокой эффективностью и опытом кибербе-

[1] См. Рабочий документ персонала Комиссии по оценке влияния, прилагаемый к предложению Комиссии по Директиве о сетевой и информационной безопасности, раздел 4.1.5.2.

зопасности превратить ее в выигрышный момент и добиться конкурентного преимущества. Обязательства, изложенные в предложенной Директиве по СИБ, также внесут значительный вклад в повышение конкурентоспособности бизнеса в охватываемых секторах.

Следует также стимулировать спрос на продукцию с высокой степенью защиты в масштабе Европы. Во-первых, данная Стратегия нацелена на укрепление сотрудничества и повышение прозрачности в отношении безопасности продукции ИКТ. Она призывает создать платформу, сводящую воедино соответствующие европейские государственные и частные заинтересованные лица, для определения надлежащей практики кибербезопасности в масштабе производственно-сбытовой цепочки и создания выгодной рыночной конъюнктуры для разработки и принятия решений по ИКТ. Основные усилия следует сосредоточить на создании стимулов для реализации соответствующего управления рисками и принятия стандартов и решений по безопасности, а также для возможного создания схем добровольной сертификации в масштабе ЕС, основанных на схемах, существующих в ЕС и в мире. Комиссия будет способствовать принятию согласованных подходов Странами-участницами во избежание неравенства, являющегося причиной местных неблагоприятных факторов для предприятий.

Во-вторых, Комиссия будет поддерживать разработку стандартов безопасности и оказывать содействие для схем добровольной сертификации в масштабе ЕС в сфере облачной обработки данных, одновременно учитывая необходимость обеспечения защиты данных. Работу следует сконцентрировать на безопасности цепочки снабжения, в частности, в критичных отраслях экономики (промышленные системы управления, энергетика и транспортная инфраструктура). Такая работа должна основываться на текущей работе по стандартизации, осуществляемой Европейскими организациями по стандартизации (Европейский комитет по нормализации, СЕНЭЛЕК и Европейский институт стандартов связи)[1], Координационной группой по кибербезопасности (*CSCG*), а также на экспертном опыте *ENISA*, Комиссии и другими соответствующими субъектами.

Комиссия:
• Откроет в 2013 году государственно-частную **платформу по решениям СИБ** по выработке стимулов для принятия защищенных решений

[1] В частности, в соответствии со Стандартом для интеллектуальных сетей *M*/490 для первого пакета стандартов по интеллектуальным сетям и эталонной архитектуре.

в области ИКТ и обеспечении надлежащей эффективности кибербезопасности, распространяющейся на продукцию ИКТ, используемую в Европе.

• Предложит в 2014 году рекомендации по обеспечению кибербезопасности в масштабе производственно-сбытовой цепочки ИКТ, основываясь на работе указанной платформы.

• Изучит, каким образом основные провайдеры аппаратного и программного обеспечения ИКТ могут информировать компетентные органы о выявленных уязвимых местах, которые могут иметь существенные последствия для безопасности.

Комиссия поручает *ENISA*:

• Разработать, совместно с соответствующими национальными компетентными органами, соответствующими заинтересованными лицами, международными и европейскими организациями по стандартизации и Совместным исследовательским центром Европейской комиссии **технические руководства и рекомендации для принятия стандартов СИБ и рекомендуемых норм** в государственном и частном секторах.

Комиссия предлагает государственным и частным заинтересованным лицам:

• Стимулировать разработку и принятие под руководством промышленности **стандартов безопасности**, технических норм и принципов проектной безопасности проектной конфиденциальности изготовителями продукции ИКТ и провайдерами услуг, в том числе провайдерами облачной обработки данных; новые поколения программного и аппаратного обеспечения следует обеспечивать **более мощными, внедренными и удобными для использования** средствами **безопасности**.

• Разработать под руководством промышленности стандарты эффективной кибербезопасности компаний и повысить качество информации, доступной для публики, путем разработки **меток безопасности** или знаков качества, помогающих потребителю ориентироваться на рынке.

Поддержка инвестиций в НИОКР и инноваций

НИОКР могут поддерживать мощную промышленную политику, способствовать развитию надежной европейской отрасли ИКТ, развивать внутренний рынок и уменьшить зависимость Европы от иностранных технологий. НИОКР должны заполнить технологические разрывы в безопасности ИКТ, готовиться к следующему поколению

вызовов в сфере безопасности, учитывать непрерывное развитие потребностей пользователей и воспользоваться выгодами технологий двойного назначения. Следует также продолжить поддержку развития криптографии. Данные мероприятия необходимо дополнить усилиями по переводу результатов НИОКР в коммерческие решения, предоставляя необходимые стимулы и устанавливая соответствующие политические условия.

ЕС следует наилучшим образом воспользоваться Рамочной программой исследований и инноваций «Горизонт 2020»[1] , которая начнет работу в 2014 году. В предложении Комиссии содержатся конкретные задачи для надежных ИКТ, а также для борьбы с киберпреступностью, которые соответствуют данной стратегии. Программа «Горизонт 2020» будет поддерживать исследования безопасности, связанные с развивающимися технологиями ИКТ, предоставлять решения для комплексных защищенных систем ИКТ, услуг и приложений, обеспечивать стимулы для реализации и принятия существующих решений, а также учитывать способность к взаимодействию между сетевыми и информационными системами. На уровне ЕС особое внимание будет уделяться оптимизации и совершенствованию координации различных программ финансирования («Горизонт 2020, Фонд внутренней безопасности, исследования Европейского оборонного агентства, в том числе Европейское рамочное сотрудничество).

Комиссия:

- Будет использовать программу «Горизонт 2020» для рассмотрения ряда направлений конфиденциальности и безопасности ИКТ, от НИОКР до инноваций и развертывания. В рамках программы «Горизонт 2020» будут также разрабатываться средства и инструменты для борьбы с преступной и террористической деятельностью, нацеленной на киберсреду.
- Будет создавать механизмы для улучшения координации исследовательских тематик учреждений Европейского Союза и Стран-участниц, а также стимулировать Страны-участницы к увеличению инвестиций в НИОКР.

[1] «Горизонт 2020» является финансовым инструментом для реализации *Инновационного союза* – флагманской инициативы *«Европа 2020»*, нацеленной на обеспечение глобальной конкурентоспособности Европы. Новая Рамочная программа исследований и инноваций ЕС, которая будет осуществляться с 2014 по 2020 год, станет частью усилий, направленных на обеспечение нового роста и создание рабочих мест в Европе.

Комиссия предлагает Странам-участницам:
• Разработать до конца 2013 г. надлежащую практику использования **покупательной способности органов государственного управления** (такую, как посредством государственных закупок) для стимулирования разработки и развертывания элементов безопасности в продукции и услугах ИКТ. • Способствовать опережающему участию промышленности и учебных заведений в разработке и координации решений. Это следует выполнять путем максимального использования промышленной базы Европы и соответствующих технологических инноваций НИОКР, при координации исследовательских тематик гражданских и военных организаций;
Комиссия поручает Европолу и *ENISA*:
• Определять возникающие тенденции и потребности с учетом изменяющихся моделей киберпреступности и кибербезопасности для разработки соответствующих цифровых аналитических инструментов и технологий.
Комиссия предлагает государственным и частным заинтересованным лицам:
• Совместно со страховой отраслью разработать **гармонизированные показатели для расчета страховых премий за риск**, которые позволят компаниям, инвестировавшим в безопасность, получать преимущества от меньших по размеру премий за риск.

2.5. Выработка последовательной политики международного киберпространства для Европейского Союза и продвижение базовых ценностей ЕС

Сохранение открытого, свободного и защищенного киберпространства является общемировой проблемой, которую ЕС следует рассматривать совместно с соответствующими международными партнерами и организациями, частным сектором и гражданским обществом.

В своей международной политике киберпространства ЕС будет стремиться способствовать открытости и свободе Интернета, поощрять усилия, направленные на развитие норм поведения и применения существующего международного законодательства в киберпространстве. ЕС также будет работать над преодолением цифрового разделения и активно участвовать в международных усилиях по развитию потенциала кибербезопасности. Международное участие ЕС в проблемах киберпространства будет определяться базовыми цен-

ностями ЕС: человеческим достоинством, свободой, демократией, равенством, верховенством закона и уважением основных прав.

Включение проблем киберпространства в международные отношения ЕС и Общую внешнюю политику и политику безопасности

Комиссия, Верховный представитель и Страны-участницы должны озвучивать последовательную политику ЕС в отношении международного киберпространства, которая будет нацелена на усиление участия и более прочные отношения с ключевыми международными партнерами и организациями, а также с гражданским обществом и частным сектором. Консультации ЕС с международными партнерами по проблемам киберпространства следует планировать, координировать и реализовывать с целью повышения ценности существующих двусторонних диалогов между Странами – участницами ЕС и третьими странами. ЕС будет снова делать акцент на диалоге с третьими странами, уделяя особое внимание партнерам, придерживающимся такого же мнения, которые разделяют ценности ЕС. Он будет содействовать достижению высокого уровня защиты данных, в том числе в отношении передачи персональных данных третьей стране. Для того, чтобы справиться с глобальными проблемами в киберпространстве, ЕС будет стремиться к более тесному сотрудничеству с организациями, которые активно действуют в данной области, такими как Совет Европы, ОЭСР, ООН, ОБСЕ, НАТО, Африканский союз, АСЕАН и ОАГ. Сотрудничество с Соединенными Штатами Америки является особенно важным на двустороннем уровне и будет развиваться и далее, в частности, в контексте Рабочей группы ЕС и США по кибербезопасности и киберпреступности.

Одним из основных элементов международной киберполитики ЕС будет заключаться в продвижении киберпространства в качестве территории свободы и основных прав. Расширение доступа к Интернету должно способствовать демократической реформе и ее продвижению в мировом масштабе. Растущая глобальная взаимосвязь не должна сопровождаться цензурой или массовым наблюдением. ЕС следует поддерживать корпоративную социальную ответственность[1] и выступать инициатором международных инициатив по улучшению глобальной координации в данной сфере.

Все субъекты мирового информационного общества, от граждан до правительств, несут ответственность за более безопасное киберпространство. ЕС поддерживает усилия по определению норм поведения

[1] Обновленная стратегия Корпоративной социальной ответственности ЕС на 2011–2014 гг.; *COM*(2011) 681 окончательный вариант

в киберпространстве, которые следует соблюдать всем заинтересованным лицом. Государства должны следовать нормам и существующему законодательству точно так же, как ЕС ожидает соблюдения гражданского долга, социальной ответственности и законодательства в Сети от граждан. ЕС поощряет выработку мер укрепления доверия в отношении кибербезопасности, увеличение прозрачности и уменьшение риска неправильного восприятия поведения государств в вопросах международной безопасности.

ЕС не призывает к созданию новых международных правовых инструментов в отношении проблем кибербезопасности.

Правовые обязательства, закрепленные в Международном пакте о гражданских и политических правах, Европейской конвенции о защите прав человека и Хартии ЕС по правам человека, должны также соблюдаться в Сети. ЕС сосредоточит свое внимание на том, чтобы обеспечить выполнение данных мер и в киберпространстве.

Будапештская конвенция является инструментом, открытым для принятия третьими странами, для решения проблемы киберпреступности. Она предусматривает модель для составления национальных законодательных актов в отношении киберпреступности и является основой для международного сотрудничества в данной сфере.

Если вооруженные конфликты будут распространяться на киберпространство, международное гуманитарное право и в случае необходимости право в области прав человека будут применяться к соответствующей ситуации.

Наращивание потенциала кибербезопасности и развитие устойчивой информационной инфраструктуры в третьих странах

Растущее международное сотрудничество будет благотворно сказываться на бесперебойном функционировании базовой инфраструктуры, которая обеспечивает и содействует оказанию услуг связи. Оно включает в себя обмен передовой практикой, совместное использование информации, заблаговременное предупреждения, совместные учения по контролю происшествий и так далее. ЕС будет способствовать достижению данной цели путем активизации текущих международных мероприятий по усилению сетей сотрудничества в сфере защиты критичной информационной инфраструктуры (ЗКИИ), при участии правительств и частного сектора.

Не все части мира получают выгоду от положительного влияния Интернета по причине отсутствия открытого, защищенного, совместимого и надежного доступа. Европейский Союз соответственно продолжит

поддержку усилий стран в их стремлении к развитию доступа и использования Интернета своими гражданами, для обеспечения целостности, безопасности, и эффективной борьбы с киберпреступностью.

Комиссия и Верховный представитель совместно со Странами-участницами:

• Будут работать над последовательной международной политикой ЕС в сфере киберпространства для большей вовлеченности ключевых международных партнеров и организаций, включения проблем киберпространства в Общую внешнюю политику и политику безопасности, а также в плане совершенствования координации по глобальным вопросам киберпространства;

• Будут поддерживать разработку норм поведения и мер укрепления давления в сфере кибербезопасности. Будут способствовать диалогу по вопросам применения существующего международного права в киберпространстве и способствовать применению Будапештской конвенции в отношении киберпреступности;

• Будут поддерживать развитие и защиту основных прав, в том числе доступ к информации и свободу самовыражения, обращая особое внимание на: *a*) разработку новых публичных основных принципов свободы самовыражения в Сети и вне Сети; *b*) контроль экспорта продукции или услуг, которые могут использоваться для цензуры или массового наблюдения в Сети; *c*) разработку мер и инструментов для расширения доступа к Интернету, открытости и устойчивости к цензуре или массовому наблюдению с помощью технологии связи; *d*) предоставление прав заинтересованным лицам для использования технологии связи с целью обеспечения основных прав;

• Будут взаимодействовать с международными партнерами и организациями, частным сектором и гражданским обществом для поддержки наращивания общемирового потенциала в третьих странах с целью совершенствования доступа к информации и открытому Интернету, предотвращения и борьбы с киберугрозами, включая случайные события, киберпреступность и кибертерроризм, а также совершенствовать координацию помощи для руководства мероприятиями по наращиванию потенциала;

• Будут использовать различные инструменты помощи ЕС для наращивания потенциала кибербезопасности, включая содействие в обучении персонала правоохранительных органов, органов юстиции и технического персонала для устранения киберугроз, а также поддерживать создание соответствующей национальной политики, стратегий и учреждений в третьих странах;

• Будут увеличивать координацию политики и совместное использование информации посредством международных сетей защиты критичной информационной инфраструктуры, таких как сеть «Меридиан», сотрудничество между компетентными органами СИБ и другими лицами.

3. Распределение обязанностей и ответственности

Киберпроисшествия не останавливаются на границах взаимосвязанной цифровой экономики и общества. Все субъекты, от компетентных органов СИБ, групп быстрого реагирования на нарушения компьютерной безопасности и правоохранительных органов до промышленности, должны принять на себя ответственность, как в национальном масштабе, так и на уровне ЕС, и совместно работать для укрепления кибербезопасности. Ключевой проблемой для ЕС является уточнение распределения ролей и ответственности большого количества участвующих субъектов, поскольку различные правовые рамочные основы и юрисдикции могут оказаться вовлеченными.

Учитывая сложность вопроса и широкий круг участвующих субъектов, централизованный европейский надзор не является ответом. Национальные правительства находятся в наилучшем положении для организации предотвращения и реагирования на киберпроисшествия и атаки, а также для налаживания контактов и создания сетей с частным сектором и широкой публикой с помощью собственных установленных политических каналов и правовой рамочной основы. В то же время для эффективного национального реагирования часто требуется участие на уровне ЕС по причине потенциальной или фактической природы рисков, не имеющих границ. Для комплексного решения проблемы кибербезопасности мероприятия должны охватывать три ключевых направления: СИБ, правоохранительные органы и оборона, которые также функционируют в рамках разных нормативных основ:

	Сетевая и информационная безопасность		**Правоохранительные органы**		**Оборона**		
ЕС	• Комиссия / ENISA • Группа CERT-EC • Сеть компетентных органов • EP3R	⬅ ➡	• EC3/ Европол • CEPOL • Евроюст	⬅ ➡	• EEAS • Европейское оборонное агентство	⬅ ➡	

	Сетевая и информационная безопасность		**Правоохранительные органы**		**Оборона**		
	⬆⬇		⬆⬇		⬆⬇		**Промышленность Учебные заведения**
НАЦИОНАЛЬНЫЙ УРОВЕНЬ	• Национальные группы CERT • Компетентные органы СИБ	⬅ ➡	• Национальные подразделения по борьбе с киберпреступностью	⬅ ➡	• Национальные органы обороны и безопасности	⬅ ➡	

3.1. Координация между компетентными органами СИБ/группами *CERT*, правоохранительными органами и оборонными ведомствами

Национальный уровень

Странам-участницам следует иметь, как уже на сегодняшний день, так и в результате применения данной Стратегии, структуры, способные заниматься киберустойчивостью, киберпреступностью и обороной, и они должны достичь потенциала требуемого уровня для реагирования на киберпроисшествия. Тем не менее, учитывая, что ряд субъектов может нести оперативную ответственность за различные стороны кибербезопасности, и принимая во внимание важность привлечения частного сектора, координацию на национальном уровне следует оптимизировать в масштабе министерств. Странам-участницам следует распределить обязанности и ответственность различных национальных органов в своих национальных стратегиях кибербезопасности.

Следует поощрять обмен информацией между национальными органами и частным сектором, позволяющий Странам-участницам и частному сектору иметь общее представление о различных угрозах и лучше понять новые тенденции и методы, используемые как для совершения кибератак, так и для более быстрого реагирования на них. Определив национальные планы сотрудничества в области СИБ, вводимые в действие в случае киберпроисшествий, Страны-участницы должны быть в состоянии четко распределять обязанности и ответственность, а также оптимизировать меры реагирования.

Уровень ЕС

Так же как и на национальном уровне, на уровне ЕС существует ряд субъектов, занимающихся кибербезопасностью. В частности, *ENISA*,

Европол/*EC*3 и Европейское оборонное агентство (*EDA*) являются тремя агентствами, действующими соответственно с позиции СИБ, охраны правопорядка и обороны. В данных агентствах имеются дирекции, в которых представлены Страны-участницы, и они представляют собой платформы для координации на уровне ЕС.

Координация и сотрудничество между *ENISA*, Европолом/*EC*3 и *EDA* будут поощряться по ряду направлений, в которых они ведут совместную деятельность, в частности применительно к анализу тенденций, оценке рисков, обучению и обмену передовой практикой. Агентства должны сотрудничать, одновременно сохраняя свою специфику. Указанные агентства, совместно с *CERT-EC*, Комиссией и Странами-участницами должны поддерживать создание надежного сообщества технических и политических экспертов в данной сфере.

Неофициальные каналы координации и сотрудничества будут дополняться связями с большей структурированностью. Военный персонал ЕС и группа проекта киберзащиты *EDA* могут использоваться в качестве вектора для координации в вопросах обороны. В Совете программы Европол/*EC*3 будут принимать участие в числе прочих ЕВРОЮСТ, *CEPOL*, Страны-участницы[1], *ENISA* и Комиссия. Совет дает возможность обменяться отличительными ноу-хау и обеспечит, чтобы мероприятия *EC*3 осуществлялись в партнерстве, признавая добавленный экспертный опыт и соблюдая мандаты всех заинтересованных лиц. Новый мандат *ENISA* позволит усилить связь агентства с Европолом и укрепить связи с заинтересованными лицами в промышленности. Самое важное состоит в том, что законодательное предложение Комиссии по СИБ создаст рамочную основу для сотрудничества посредством сети компетентных национальных органов СИБ и решить вопрос обмена информацией между органами СИБ и правоохранительными органами.

Международный уровень

Комиссия и Верховный представитель совместно со Странами-участницами, обеспечат скоординированные международные действия в сфере кибербезопасности. При этом Комиссия и Верховный представитель будут поддерживать базовые ценности ЕС и способствовать мирному, открытому и прозрачному использованию кибертехнологий. Комиссия, Верховный представитель и Страны-участницы ведут политический диалог с международными партнерами и международны-

[1] Через представительство в Рабочей группе по киберпреступности ЕС, в состав которой входят руководители подразделений по борьбе с киберпреступностью Стран – участниц ЕС

ми организациями, такими как Совет Европы, ОЭСР, ОБСЕ, НАТО и ООН.

3.2. Поддержка ЕС в случае серьезного киберпроисшествия или атаки

Существует вероятность того, что серьезные киберпроисшествия или атаки окажут влияние на правительства, предприятия и частных лиц в ЕС. В результате принятия данной Стратегии и, в частности, предлагаемой директивы по СИБ, предотвращение, выявление и реагирование на киберпроисшествия должны улучшиться. Страны-участницы и Комиссия станут более информированными о серьезных киберпроисшествиях или атаках. Тем не менее механизмы реагирования будут различаться в зависимости от характера, величины и трансграничных последствий инцидента.

Если происшествие оказывает серьезное влияние на непрерывность ведения деятельности, в директиве по СИБ предлагается ввести в действие национальные планы сотрудничества по СИБ или планы на уровне ЕС, в зависимости от трансграничного характера происшествия. Сеть компетентных органов СИБ будет использоваться в данном контексте для обмена информацией и поддержки. Это позволит сохранить и/или восстановить пострадавшие сети и услуги.

Если, как представляется, происшествие связано с преступлением, следует проинформировать Европол/*EC*3, с тем чтобы указанные организации совместно с правоохранительными органами пострадавших стран могли начать расследование, сохранить доказательства, выявить злоумышленников и в конечном счете убедиться, что в отношении таковых начато преследование.

Если происшествие, как представляется, относится к кибершпионажу или атаке, организованной государством, или же влечет за собой последствия для национальной безопасности, национальные органы безопасности и обороны будут предупреждать своих соответствующих коллег, с тем чтобы они знали о том, что их атакуют, и могли защитить себя. В этом случае будут введены в действие механизмы раннего предупреждения, а также процедуры управления кризисными ситуациями или другие процедуры при необходимости. Особо серьезное киберпроисшествие или атака могут представлять собой достаточное основание для Страны-участницы для ввода в действие Статьи о солидарности ЕС (статья 222 Договора о функционировании Европейского Союза).

Если представляется, что персональные данные оказались скомпрометированными в результате происшествия, следует привлечь на-

циональные органы защиты данных или национальные регулирующие органы в соответствии с Директивой 2002/58/ЕС.

В конечном счете контактные сети и поддержка со стороны международных партнеров принесут пользу в решении проблем с киберпроисшествиями и атаками. Сюда могут относиться техническое уменьшение угрозы, уголовное расследование или ввод в действие механизмов кризисного реагирования.

4. Заключение и последующие действия

В данной предлагаемой Стратегии кибербезопасности Европейского Союза, внесенной Комиссией и Верховным представителем Союза по иностранным делам и политике безопасности, изложено видение ЕС и определены требуемые действия, основанные на мощной и эффективной защите и содействии правам граждан для того, чтобы сетевая среда ЕС стала самой безопасной в мире[1].

Данное видение можно реализовать только в подлинном партнерстве, с участием большого количества субъектов, с тем чтобы принять на себя ответственность и решать будущие проблемы.

Комиссия и Верховный представитель соответственно предлагают Совету и Европейскому парламенту одобрить стратегию и помочь осуществить изложенные мероприятия. Мощная поддержка и готовность выполнять обязательства также потребуются со стороны частного сектора и гражданского общества, которые являются ключевыми действующими лицами в деле повышения уровня безопасности и защиты прав граждан.

Время для действий наступило. Комиссия и Верховный представитель настроены на совместную работу со всеми субъектами для обеспечения безопасности, которая необходима Европе. Комиссия и Вер-

[1] Финансирование Стратегии будет осуществляться в пределах предусматриваемых сумм для каждого из соответствующих направлений политики (Программа *CEF*, «Горизонт 2020», Фонд внутренней безопасности, Общая внешняя политика и политика безопасности и Внешнее сотрудничество, в частности «Инструмент стабильности»), как определено в предложении Комиссии для Долгосрочной финансовой рамочной основы на 2014–2020 гг. (с учетом утверждения Бюджетным органом и окончательных сумм для принятой Долгосрочной финансовой рамочной основы на 2014–2020 гг.). Учитывая необходимость обеспечения общей совместимости с рядом позиций, имеющихся для децентрализованных агентств, и подуровня для децентрализованных агентств по каждой статье расходов, в следующей Долгосрочной финансовой рамочной основе агентствам (*CEPOL, EDA, ENISA*, ЕВРОЮСТ и ЕВРОПОЛ/*ЕС*3), от которых в настоящем Информационном докладе требуется, чтобы они приняли на себя новые задачи, настоятельно предлагается сделать это с учетом того, что фактическая способность агентства принять растущие ресурсы установлена и все возможности для реорганизации определены.

ховный представитель соберут все соответствующие стороны на конференции высокого уровня и оценят ход выполнения работ за год с целью обеспечить оперативную реализацию стратегию и ее оценку с учетом возможных будущих событий.

4.9. «Группа восьми» (*G*8)

ДОВИЛЬСКАЯ ДЕКЛАРАЦИЯ «ГРУППЫ ВОСЬМИ»: «НЕИЗМЕННАЯ ПРИВЕРЖЕННОСТЬ СВОБОДЕ И ДЕМОКРАТИИ»

(27 мая 2011 г.)
(Извлечение)

<...>

II. Интернет

4. Во всем мире интернет стал неотъемлемой частью общества и экономики, залогом экономического роста и социального развития.

5. Для граждан интернет – это уникальный информационный и образовательный ресурс, что делает его ценным инструментом для продвижения свободы, демократии и прав человека.

6. Для бизнеса интернет стал важнейшим и незаменимым инструментом ведения торговли и совершенствования отношений с потребителями. Интернет как движущая сила развития инноваций и фактор повышения эффективности способствует экономическому росту и повышению занятости.

7. Для правительств интернет является инструментом, позволяющим более эффективно осуществлять администрирование и предоставлять услуги частным лицам и бизнесу, а также улучшать отношения со своими гражданами и обеспечивать уважение и поддержку прав человека.

8. Интернет стал одной из основных движущих сил глобальной экономики, фактором стимулирования роста и инновационного развития.

9. Открытость, транспарентность и свобода интернета стали ключевыми факторами его развития и успешного функционирования. Эти принципы, равно как и принципы недискриминации и добросовестной конкуренции, должны и впредь лежать в основе развития интернета.

10. Соблюдение этих принципов должно осуществляться в более широком контексте уважения верховенства закона, прав человека и основных свобод, защиты прав на интеллектуальную собственность – то есть всего того, что составляет суть любого демократического общества и служит на благо всех

его граждан. Мы абсолютно убеждены, что необходимо стремиться одновременно к достижению свободы и безопасности, соблюдению транспарентности и конфиденциальности в той же неразрывной связи, как между соблюдением прав человека и исполнением им своих обязанностей. Защита этих базовых механизмов и принципов и предоставление соответствующих гарантий должны осуществляться как в интернете, так и в любой другой сфере нашей жизни.

11. Интернет стал общественной ареной нашего времени, рычагом экономического развития и инструментом достижения политической свободы и эмансипации. Соблюдение свободы слова, выражения мнений, информации, собраний и ассоциации должно быть гарантировано в отношении интернета в той же степени, что и в любой другой сфере общества. Наличие произвольной или неизбирательной цензуры и ограничение доступа в интернет идут вразрез с международными обязательствами государств и абсолютно неприемлемы. Более того, это препятствует экономическому и социальному росту.

12. Интернет и его будущее развитие, поддерживаемые частными инициативами и инвестициями, требуют благоприятного, транспарентного, стабильного и предсказуемого климата, основанного на изложенных выше принципах. В этой связи от всех правительств требуется осуществление соответствующей национальной политики, а также интенсификация международного сотрудничества в этой области.

13. Мы решительно нацелены на стимулирование использования интернета в качестве инструмента продвижения прав человека и демократии во всем мире.

14. Глобальная цифровая экономика стала мощным экономическим фактором и локомотивом роста и инноваций. Доступ к широкополосному интернету является абсолютно необходимым условием участия в сегодняшней экономической жизни. Для того, чтобы наши страны могли получить максимальную отдачу от цифровой экономики, нам нужно использовать открывающиеся возможности, связанные в том числе с технологиями «облачных» вычислений, социальными сетями и публикацией информации гражданами, которые способствуют инновациям и социальному росту. По мере того, как мы переходим к более инновационным интернет-услугам, мы сталкиваемся с вызо-

вами, связанными с обеспечением совместимости и конвергенции политики наших государств по таким вопросам, как защита личных данных, нейтральность сетей, трансграничное перемещение данных, безопасность ИКТ и интеллектуальная собственность.

15. В отношении защиты интеллектуальной собственности, в частности авторского права, торговых марок, профессиональных секретов и патентов, мы признаем необходимость национальных законов и механизмов, которые позволили бы более эффективно осуществлять такую защиту, в то же время стимулируя развитие интернет-торговли товарами и контентом, не нарушающей прав на интеллектуальную собственность. Таким образом, мы еще раз подтверждаем нашу приверженность обеспечению эффективных действий по борьбе с нарушениями прав на интеллектуальную собственность в сфере цифровых технологий в настоящее время и в будущем. Мы признаем, что эффективное внедрение правил, регулирующих сферу интеллектуальной собственности, требует соответствующих усилий со стороны заинтересованных сторон в рамках международного сотрудничества, в том числе с частным сектором. Мы решительно нацелены на определение путей, способствующих большему доступу и открытости в отношении знаний, образования и культуры, включая поощрение постоянных инноваций в осуществлении законной интернет-торговли товарами и контентом при уважении к правам интеллектуальной собственности.

16. Эффективная защита личных данных и неприкосновенности частной жизни в интернете является важнейшим условием доверия пользователей. Это касается всех заинтересованных сторон: пользователей, которые должны быть лучше осведомлены о своей ответственности при размещении в интернете личных данных; поставщиков услуг, которые хранят и обрабатывают эти данные; правительств и регулирующих органов, которые должны обеспечивать эффективную защиту этих данных. Мы призываем разработать общие подходы, с учетом национальных законодательств и на основе соблюдения основных прав, которые защищали бы персональные данные, в то же время позволяя осуществлять законную передачу данных.

17. Безопасность сетей и услуг в интернете – это вопрос, касающийся многих заинтересованных сторон. Это требует скоординированных усилий со стороны правительств, региональных и международных организаций, частного сектора, гражданского общества, а также самой «восьмерки» по линии Римской/Лионской группы, с тем чтобы предотвращать, сдерживать и пресекать использование ИКТ в террористических и криминальных целях. Особое внимание необходимо

уделять всем видам атак, направленных против инфраструктуры, сетей и сервисов, в том числе распространению через интернет вредоносного программного обеспечения и действию «зомби-сетей» (ботнетов). В этой связи мы признаем, что чрезвычайно важно повышать осведомленность пользователей. Мы также признаем, что необходимо интенсифицировать международное сотрудничество для защиты критически важных ресурсов, ИКТ и других объектов инфраструктуры. Предметом нашей озабоченности остается потенциальная возможность использования интернета в целях, противоречащих задачам поддержания международного мира и безопасности, или же способных оказать негативное воздействие на целостность критически важных систем. Правительства в контакте со всеми другими заинтересованными сторонами должны заниматься разработкой норм поведения в киберпространстве и общих подходов к его использованию. По всем этим вопросам мы нацелены на осуществление дальнейших шагов в рамках всех соответствующих форумов.

18. Мы призываем все заинтересованные стороны вести борьбу с использованием интернета для торговли детьми и их сексуальной эксплуатации. Мы будем вести работу по созданию среды, в которой дети могут безопасно пользоваться интернетом, путем повышения осведомленности детей, в том числе о рисках, и стимулирования достаточного контроля со стороны родителей, не нарушающего при этом свободы выражения мнений.

19. Мы признаем важность облегчения доступа к интернету для развивающихся стран. После Окинавского саммита был достигнут значительный прогресс, и в этом отношении мы отдаем должное усилиям развивающихся стран, а также других заинтересованных сторон, правительств, представителей частного сектора и НПО, которые предоставляют ресурсы, делятся экспертным опытом и внедряют инновации. Мы приветствуем инициативы, в партнерстве с частным сектором, по использованию интернета для целей развития, связанных, в частности, с образованием и медицинским обслуживанием.

20. Поддерживая модель управления интернетом с участием широкого круга заинтересованных сторон, мы призываем всех участников данного процесса активизировать сотрудничество в рамках всех международных форумов, где рассматриваются вопросы управления интернетом, а также между ними. В этой связи необходимо проявлять гибкость и открытость, с тем чтобы адаптироваться к высоким темпам развития и расширения области применения технологий и методов ведения бизнеса. В этой модели правительства должны играть ключевую роль.

21. Мы приветствуем проведение интернет-форума «Группы восьми» (e-G8), который состоялся 24–25 мая в Париже накануне нашего Саммита, и подтверждаем нашу приверженность таким усилиям с участием широкого круга заинтересованных сторон, которые до сегодняшнего времени обеспечивали эволюционное развитие Интернет-экономики. Инновационный формат этого форума обеспечил участие целого ряда действующих в Интернет-пространстве субъектов в обсуждении основополагающих целей и основных проблем, с которыми сталкиваются граждане, бизнес и правительства в этой сфере. Свободная и плодотворная дискуссия в рамках этого форума – вклад в работу всех соответствующих форумов, на которых рассматриваются существующие и будущие вызовы.

22. Мы с надеждой ожидаем появления новых возможностей для укрепления международного сотрудничества во всех перечисленных областях, в т.ч. в контексте предстоящего в сентябре с.г. в Найроби Форума по вопросам управления интернетом, других посвященных этой тематике мероприятий ООН, Встречи высокого уровня в рамках ОЭСР по теме «Интернет-экономика: инновации и развитие», провести которую планируется в июне с.г. в Париже, Лондонской конференции по кибербезопасности в ноябре с.г. и Конференции по вопросам авторского права (Авиньон, ноябрь с.г.). Эти мероприятия мы рассматриваем как позитивные шаги, направленные на достижение прогресса в этой важной сфере.

<...>

Содержание

Предисловие 3
Раздел I. Кибербезопасность и управление интернетом 8
М.Б. Касенова Основы трансграничного управления интернетом 8
О.В. Демидов. Международная безопасность в области использования ИКТ: глобальные тенденции и национальные интересы России 47
Раздел II. Документы и материалы 87
1. Техническое сообщество, частный сектор 87
• **Корпорация интернета по распределению имен и адресов (*ICANN*)** 87
Подтверждение обязательств со стороны Министерства торговли США и Корпорации интернета по распределению имен и адресов 87
Стратегический план *ICANN*. Июль 2012 г.– июнь 2015 г. *(Извлечения)* 94
• **Форум по управлению интернетом (*IGF*). Динамичная коалиция по правам и принципам интернета Форума по управлению интернетом** 111
Предварительная Хартия по правам человека и принципам интернета. 2010 г. 111
• **Ассоциация прогрессивных коммуникаций (*APC*)** 113
Кодекс лучшей практики по информации, участию и информационной открытости (прозрачности) управления интернетом. Версия 1.1. 2010 г. ...113
2. Государства 119
2.2. Российская Федерация 119
Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» 119
Концепция внешней политики Российской Федерации (утверждена Президентом РФ 12 февраля 2013 г.) 121
Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года 152
Конвенция об обеспечении международной информационной безопасности (концепция). 2011 г. 160
Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. 2011 г. 178
2.3. Соединенные Штаты Америки 188
Международная стратегия в отношении киберпространства. 2011 г. (*Извлечение*) 188
Государственный департамент США о Докладе ООН по вопросам кибербезопасности и киберпространства от 8 июня 2013 г. 208
2.4. Финляндия 210
Стратегия кибербезопасности Финляндии. 2013 г. 210
2.5. Индия 225
Национальная политика кибербезопасности. 2013 г. 225
3. Международное сотрудничество государств 237
Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности. 2010 г. 237
Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций

от 12 сентября 2011 г. на имя Генерального секретаря ООН (с Приложением: «Правила поведения в области обеспчения международной информционной безопасности») 245
4. Международные организации....249
4.1. Организация Объединенных Наций (ООН)....249
Резолюция Генеральной ассамблеи ООН от 21 декабря 2009 г. «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» 249
Резолюция Генеральной ассамблеи ООН от 3 декабря 2012 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» 256
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Проект резолюции Генеральной Ассамблеи. 2013 г. 259
Право на неприкосновенность частной жизни в цифровую эпоху: Проект резолюции Генеральной Ассамблеи. 2013 г. 263
Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. 2010 г.....266
Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. 2013 г. 278
4.2. Международный союз электросвязи (МСЭ) 294
Регламент Международной Электросвязи. 14.12.12 г.....294
Резолюции Международного союза электросвязи. 2012 311
4.3. Совет Европы (СЕ)....319
Декларация Комитета министров о принципах управления интернетом. 2011 г. 319
Стратегия Совета Европы по управлению интернетом на 2012–1015 годы. 2012 г. (*Извлечения*)....323
Программа подготовки судей и прокуроров по вопросам киберпреступности: концепция. 2009 г. (*Извлечения*) 324
4.4. Организация по безопасности и сотрудничеству в Европе (ОБСЕ).....367
Совместная декларация о свободе выражения мнения в интернете. 2011 г. (*Извлечение*)....367
4.5. Организация экономического сотрудничества и развития (ОЭСР).....373
Рекомендация Совета ОЭСР о принципах формирования интернет-политики. 2011 г. 373
4.6. Содружество Независимых Государств (СНГ)....385
Модельный закон «Об основах регулирования Интернета». 2011 г. 385
Модельный информационный кодекс для государств – участников СНГ. 2012 г.....392
4.7. Шанхайская организация сотрудничества (ШОС) 417
Соглашение между Правительствами государств – членов Шанхайской организации сотрудничества «О сотрудничестве в области обеспечения международной информационной безопасности» (Екатеринбург, 2009 г.) 417
4.8. Европейский Союз (ЕС)....428
Стратегия кибербезопасности Европейского Союза. 2013 г. 428
4.9. «Группа восьми» (*G*8)....457
Довильская Декларация «Группы восьми». 2011 г. (*Извлечение*) 457

КИБЕРБЕЗОПАСНОСТЬ И УПРАВЛЕНИЕ ИНТЕРНЕТОМ:

Документы и материалы
для российских регуляторов и экспертов

Редактор *В.Ю. Станковская*
Корректор
Художественное оформление: *В.В. Самойлова*
Компьютерная верстка: *О.Л. Божьева*

Подписано в печать 00.01.2014. Формат 60×90 $^{1}/_{16}$. Бумага офсетная.
Гарнитура Newton. Печать офсетная. Печ. л. 29. Тираж 0000 экз.
Заказ №

Издательство «Статут»:
119454, г. Москва, ул. Лобачевского, д. 92, корп. 2;
тел./факс: +7(495) 649-18-06
E-mail: book@estatut.ru
www.estatut.ru